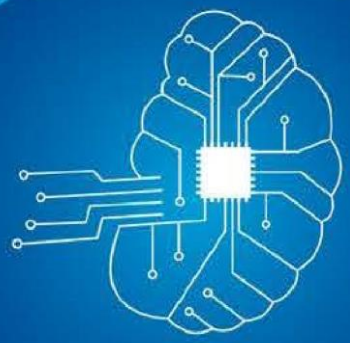
NEAR EAST UNIVERSITY

JOURNAL FOR ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS

Volume: 5 Issue: 1

ISSN: 3062-1968



www.neu.edu.tr

JOURNAL OF ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS
Uluslararası, Hakemli Dergi / International, Refereed Journal

July, 2026
Cilt-Volume 05/ Sayı-Issue 01

Foundation Year of the Journal
2022

Publication Contact
Editorial Board
editor.aiit@neu.edu.tr

Contact for Information
info.aiit@neu.edu.tr

Address and Contact

Near East University Innovation and Information Technologies
Centre International Research Center for AI and IoT
Yakın Doğu Bulvarı, PK: 99138Lefkoşa / TRNC, Mersin 10 –
Türkiye Phone:+90 (392) 223 64 64/+90 (392) 680 20 00
Faks:+90 (392) 223 64 61

http://dergi.neu.edu.tr/ https://iot.neu.edu.tr/

CONTENTS

Near East University

Journal for Artificial Intelligence and Internet of Things

Volume: 5
Issue: 1

ISSN
3062-1968

A MULTI-TASK VISION TRANSFORMER FOR JOINT PLANT DISEASE CLASSIFICATION AND LOCALIZATION
ORTAK BİTKİ HASTALIĞI SINIFLANDIRMASI VE KONUMLANDIRMASI İÇİN ÇOK GÖREVLİ BİR GÖRSEL TRANSFORMER MODELİ

Nasim AHMADZADEH NOBARI AZAR[1]

ABSTRACT

Plant diseases pose a serious threat to agricultural productivity and food security, particularly in regions with limited access to expert diagnosis. While deep learning–based methods have shown strong performance in plant disease recognition, most existing approaches focus solely on classification and provide limited spatial interpretability. In this paper, we present MTL-ViT, a multi-task Vision Transformer framework for joint plant disease classification and localization using leaf images. The proposed model employs a shared Vision Transformer backbone with task-specific heads for disease classification and bounding-box localization. Experiments are conducted on a curated subset of the PlantVillage dataset using an 80:20 train–validation split. The results show that the proposed framework achieves 88.89% classification accuracy while simultaneously localizing disease regions with a mean IoU of 0.99 under controlled imaging conditions. Ablation studies highlight the trade-off between predictive accuracy and spatial interpretability, demonstrating the practical value of multi-task learning for explainable plant disease analysis.

Keywords: *Vision Transformer, Multi-Task Learning, Plant Disease Classification, Disease Localization, Agricultural Computer Vision.*

ÖZ

Bitki hastalıkları, özellikle uzman teşhisine erişimin sınırlı olduğu bölgelerde tarımsal verimlilik ve gıda güvenliği açısından ciddi bir tehdit oluşturmaktadır. Derin öğrenme tabanlı yöntemler bitki hastalığı tanımada güçlü bir performans sergilemiş olsa da, mevcut yaklaşımların çoğu yalnızca sınıflandırmaya odaklanmakta ve sınırlı mekânsal yorumlanabilirlik sunmaktadır. Bu çalışmada, yaprak görüntüleri kullanılarak bitki hastalığının hem sınıflandırılması hem de konumlandırılması için çok görevli bir Görsel Transformer (Vision Transformer) çerçevesi olan MTL-ViT önerilmektedir. Önerilen model, hastalık sınıflandırması ve sınırlayıcı kutu (bounding-box) konumlandırması için göreve özgü başlıklara sahip, paylaşılan bir Görsel Transformer omurgası kullanmaktadır. Deneyler, PlantVillage veri kümesinin seçilmiş bir alt kümesi üzerinde, %80:20 eğitim-doğrulama ayrımı kullanılarak gerçekleştirilmiştir. Sonuçlar, önerilen çerçevenin kontrollü görüntüleme koşulları altında %88,89 sınıflandırma doğruluğu elde ederken, hastalıklı bölgeleri 0,99 ortalama IoU değeriyle eş zamanlı olarak konumlandırabildiğini göstermektedir. Ablasyon çalışmaları, tahmin doğruluğu ile mekânsal yorumlanabilirlik arasındaki dengeyi ortaya koyarak, çok görevli öğrenmenin açıklanabilir bitki hastalığı analizindeki pratik değerini göstermektedir.

Anahtar kelimeler: *Görsel Transformer, Çok Görevli Öğrenme, Bitki Hastalığı Sınıflandırması, Hastalık Konumlandırması, Tarımsal Bilgisayarlı Görü.*

[1] Assist. Prof., Yakın Doğu Üniversitesi, Yapay Zeka ve Bilişim Fakültesi, Bilgisayar Bilgi Sistemleri Bölümü,nasim.ahmadzadeh@neu.edu.tr

1. INTRODUCTION

Agriculture is a key sector in food chains, employment, and economies globally. The need for agricultural produce is on a greater scale as the population of the world keeps expanding. Nevertheless, agriculture is now confronted with new threats due to the impact of climate change, land degradation, limited water supplies, and a greater incidence of pests and plant diseases. Of the many stresses, plant diseases have posed a significant threat to crops. Plant pests and diseases cause an annual loss of between 20%–40% of the world's crop by weight [1]. This results not only in great economic loss but also contributes to hunger. Smallholder farmers are particularly affected by the absence of effective diagnostic and control tools, as they depend on few individuals for their livelihoods. This is especially true where there are late diagnoses using large quantities of pesticides.

