SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I8P103

Volume 11 Issue 8, 22-30, August 2024
© 2024 Seventh Sense Research Group®

Original Article

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

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

[1]*Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Tamilnadu, India.*
[2]*Department of Computer Science and Engineering, RMK College of Engineering and Technology, Tamilnadu, India.*

[1]*Corresponding Author : maniveenac@gmail.com*

Received: 27 May 2024 Revised: 10 July 2024 Accepted: 04 August 2024 Published: 31 August 2024

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 generate EfficientNet b7 feature frameworks for text classification tasks automatically. 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.*

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]. The Internet of Things (IoT) has become ubiquitous as a result of urbanisation. 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 IoT, 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 decryptable by a user chosen by the data owner [5]. Deep learning techniques have contributed significantly to 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. Using an activation function, other cutting-edge CNN models use ReLU, although EfficientNet uses a novel activation function termed Swish, which is the sigmoid and linear activation functions reduplicated. 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 internet communication technology, which satisfies the need 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 that 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 that 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.

By suggesting that parking recommender systems take advantage of Elliptic Curve Cryptography (ECC) and Local Differential Privacy (LDP), Khaliq et al. (2022) [11] addressed research gaps as were previously identified [11]. We recommended using a Hash for the Messages Authentication Code (HMAC) equal authentication method based on ECC that guarantees secrecy and communication integrity.

Shen et al. (2022) [12] have proposed that This research offers a confidentiality social computing architecture for health management federated learning, which addresses this problem. Multiple user terminals hold user data to reduce exposure. For an Internet with Things data sharing strategy based on edge computing, Shen et al. (2023) [13] have provided the evolutionary preservation of privacy learning techniques. This solves the previously described issue. By applying evolutionary game theory, this method generates a reward matrix that appropriately captures the interaction with edge nodes and Internet - Things devices, which 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 that 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 that Academics from all over the world are interested in the difficult task of routing in MANETs. Using the augmented chaotic map, a novel method for controlling encryption and decryption operations for MANET and IoT data processing is proposed. The SP-DAC approach was proposed by Singh et al. (2023) [17]. It leverages cloud and fog architecture to offer a private and secure solution for data classification and aggregation. Using the SP-DAC method, three machine learning models in the externalized cloud identify the combined data at the fog node.

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] use the idea of Ciphertext-Policy Attributes-Based Encryption (CP-ABE) to secure the data and offer fine-grained access control. To assess the accuracy of the classifier, the total likelihood of the data across an array of users is called the Bayes Score.

Kumar et al. (2024) [20] have proposed encrypting a person's private and sensitive information using deep neural networks and Statistical Differential Privacy (SPD). Human-specific category-based and numeric data are sent into the neural network's input layer. The following restrictions were discovered with these techniques. Low accuracy with various methods for detection of text for real-time image datasets.

- The methods cannot detect all aspects of the text, and it affects training.
- The existing methods cannot detect new features; they only collect unique features and detect them as ensemble results.

The proposed method is designed to overcome these disadvantages.

3. Proposed Method

This section provides a detailed explanation of our suggested security augmentation technique and explains the CNN approach within the framework of social IoT. Our EfficientNetb7 technique generates the countermeasure samples. 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 analysing 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 significantly reduce the model's accuracy.

Our approach is based on the mechanisms of attention. 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.

Word2vec vector word integration and word location data embedding are two more important concepts. Prior to feature extraction, the word is preprocessed. Preprocessing includes operations such as breaking, feature extraction, identification, and word cleaning. A lot of noise data, such as misspelt words, words from other languages, and absurd sentences, is usually used to provide training examples for information extraction. Such noisy input will affect the fine-grained preference variables that are recreated. Denoising the assessment data in advance is, therefore, essential. Splitting is then eliminated to begin the feature extraction procedure, which will require more analysis. Roots can only be obtained by removing affixes.

For example, "cat-like," "cats," and "catty" are the roots that determine the string "cat;" The phrases "stemmed," "stemming," and "originated in conclusion" are derived from the word "stem," which acts as the basis of these expressions. Nouns, verbs, and adjectives are more inclined to convey fine-grained features. A segment of the speaking-tagged function is utilized in order to extract relevant speech bits from replies.