Traditional identification of plant diseases is through visual inspection and then referral to experts or laboratories. Though this is perhaps reliable, it is also a long and expensive process, and not very pragmatic for large farms. In villages, it may be difficult to locate a laboratory or someone who feels comfortable performing plant disease detection.

The rapid development of artificial intelligence (AI), especially deep learning technology, has offered a new approach to automatic farming diagnosis. In recent years, deep learning-based methods have gained significant success in visual recognition tasks by exploiting hierarchical feature representations [2]. Computer vision has significantly advanced plant disease detection by enabling automated, accurate, and large-scale analysis of crop health in smart agriculture systems [3]. CNNs are capable of discriminatively learning features that can be used for image classification. In plant disease diagnosis, CNNs have been found to be capable of capturing small visual signs that may indicate disease in a plant and may also be imperceptible to humans. Recent systematic reviews have pointed out that the application of computer vision and deep learning for plant disease diagnosis is on the rise [4].

This work focuses on integrating Vision Transformer-based representations into a multi-task learning framework for joint plant disease classification and localization, rather than proposing a novel transformer architecture. This research shows that the application of attention-driven feature learning can significantly improve disease classification and location within a controlled dataset setting.

Contribution and Scope. In this paper, we address the question of how to incorporate Vision Transformers into a multi-task learning pipeline for simultaneously classifying and localizing plant diseases. Instead of introducing a new transformer architecture, the contribution of this work is the empirical study and system-level design of how shared transformer representations trade off predictive accuracy and spatial interpretability. Under controlled imaging conditions, this framework is evaluated with the goal of providing a clear picture of how transformer-based multi-task learning for agri-vision scales and of outlining its strengths and pitfalls as an alternative to conventional deep networks in agricultural vision tasks, in line with the empirical and application-centered focus of conference contributions.

2. RELATED WORKS

Plant disease is a signaling symptom that has been widely studied in the literature using computer vision and machine learning methods. Existing works can be roughly grouped into classical machine learning approaches, deep learning–based frameworks, transfer learning algorithms, multi-task models, and more recent Vision Transformer–based architectures.

Before deep learning became well known in the object and disease-detection field, classical machine-learning methods like Support Vector Machines (SVM), K-Nearest Neighbor Methods (K-NN), Decision Trees and Random Forests were typically used to detect plants and/or plant diseases from images. When these methods were employed at the time, they mainly made use of handcrafted features of image properties, including texture, color and shape. While they exhibited reasonable success on properly aligned and free-of-noise images, their performance did not hold up as well in real-world applications. In such cases, visual backdrops, fluctuations in the amount of light present (occasionally affecting what can be seen in an image), and noise exist. In addition, methods that used handcrafted features were limited in terms of scalability and/or transferability to other species of plants and different characteristics of diseases. This resulted in the push to utilize deep-learning methodologies. The introduction of Convolutional Neural Networks (CNNs) has been a game-changer with respect to the automatic identification of plant diseases. For example, Sladojevic et al.[4], conducted research that established CNNs could identify distinct features from leaf images directly, without creating additional features through human initiative, using only raw images. After that, researchers began to pursue more complicated types of CNNs, namely VGG, ResNet50 and Inception, due to their superior capabilities related to the extraction of features from a hierarchy of different types of features[5], [6]. Collectively, the aforementioned CNNs allowed for increased classification accuracy across various types of crops and various types of diseases, using well-established datasets, such as PlantVillage. Nonetheless, CNN-based methodologies rely heavily on local regions to determine classification. Therefore, they struggle with detecting long-range dependencies and/or global context when assessing leaf-disease patterns due to the properties of the items being analyzed. CNN-based methodologies also normally suffer from a decrease in performance when/if images are collected in the field under unconstrained conditions.

The limited availability of labeled datasets for plant disease images has created a strong interest in transfer learning as a suitable method. Fine-tuning convolutional neural networks (CNNs) previously trained on large datasets such as ImageNet has provided faster convergence, higher accuracy, and the requirement for less training data [7]. Research comparing the various visualizer-based (e.g., VGG, ResNet, and Inception) transfer learning techniques have found great success for classification on controlled datasets (e.g., PlantVillage). Unfortunately, most transfer learning models experience a domain shift issue when used for an actual real-world application. i.e., when transferring domains, there are unaccounted factors such as lighting differences, background differences, and hardware differences between the original trained model and the real model.

Thus, generalization remains a significant challenge to TPDD systems engaged in transfer learning. In order to deal with the challenge of generalization, the concept of multi-task learning (MTL) has arisen. It is to create a common representation of several tasks that are related in some manner in order to improve generalization. There are limited published papers on the utilization of MTL to address plant disease assessment once multiple complementary tasks (1) disease type and symptoms, and/or (2) symptoms and severity) are performed

simultaneously. Previous studies have shown that there are benefits to creating shared representations among complementary tasks. These allow the model to be more discriminative in its ability to locate biologically meaningful features. Recent research has proposed the use of a MTL approach using vision transformer (ViT) models to locate and classify plant diseases in an environment similar to those of the PlantVillage project [8]. In summary, while there are several potential advantages to MTL for grape plant disease classification and symptom detection, most agricultural applications are still reliant on CNNs. There is currently very little research involved in the application of transformer architectures for classifying and locating plants. ViTs provide a novel way of representing a photograph as a collection of patches [9]. Self-attention mechanisms allow for the contextualization of a photograph globally by considering how each patch relates to all other patches [9]. A key difference between CNNs and ViTs is that the latter process an image as a sequence of fixed-size patches, thus enabling better modeling of long-range dependencies and global context.

Recent studies have shown that ViTs achieve superior or competitive performance compared to traditional CNNs in several plant disease recognition tasks, especially under challenging conditions such as cluttered backgrounds and variable illumination. Additionally, hybrid CNN–ViT models have been introduced to fuse local representation learning with global attention mechanisms. However, most current research on ViTs is limited to disease classification tasks, and little attention has been paid to incorporating ViTs into MTL frameworks for jointly performing classification and localization. In addition to leaf-scale image classification, image-based plant disease detection systems have also been designed for field-based usage. Deep learning models that can be implemented on smartphones could act as quick diagnostic tools for farmers, while aerial vehicles such as UAVs mounted with RGB or multispectral sensors provide large-scale monitoring by automatically capturing images.

While these methods improve early disease detection and field coverage, they introduce additional challenges related to computational workload, environmental variation, and data complexity. Models trained on laboratory-collected datasets often lose a significant amount of their predictive power under real-world agricultural conditions, making it increasingly necessary to develop robust and interpretable learning methodologies. Although the problem of plant disease detection has been widely studied, several key issues remain insufficiently explored in the literature:

- Poor generalization to different environments and field situations
- Absence of unified architectures for disease classification and localization
- Lack of effective utilization of Vision Transformers (ViTs) in multi-task architectures
- Limited information on spatial disease patterns from large-scale annotated datasets
- Infeasibility of early infection and co-infection monitoring
- Difficulty in deployment within resource-starved environments due to excessive computational requirements
- Limited validation under field conditions with reduced control

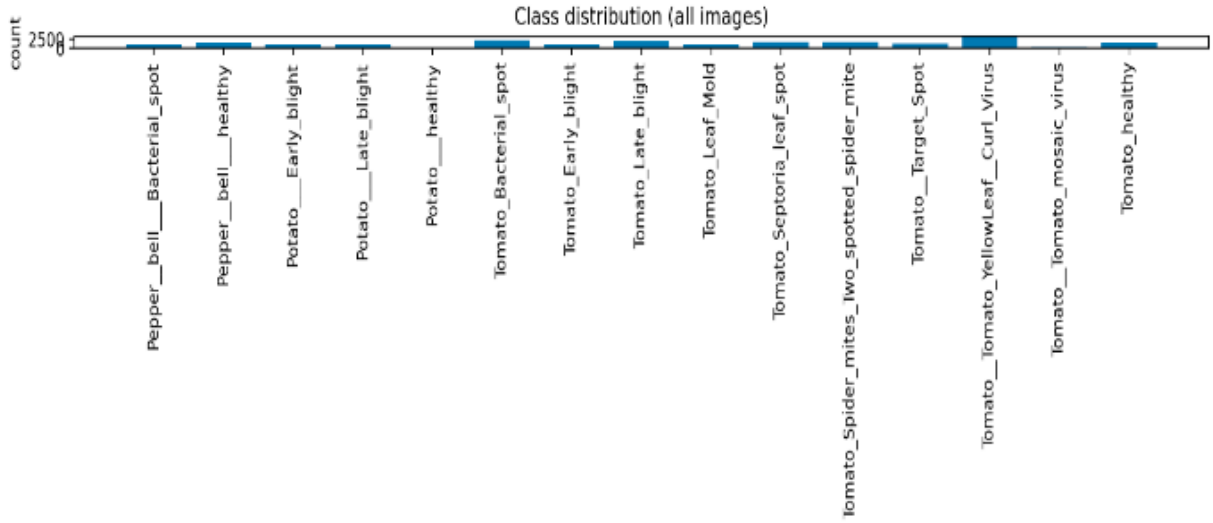
These shortcomings motivate the proposed Multi-Task Learning Vision Transformer (MTL-ViT) model, which aims to address plant disease classification and localization simultaneously using a transformer-based representation.

3. METHODOLOGY

In this section, we describe the data used to generate the training data for the Plant Disease Classification and Localization system, the multi-task Vision Transformer architecture used to train the model, as well as the procedure for evaluating the trained model. The PlantVillage dataset consists of 50,000+ images that depict 38 different crops/disease combinations. Therefore, it cannot be used in that entire dataset for the evaluation of the classification and localization of plant diseases [10]. The PlantVillage dataset consists of 50,000+ images that depict 38 different crops/disease combinations. Therefore, it cannot be used in that entire dataset for the evaluation of the classification and localization of plant diseases. The dataset was then divided into training and validation with an 80:20 stratification, giving us 1,980 images for the training set and 495 images in the validation set.

Figure 1 illustrates the distribution of classes in the curated PlantVillage subset taken for this study. By not being very skewed toward just one class, we can infer that the dataset does not suffer from a severe imbalance, and therefore the impact on training of potential unbalancing is minimized.