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

The phrases "wi" and "wj" 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 vector of weights for each conceptual unit in connection to sentence A by incorporating the elements of the matrix column into sentence B.

$$w_2vmatrix = \sum_i^n \sum_f^m cos\left(w_1, w_j\right) \quad (2)$$

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 = wc1, wc2, wck, 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.

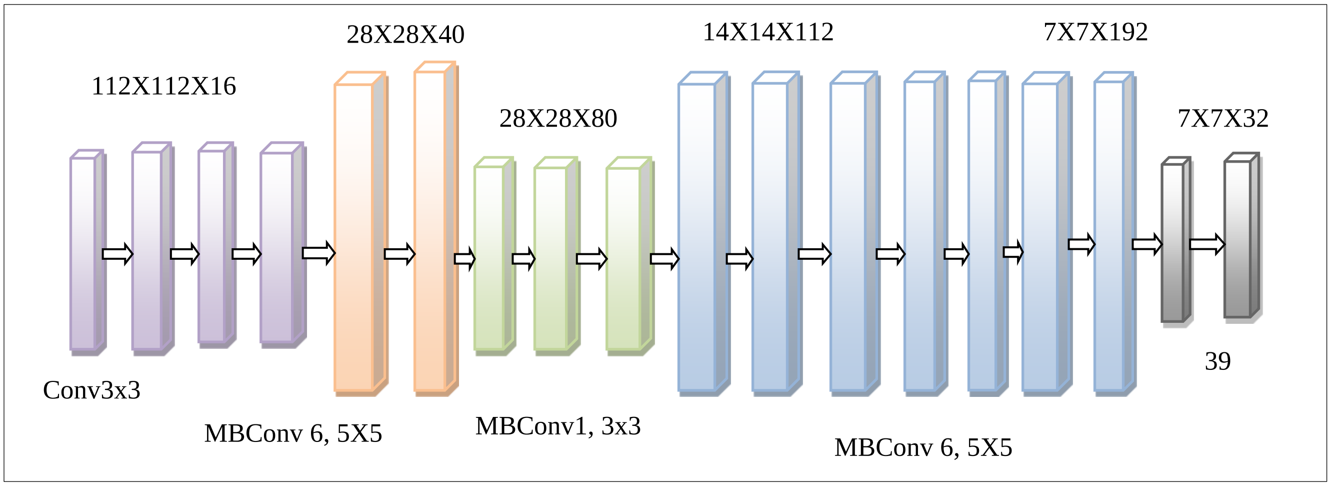

Fig. 1 EfficientNetb7 architecture

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 substantial blocks that 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 kernel size or k reflects the 2D convolution window's height and width. Equation (3) defines EfficientNet mathematically as:

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

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:

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

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

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 an 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 Social Web of Things' Essential Elements

Six main components make up the SIoT architecture, which is depicted in Figure 2: information, web services, trust management, relation leadership, architecture, and SIoT tools, which include platforms and datasets.

The majority of publications suggested a four-tier structure following the IoT architecture, which consists of devices (objects), worldwide connections, platforms, and applications, even though there is no standard design for SIoT. In order for devices to exchange or transfer data from a particular platform of the user application, they need to be somehow connected to the gateway's internet. In order to read and exchange data among objects such as middleware over the Internet, global connections are in charge of connecting objects or acting as an interface layer in platforms and devices using communication norms, gateways, and procedures (MQTT, HTTP, HTTPS, and CoAP).