Figure 1: Class distribution of the PlantVillage subset across all disease and healthy categories



The entire dataset was split 80:20 into training and validation subsets to have enough data to train the model and at the same time test on unseen samples. Stratified sampling was used in order to maintain a balance of classes between the two subsets. The splitting stage was performed by means of TensorFlow's ImageDataGenerator utilities in order to guarantee reproducibility and coherence. The size of each input image was rescaled to 224 × 224, which is a commonly used scaling factor used in standard Vision Transformer architecture. The pixel values were rescaled from [0, 255] to [0, 1] for better numerical stability during training. MobileNetV2-based preprocessing is popular in previous works, but it was not used here. Instead, all preprocessing steps are narrowly tailored for the ViT-B/16 backbone. Data augmentation was used during

training for generalization with random rotations, horizontal reflection, and marginal scaling.

The PlantVillage dataset does not have annotations indicating the spatial location of disease regions. Bounding boxes were manually annotated for each of the 2,475 images in order to assist the localization for segmentation. These annotations indicate the main disease area of every leaf image. The bounding box was described by four coordinates of the upper-left and bottom-right corners of the disease area. One bounding box was marked around the largest observed infected region when several areas with disease were visible to prevent confusion. For healthy leaf images, bounding box targets were nullified. These bounding box annotations allow the model to learn spatial disease localization and classification simultaneously, thus improving model interpretability for implementation in agricultural decision-support systems.

A Vision Transformer (ViT-B/16) was used as the shared feature extraction model. In contrast to CNNs with local receptive fields, transformers communicate information about images as sequences of patches of a fixed size and leverage self-attention to model global contextual relationships [9]. The input image is split into non-overlapping patches of size 16 × 16 pixels [9]. Each patch is projected to a feature vector, and a positional embedding is added for encoding spatial information. The output sequence is fed to several transformer encoder layers, which are composed of multi-head self-attention and feed-forward networks combined with residual connections. The ViT backbone could help the model capture long-range dependencies on leaf surfaces, which is crucial for detecting plant diseases with symptomatically distributed patterns across leaf surfaces such as discoloration, vein distortion, or irregular lesions.

The ViT backbone generates a unified latent representation, which is then shared by the classification and localization heads. For joint disease classification and localization, the proposed method was formulated in a multi-task learning (MTL) framework [11]. A ViT encoder shared between the two task-specific output heads is used:

- Disease Classification Head

  This head is comprised of fully connected layers and a softmax activation layer to predict disease class labels. Categorical cross-entropy loss is utilized to optimize the classification task [12].

- Disease Localization Head

  The coordinates (x_1, y_1, x_2, y_2) of the bounding box are predicted in the localization head through regression layers. During the optimization of bounding box predictions, Smooth L1 loss is used [13].

Both heads are fine-tuned simultaneously, and gradients from both tasks update the same transformer backbone. The total training objective is a weighted combination of classification and localization losses. The loss was weighted equally to balance classification and spatial localization. An overview of our MTL-ViT framework is depicted in Fig. 2; it has a common ViT backbone with two task-specific heads.

The model was trained on a GPU-enabled Google Colab environment. The hyperparameters were selected based on empirical performance observed in preliminary experiments and are consistent with best practices for transformer-based models.

Figure 2: Overall architecture of the proposed MTL-ViT framework for plant disease classification and localization.

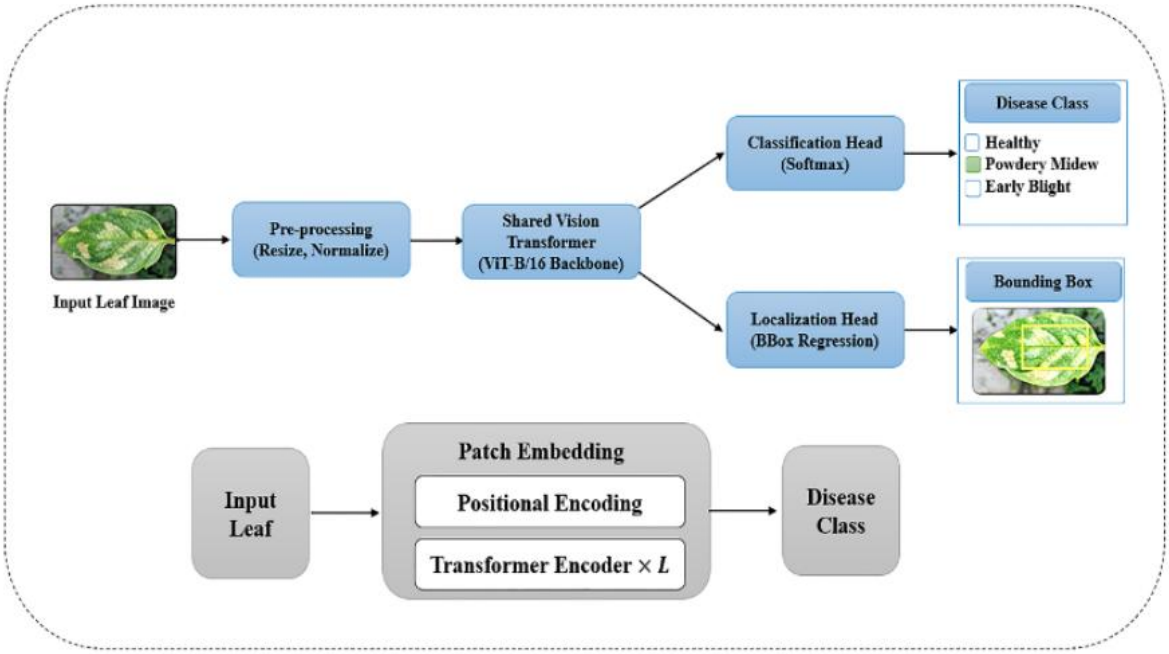


Table 1: Reported Methods Perform Classification Only And Do Not Provide Localization

Hyper-parameter	Value
Optimizer	AdamW
Initial learning rate	1e-4
Batch size	8
Epochs	20
Weight decay	0.01
Scheduler	Cosine Annealing
Loss weights	Classification: 1.0, Localization: 1.0
Data Split	80:20

Early stopping and learning rate annealing were employed to prevent overfitting and ensure smooth convergence. Model weights were saved based on validation performance. The localization performance was measured in terms of Intersection over Union (IOU) between predicted and actual bounding boxes. IOU is calculated by the intersection area divided by the union area of predicted and annotated bounding boxes [14] (equation (1)):

$$IOU = \frac{Area\ of\ Overlap}{Area\ of\ Union} \quad (1)$$

For IOU calculation, only images with visible symptoms of the disease were considered and healthy samples are not involved. Healthy leaf samples were excluded from the IoU evaluation because no disease bounding boxes are defined for these images, making localization metrics inapplicable. The localization performance in the number is the average IOU across all annotated validation images. All experiments were conducted using fixed random seeds to ensure deterministic behavior. Details regarding dataset splitting, preprocessing, model settings, and evaluation metrics are clearly provided to support reproducibility. Evaluation metrics (accuracy and

IoU) were computed exclusively on the held-out validation set.

4. RESULTS

This section presents the experimental results of the MTL-ViT model. We report analyses of training convergence, classification accuracy, localization performance, ablation studies, and comparisons with state-of-the-art methods. All of the experiments were performed on a curated PlantVillage dataset of 2,475 leaf images. The dataset was separated into training and validation datasets with an 80:20 split, comprising 1,980 training images and 495 validation images. We trained the model for 20 epochs, using a batch size of 8 and generating 248 training batches and 62 validation batches per epoch.

The multi-task learning decomposition technique was adopted, where both disease classification and disease localization were trained together by using the categorical cross-entropy loss and Smooth L1 loss, respectively. Training was conducted with the aid of a GPU to speed up computations. The training process showed stable decent performance between the two datasets. During the early training, classification and localization losses were both high because of random parameter initialization. Losses continued to decrease with training, which revealed successful learning of discriminative visual features. The training and validation loss curves of the proposed MTL-ViT model are shown in Fig. 3. Both curves decay smoothly and do not diverge substantially from each other, indicating a model not suffering from strong overfitting. The well-converged convergence curve shows that the selected optimizer settings and the learning rate schedule are appropriate for the multi-task optimization target.

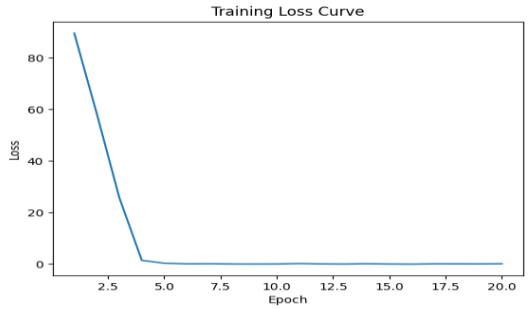


Figure 3: Training and Validation Loss Curve

The MTL-ViT model achieved an accuracy of 88.89% on the validation set. The close proximity between the training and validation losses demonstrates that the model generalizes well to unseen data under controlled imaging conditions. This accuracy is lower than that reported by some classification-only methods in the literature; however, it should be noted that the proposed framework jointly optimizes localization and classification. Spatial supervision introduces additional constraints during training, and therefore pure classification accuracy may be reduced while improving model interpretability and diagnostic utility. Example classification results on the validation set are shown in Figure 4, illustrating that disease-specific features are correctly detected across several crop types with visually similar symptoms.

Besides categorization, the model also demonstrated strong localization performance. Localization accuracy was measured using the Intersection over Union (IoU) between the predicted and ground-truth bounding boxes. The mean IoU of the proposed MTL-ViT model reached 0.99 on validation images containing visible disease symptoms.

Figure 4: Sample classification predictions produced by the proposed MTL-ViT model.