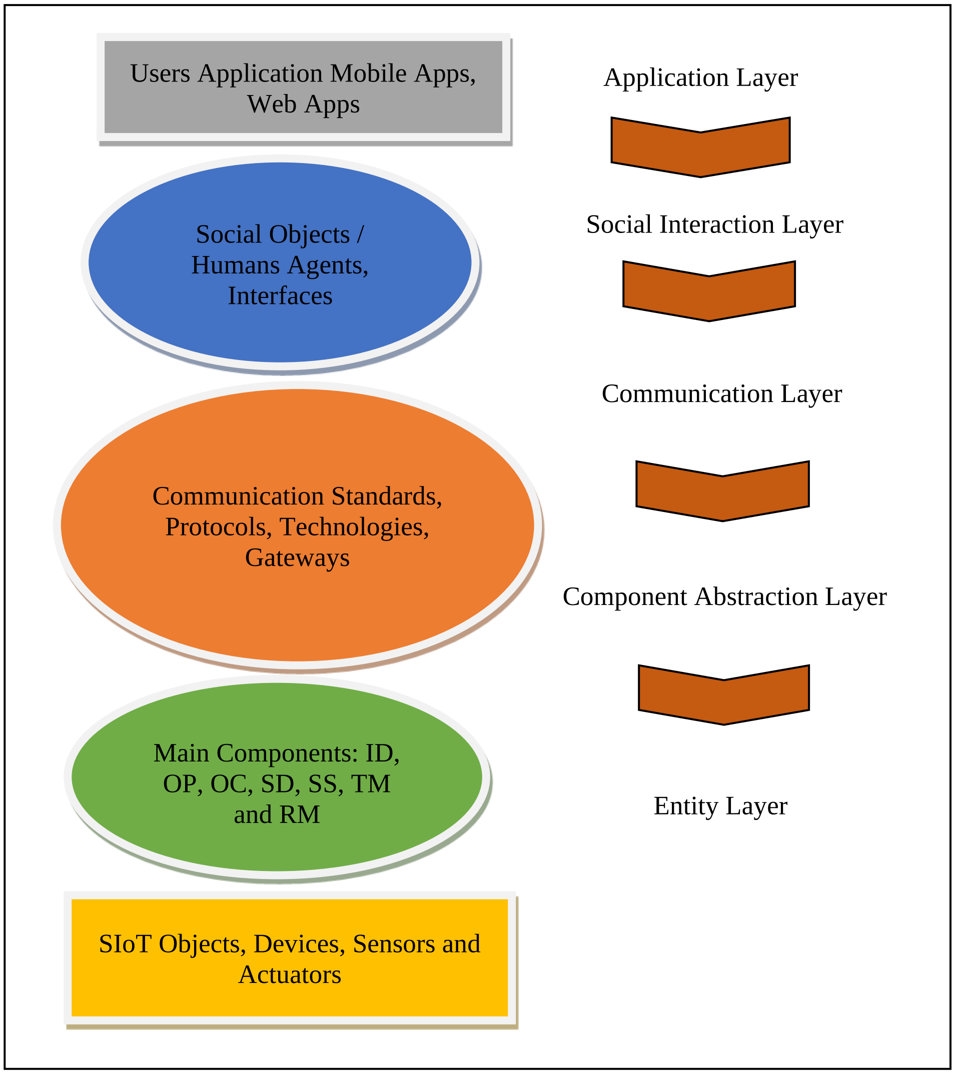
Users Application Mobile Apps, Web Apps
Application Layer
Social Objects / Humans Agents, Interfaces
Social Interaction Layer
Communication Layer
Communication Standards, Protocols, Technologies, Gateways
Component Abstraction Layer
Main Components: ID, OP, OC, SD, SS, TM and RM
Entity Layer
SIoT Objects, Devices, Sensors and Actuators

Fig. 2 SIoT architecture

3.4. Security and Privacy

Arguments for non-interactive zero awareness, Non-Interactive Zero-Knowledge (NIZK) reasons allow a prover to convince any verifier that a statement's validity without providing any additional 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.

4. Experimental Results

4.1. Datasets

We conduct our analysis using the MSRP, or Microsoft Researcher Paraphrase Corpus (MSRP) dataset. The Microsoft Researcher Semantic Corpus, which consists of 5100 pairs of translated sentences from online news sources, was used to construct the MSRP dataset. 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 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 Equations (6), (7), (8) and (9).

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \tag{6}$$

$$Precision = \frac{TP}{TP+FP} \tag{7}$$

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

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

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 shows that the EfficientNetb7-biLSTM model has 94% accuracy.