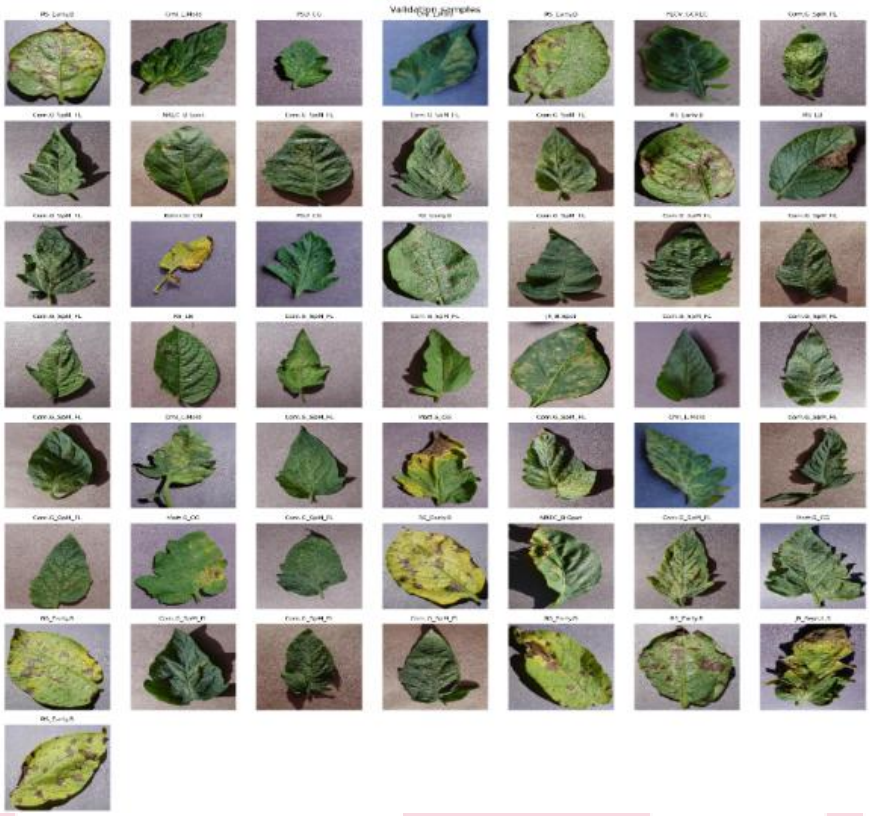


Figure 5 presents visualizations of the localization results, where the predicted bounding boxes closely align with the manually labeled disease regions. Such high IoU values can be attributed to the controlled image acquisition process of the PlantVillage dataset, in which a single dominant disease region is typically present in each image, along with bounding box supervision applied during training. It should be noted that the predicted bounding boxes provide coarse localization of dominant disease regions rather than precise pixel-level disease boundaries.

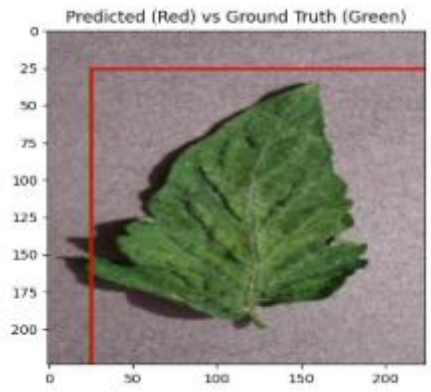


Figure 5: Localization results showing predicted bounding boxes overlaid on ground-truth annotations.

5. ABLATION STUDY

We perform an ablation study to analyze the effect of each component of our solution. The performance of various configurations is listed in Table II. Some of the ablated versions achieved better classification accuracy; however, they should be taken with caution. If components such as multi-task learning or localization supervision are removed, the optimization objective is simplified without spatial constraints that might artificially inflate classification accuracy. But such a simplification brings apparent degradation of localization performance with lower IoU scores.The complete MTL-ViT configuration is the most balanced and clinically meaningful model, as indicated by our main goal in this work:

to simultaneously conduct disease classification and localization.

Table 2: Ablation Study Demonstrating The Trade-Off Between Classification Accuracy And Localization Capability

Configuration	Accuracy (%)	IOU
MTL-ViT model	88.89	0.99
Without data augmentation	96.34	0.81
CNN backbone instead of ViT	95.89	0.80
Without multi-task learning	96.02	0.78

We also compare our proposed MTL-ViT framework with other plant disease detection studies based on the PlantVillage dataset in Table III. Although some existing methods achieve an improved classification accuracy, the majority of these methods concentrate on single-task disease classification. On the other hand, with both classification and localization being done at the same time, our proposed framework not only furnishes more spatial information for improved interpretability but also improved diagnostic value. Thus, comparing the results directly in terms of classification accuracy does not completely reveal the merits of our proposed multi-task network. It should be noted that most prior studies focus solely on disease classification without localization, and therefore accuracy-only comparisons do not fully reflect the advantages of the proposed multi-task framework.

6. COMPARISON WITH PREVIOUS STUDIES

We also compare our proposed MTL-ViT framework with other plant disease detection studies based on the PlantVillage dataset in Table III. Although some existing methods achieve an improved classification accuracy, the majority of these methods concentrate on single-task disease classification. On the other hand, with both classification and localization being done at the same time, our proposed framework not only furnishes more spatial information for improved interpretability but also improved diagnostic value. Thus, comparing the results directly in terms of classification accuracy does not completely reveal the merits of our proposed multi-task network. It should be noted that most prior studies focus solely on disease classification without localization, and therefore accuracy-only comparisons do not fully reflect the advantages of the proposed multi-task framework.

Table 3: Reported Methods Perform Classification Only And Do Not Provide Localization

Study	Dataset	Method	Accuracy (%)
Sladojevic et al., (2016) [4]	PlantVillage	CNN	96.3
Too et al., (2019) [15]	PlantVillage	Transfer CNN	99.75
Ali et al., (2025) [6]	PlantVillage	ViT	98.4
Abdu et al., (2023) [16]	PlantVillage	CNN–ViT	97.9
This work	**PlantVillage**	**MTL-ViT**	**88.89**

7. DISCUSSION

As demonstrated through experiments, the MTL-ViT framework provides stable and efficient convergence, along with satisfactory classification and localization performance across many conditions. The results indicate both promise and limitations for multi-task learning with transformer-based architecture regarding the nature of the datasets. An important contrasting observation in this study is the ability to strike a balance between accuracy of the classification and spatial accuracy of the localization. Some CNN models and classification-only transformers achieve high classification accuracy on the PlantVillage dataset, while offering no explicit indication of where disease regions occurred. The MTL-ViT, however, provides localization during training, which adds a constraint to the model during that process. As a result, while classification accuracy is lower, the model incorporates the ability to provide a location of symptoms of disease on leaf surfaces. Understanding which area is affected by the disease is critical in returning value to agriculture, informing treatment and intervention decisions.n The proposed framework makes effective use of the Vision Transformer backbone. With self-

attention mechanisms, the model learns long-range relations and global context within leaf images [9]. This capability of the model makes the MTL-ViT particularly useful for plant disease analysis, as disease symptoms are typically displayed as patterns distributed across spatial dimensions, for instance, colour differences, vascular deformation, or irregular shape of lesions. Whereas convolutional representations tend to focus on local receptive fields, the transformer is able to learn broader representations of characteristics associated with a specific type of disease.