Table 1. Comparison of the precision of various cutting-edge techniques

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

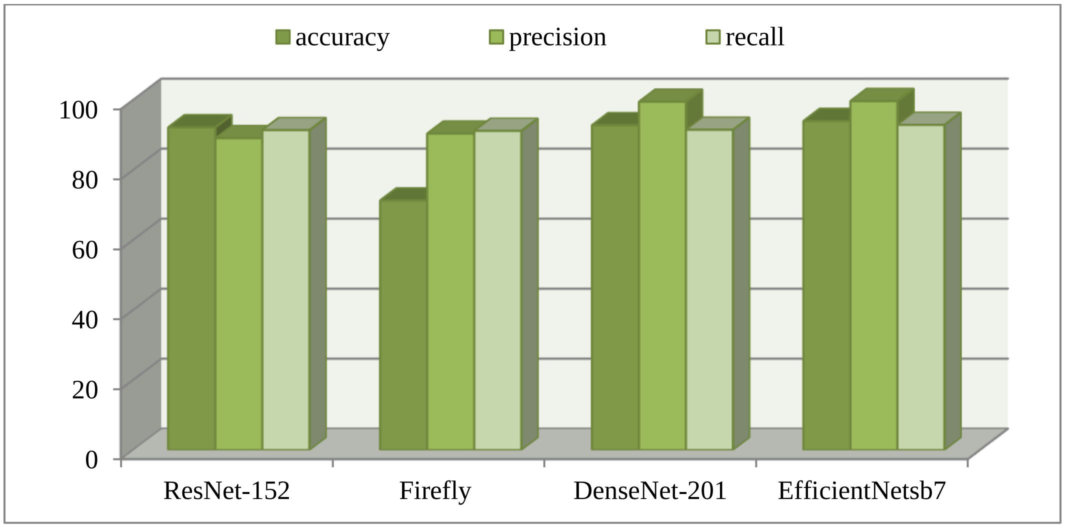

Fig. 3 Comparison plot of proposed work with existing works

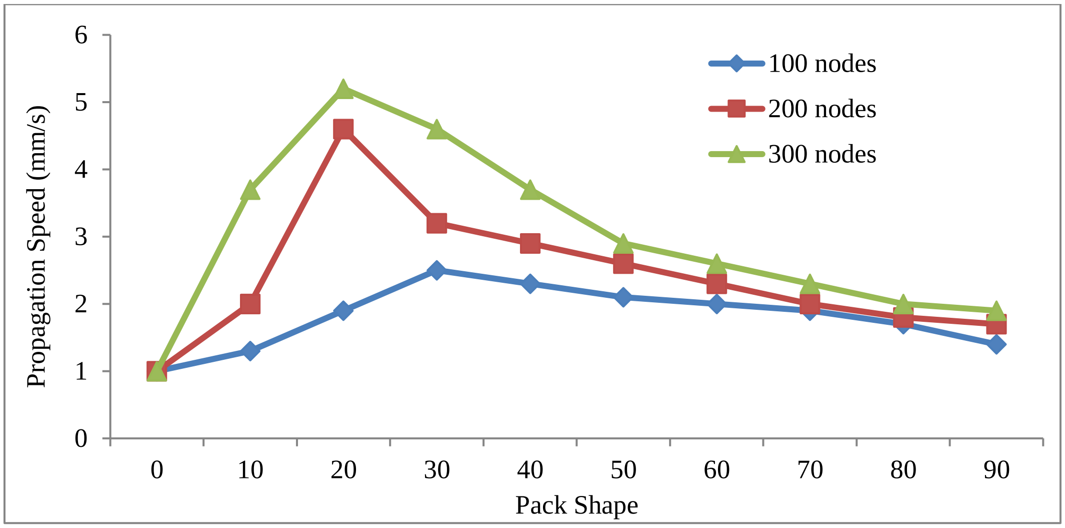

Fig. 4 Edge node propagation shapes

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 uniformly scales depth, width, and resolution for more efficient outcomes. EfficientNet employs a brand-new activated function called Swish, which is a replication of sigmoid or linear activation functions, while other cutting-edge CNN models use ReLU.

Additionally, with a score of 92.9%, EfficientNetsb7 had the highest F1 score. As Table 1 and Figure 3 show, the recommended approach outperforms other cutting-edge systems with an accuracy rate of 99.7%. The recommended EfficientNetsb7 performs more effectively compared to other cutting-edge methods.