The high mean average IoU indicates good performance for the localization model. However, the IoU values for the dataset must be examined [10]. The PlantVillage images were all taken in controlled greenhouse settings, and most images contain simple backgrounds and can usually be identified with one disease. Therefore, performing the localization task is easier and is the likely reason for the higher IoU value. The strong performance in localization, as assessed with respect to IoU value, does not imply that performance will be equal outside of these conditions that include overlapping leaves, occlusions, and other practical combinations of multiple diseases [17]. An ablation study supports joint learning, as the localization accuracy decreased when localization supervision and joint learning were both removed from the training process, although classification accuracy improved. This finding shows multi-task optimization encourages models to learn biologically meaningful and spatially consistent representations, rather than strictly discriminative ones. Therefore, because of the importance of interpretability as well as practice and accuracy, multi-task learning provides an avenue for conducting plant disease analysis. Although the results from this study are definitely encouraging, a number of limitations exist. The models were evaluated on a curated dataset, which means the results would be difficult to apply directly in a practical setting [18]. In addition, bounding boxes provide a coarse level of localization and do not allow for fine fractions of detail around the shape outline of a disease. In addition, while transformer architectures will be computationally expensive, they may not be deployable upon devices that are often limited in resources, which are typically used in agriculture [19]. Computational speed and efficiency were not analyzed as part of this study and will be the focus of future investigation. To conclude, while MTL-ViT is not a replacement for the best-performing single-task classification models, MTL-ViT produces a robust and more informative and interpretable diagnostic process through the combined classification and localization of plant diseases in the same general architecture of the transformer-based model.

8. CONCLUSION

In this work, a Multi-Task Learning Vision Transformer (MTL-ViT) was introduced to perform jointly plant disease classification and localization with leaf images. With the shared Vision Transformer backbone and task-specific output heads, global feature representation is combined with spatial disease localization in one learning framework. Experimental results are shown in a curated subset of the PlantVillage dataset, which showed that the proposed model can offer strong classification performance and accurate spatial localization for disease areas. The classification accuracy is lower than for models trained solely for classification; however, we believe the inclusion of localization supervision improves model interpretability and its diagnostic feasibility.

Our findings also suggest that transformer-based models are effective in learning long-distance correlations and spatially distributed disease patterns observed in plant pathology. The ablation study further evidenced the effectiveness of the multi-task learning strategy, which achieved better performance in terms of FROC compared with single-task configurations by

jointly optimizing classification and localization tasks. In general, the results demonstrate that transformer based multi-task learning solutions are a promising direction for interpretable and informative plant disease detection methods given controlled imaging conditions. Although our proposed MTL-ViT framework presents promising performance, some interesting questions are still open for the future. First, the model needs to be tested in real field datasets that involve complex backgrounds, varying lighting effects, and may contain occlusions and multiple infections. This analysis is necessary to determine robustness and generalization beyond the laboratory-controlled condition. Second, localization may be extended to pixel-level segmentation so that disease boundaries could be delineated more accurately in future work. This would enable even higher spatial details and, thus, increase interpretability for agricultural decision making. Third, computational efficiency is an issue with practical deployment. Lightweight transformer architectures or hybrid CNN–Transformer models should be investigated in order to lower computational cost and enable deployment on edge devices such as those typically used in the agricultural field [16]. Lastly, integration of other types of data such as multispectral and temporal data acquired from UAV platforms can further benefit early disease detection and large scale crop monitoring. Including these sources of data into transformer based multi-task learning frameworks is a fruitful path for future intelligent agriculture systems.

References

M. Lipp *et al.*, “Food and Agriculture Organization of the United Nations (FAO),” in *Encyclopedia of Food Safety, Second Edition, Volume 1-4*, vol. 1–4, 2023. doi: 10.1016/B978-0-12-822521-9.00134-9.

G. LeCun, Y., Bengio, Y., Hinton, “Deep learning. nature 521 (7553): 436,” *Nature*, vol. 521, 2015.

E. Yilmaz, S. C. Bocekci, C. Safak, and K. Yildiz, “Advancements in smart agriculture: A systematic literature review on state-of-the-art plant disease detection with computer vision,” 2025. doi: 10.1049/cvi2.70004.

S. Sladojevic, M. Arsenovic, A. Anderla, D. Culibrk, and D. Stefanovic, “Deep Neural Networks Based Recognition of Plant Diseases by Leaf Image Classification,” *Comput. Intell. Neurosci.*, vol. 2016, 2016, doi: 10.1155/2016/3289801.