In this case, p, 0.45, 0.47, and 0.49 represent the likelihood that Internet of Things devices will make malicious requests, and q = 0.8 represents the chance that edge nodes will reject their requests. It is noteworthy to observe that the likelihood of damaging requests from IoT devices decreasing leads to a faster convergence, suggesting a higher likelihood of adherence to the demands by edge nodes. The former achieves zero in around a half-game, whereas the later needs the third game to accomplish so, as seen by the cases of p = 0.45 and p = 0.49. If p is positive, it is anticipated that the transformation edge node approach, which is depicted in Figure 4, will be the authorized request.

Shapes of edge node propagation: selecting a strategy when $p < \frac{\beta\gamma+\varepsilon}{2\pi\tau\epsilon-\alpha\delta\epsilon+\beta\gamma+\epsilon\rho}$.

4.3. ROC Curves

The measurement of the Area Under the Curve of ROC (AUC) Ac, which is useful in assessing a device's ability to distinguish between two diagnostic classifications, is displayed in Figure 5. The ROC curves produced by several deep learning techniques are displayed in Figure 5.

The region (Ac) under the contour of the ROC curve for the EfficientNetB7 method is greater compared to any of the other methods, suggesting that compared to the other numbers, it is more akin to 1. The recommended method, therefore, has the greatest discriminating power.

4.3.1. Accuracy vs Epoch

Figure 6 displays the precision %. Epoch graph that was obtained during the validation and training stages. It illustrates how important the suggested system is.

4.3.2. Loss vs Epoch

As observed by Figure 7, which displays the loss vs epoch graph produced during the training and validation phase, the proposed system is highly significant.

4.3.3. Friedman Aligned Ranking (FAR)

The proposed method's superiority was statistically confirmed by the use of the Fried Aligned Ranking (FAR) test, which is not parametric. Table 2 presents the results of the FAR test. The area that is beneath the curve, also known as the AUC measure is used in the study. The null assumption, and H0, is as follows: Even if all of the anticipated results are similar to one another and do not differ greatly from one another, the alternate theory (H1) contradicts the original hypothesis.

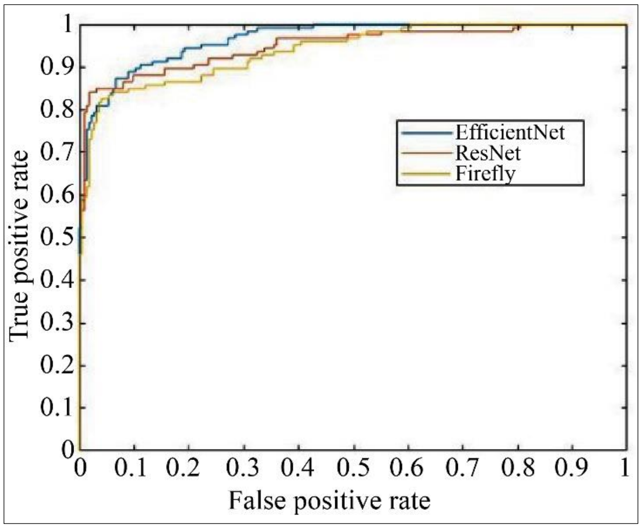

Fig. 5 ROC curves of different methods

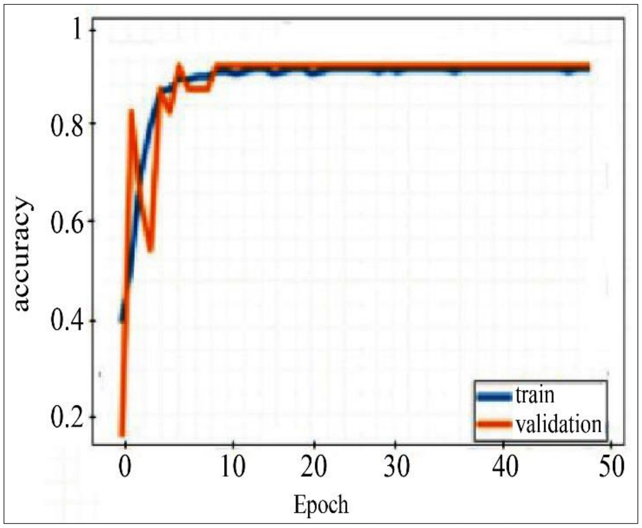

Fig. 6 Accuracy vs Epoch

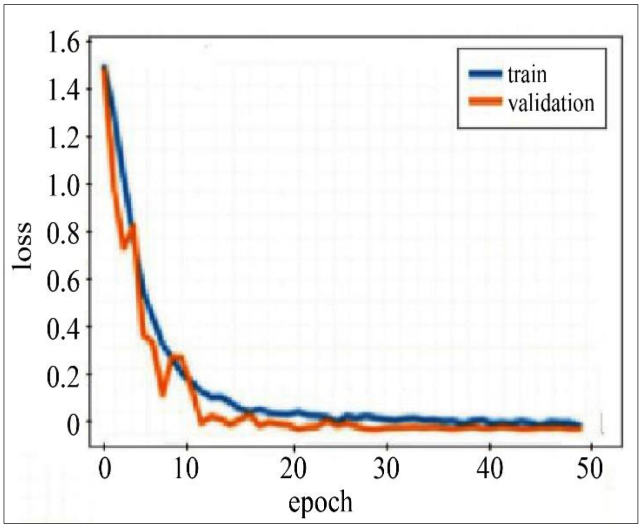

Fig. 7 Loss vs Epoch

To determine the models' statistical significance in this instance, the Friedman test was employed. Every model that passes the power source Friedman Test is assigned a rank based on its AUC. The lowest rank receives the largest number, while the highest rank receives the smallest.

Table 2 shows how well the recommended system performs in comparison to other available methods, such as Firefly and Resents. The recommended system has produced a higher score of 3.09.

Table 2. AUC curve based FAR rank

Methods	FAR rank
EfficientNet	3.09
ResNet	7.3
Firefly	9.5

Following the Holm procedure's rejection of the null hypothesis, a post-hoc study was carried out. The Holm approach compares the performance of one model against the others using the z-value and p-value. However, utilizing the Holm test, we were able to get 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 technique nor the KNN were disregarded. Unlike the other approaches, only the ANN network was removed because of its poor performance and notable variations.

Table 3. FAR rank based on the AUC curve

Methods	Unadjusted p-value
EfficientNetB7	0.147299
ResNet	0.09769
Firefly	0.000084

5. Conclusion

This paper proposed to automatically create EfficientNet b7 feature frameworks for text classification tasks using evolution deep learning. According to this study, text can be produced with more unique features while reducing loss and training time by utilising the EfficientNetsb7 architecture. A new adversarial text generation technique built on the EfficientNetsb7 architecture is advised. Moreover, the concept of adversarial training is extended to the field of text-Similarity analysis with the proposal of a proposed adversarial convolution neural network model.

In order to automatically generate feature EfficientNetsb7 frameworks and text classification tasks, this research proposed the development of a deep learning technique. Using only 25% of the provided datasets, EfficientNetsb7 did manage to generate network topologies for the manufacturing technique. Compared to other state-of-the-art approaches, the EfficientNetsb7 method is suggested and performs better. In the third, we developed a technical taxonomy of the core elements of the SIoT ecosystem. 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 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.

Acknowledgments

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support.

References

[1] Bao Le Nguyen et al., “Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data,” *Computers, Materials & Continua*, vol. 65, no. 1, pp. 87-107, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Rafik Hamza et al., “A Privacy-Preserving Cryptosystem for IoT E-Healthcare,” *Information Sciences*, vol. 527, pp. 493-510, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Prabhat Kumar et al., “PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326-2341, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xu Zheng, and Zhipeng Cai, “Privacy-Preserved Data Sharing Towards Multiple Parties in Industrial IoTs,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968-979, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Hua Deng et al., “A Flexible Privacy-Preserving Data Sharing Scheme in Cloud-Assisted IoT,” *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11601-11611, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mehdi Gheisari et al., “OBPP: An Ontology-Based Framework for Privacy-Preserving in IoT-Based Smart City,” *Future Generation Computer Systems*, vol. 123, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yi Sun et al., "PMRSS: Privacy-Preserving Medical Record Searching Scheme for Intelligent Diagnosis in IoT Healthcare", *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1981-1990, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Lei Cui et al., "Security and Privacy-Enhanced Federated Learning for Anomaly Detection in IoT Infrastructures," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3492-3500, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Omar A. Alzubi et al., "Blockchain and Artificial Intelligence Enabled Privacy-Preserving Medical Data Transmission in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Huiying Xu et al., "Privacy-Preserving Incentive Mechanism for Multi-Leader Multi-Follower IoT-Edge Computing Market: A Reinforcement Learning Approach," *Journal of Systems Architecture*, vol. 114, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Awais Abdul Khaliq et al., "A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy," *IEEE Access*, vol. 10, pp. 56410-56426, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Zhangyi Shen et al., "A Privacy-Preserving Social Computing Framework for Health Management Using Federated Learning," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1666-1678, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Yizhou Shen et al., "Evolutionary Privacy-Preserving Learning Strategies for Edge-Based IoT Data Sharing Schemes," *Digital Communications and Networks*, vol. 9, no. 4, pp. 906-919, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Nahla El-Haggar et al., "The Effectiveness and Privacy Preservation of IoT on Ubiquitous Learning: Modern Learning Paradigm to Enhance Higher Education," *Applied Sciences*, vol. 13, no. 15, pp. 1-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Mohit Kumar et al., "A Smart Privacy Preserving Framework for Industrial IoT Using Hybrid Meta-Heuristic Algorithm," *Scientific Reports*, vol. 13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] P. Satyanarayana et al., "Comparative Analysis of New Meta-Heuristic-Variants for Privacy Preservation in Wireless Mobile Adhoc Networks for IoT Applications," *Computer Communications*, vol. 198, pp. 262-281, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ashutosh Kumar Singh, and Jatinder Kumar, "A Secure and Privacy-Preserving Data Aggregation and Classification Model for Smart Grid," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 22997-23015, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Prashant Kumar Shukla et al., "Effective Privacy Preserving Model Based on Adversarial CNN with IBOA in the Social IoT Systems for CEC," *International Journal of Communication Systems*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kavitha Guda, K. Kavitha, and B. Sujatha, "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*, vol. 12, no. 8s, pp. 93-107, 2024. [CrossRef] [Publisher Link]

[20] G. Sathish Kumar et al., "Differential Privacy Scheme Using Laplace Mechanism and Statistical Method Computation in Deep Neural Network for Privacy Preservation," *Engineering Applications of Artificial Intelligence*, vol. 128, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] B. K. Tripathy, Deboleena Dutta, and Chido Tazivazvino, *On the Research and Development of Social Internet of Things*, Internet of Things (IoT) in 5G Mobile Technologies, Springer, Cham, pp. 153-173, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[22] Antonio M. Ortiz et al., "The Cluster Between Internet of Things and Social Networks: Review and Research Challenges," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 206-215, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jieun Kim, Xiangmin Fan, and Daniel Mossé, "Empowering End Users for Social Internet of Things," *IoTDI '17: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pp. 71-82, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[24] Luigi Atzori, Antonio Iera, and Giacomo Morabito, "SIot: Giving a Social Structure to the Internet of Things," *IEEE Communications Letters*, vol. 15, no. 11, 1193-1195, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[25] Nancy Gulati, and Pankaj Deep Kaur, "When Things Become Friends: A Semantic Perspective on the Social Internet of Things," *Proceedings of ICSICCS 2017 Smart Innovations in Communication and Computational Sciences*, Singapore, vol. 2, pp. 149-159, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Nancy Gulati, and Pankaj Deep Kaur, "Towards Socially Enabled Internet of Industrial Things: Architecture, Semantic Model and Relationship Management", *Ad Hoc Networks*, vol. 91, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] Orfefs Voutyras et al., "An Architecture Supporting Knowledge Flow in Social Internet of Things Systems," *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 100-105, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[28] Jens Groth, "On the Size of Pairing-Based Non-Interactive Arguments," *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Vienna, Austria, pp. 305-326, 2016. [CrossRef] [Google Scholar] [Publisher Link]