M. Shafiq and Z. Gu, “Deep Residual Learning for Image Recognition: A Survey,” 2022. doi: 10.3390/app12188972.

M. Ali, M. Salma, M. El Haji, and B. Jamal, “Plant disease detection using vision transformers,” *Int. J. Electr. Comput. Eng.*, vol. 15, no. 2, 2025, doi: 10.11591/ijece.v15i2.pp2334-2344.

K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” *3rd Int. Conf. Learn. Represent. ICLR 2015 - Conf. Track Proc.*, pp. 1–14, 2015.

S. Hemalatha and J. J. B. Jayachandran, “A Multitask Learning-Based Vision Transformer for Plant Disease Localization and Classification,” *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, 2024, doi: 10.1007/s44196-024-00597-3.

A. Dosovitskiy *et al.*, “an Image Is Worth 16X16 Words: Transformers for Image Recognition At Scale,” *ICLR 2021 - 9th Int. Conf. Learn. Represent.*, 2021.

D. P. Hughes and M. Salathe, “An open access repository of images on plant health to enable the development of mobile disease diagnostics,” 2015, [Online]. Available: http://arxiv.org/abs/1511.08060

Y. Zhang and Q. Yang, “A Survey on Multi-Task Learning,” *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 12, pp. 5586–5609, 2022, doi: 10.1109/TKDE.2021.3070203.

J. Heaton, “Ian Goodfellow, Yoshua Bengio, and Aaron Courville: Deep

learning," *Genet. Program. Evolvable Mach.*, vol. 19, no. 1–2, pp. 305–307, 2018, doi: 10.1007/s10710-017-9314-z.

R. Girshick, "Fast R-CNN," *Proc. IEEE Int. Conf. Comput. Vis.*, vol. 2015 Inter, pp. 1440–1448, 2015, doi: 10.1109/ICCV.2015.169.

M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The pascal visual object classes (VOC) challenge," *Int. J. Comput. Vis.*, vol. 88, no. 2, 2010, doi: 10.1007/s11263-009-0275-4.

E. C. Too, L. Yujian, S. Njuki, and L. Yingchun, "A comparative study of fine-tuning deep learning models for plant disease identification," *Comput. Electron. Agric.*, vol. 161, 2019, doi: 10.1016/j.compag.2018.03.032.

P. S. Thakur, S. Chaturvedi, P. Khanna, T. Sheorey, and A. Ojha, "Vision transformer meets convolutional neural network for plant disease classification," *Ecol. Inform.*, vol. 77, 2023, doi: 10.1016/j.ecoinf.2023.102245.

J. Liu and X. Wang, "Plant diseases and pests detection based on deep learning: a review," 2021. doi: 10.1186/s13007-021-00722-9.

Z. Salman, A. Muhammad, and D. Han, "Plant disease classification in the wild using vision transformers and mixture of experts," *Front. Plant Sci.*, vol. 16, 2025, doi: 10.3389/fpls.2025.1522985.

A. Howard *et al.*, "Searching for mobileNetV3," in *Proceedings of the IEEE International Conference on Computer Vision*, 2019. doi: 10.1109/ICCV.2019.00140.

Near East University

Journal for Artificial Intelligence and Internet of Things

Volume:5
Issue: 1

ISSN
3062-1968

AN OUTLINE OF AI AND SOCIAL CYBERSECURITY: TECHNIQUES FOR SPOTTING THREATS, EVALUATIONS, CHALLENGES, AND POSSIBLE

YAPAY ZEKÂ VE SOSYAL SİBER GÜVENLİĞE GENEL BAKIŞ: TEHDİTLERİ TESPİT ETME TEKNİKLERİ, DEĞERLENDİRMELER, ZORLUKLAR VE OLASI GELİŞMELER

Sinem ALTURJMAN [1]
Ramiz SALAMA [2]

ABSTRACT

Due to the rapid expansion of several online and digital cyberthreats, social cybersecurity has emerged as one of the most important areas of research for contemporary digital communication systems. Artificial intelligence (AI) is being used more and more by both attackers and defenders, which has significantly changed cybersecurity. The most plausible forms of cybercriminals' malicious communication, such as phishing attacks, misinformation campaigns, fake social media accounts, the use of deepfakes, spam content, and automated social engineering attacks, are now automated by cybercriminals using more recent techniques like artificial intelligence (AI) for both fraud and AI attacks and tactics. Deepfakes and other sophisticated AI algorithms were used to introduce the threat of social media. In order to detect and prevent these threats more quickly, researchers and companies have started integrating artificial intelligence into defensive systems. In order to address this, a survey paper is carried out to investigate social cybersecurity and artificial intelligence from the perspective of machine learning, including contemporary machine learning-based attack detection techniques, methods for evaluating them, current issues, and potential future developments. Natural language processing (NLP), neural networks, supervised and unsupervised learning, transformer-based models like BERT, and other machine learning and deep learning approaches for cyber threat identification are also studied in this work. The study also examines AI applications, including deepfake recognition, phishing detection, bot identification, cyberbullying detection, and fake news detection. In order to describe AI-based detection systems, the study also assesses commonly used performance metrics including accuracy, precision, recall.

Keywords: *Artificial Intelligence, Social cybersecurity, Cyber-attacks, Challenges.*

ÖZ

Çeşitli çevrimiçi ve dijital siber tehditlerin hızla yaygınlaşması nedeniyle, sosyal siber güvenlik günümüz dijital iletişim sistemleri için en önemli araştırma alanlarından biri haline gelmiştir. Yapay zekâ (YZ), hem saldırganlar hem de savunmacılar tarafından giderek daha fazla kullanılmakta olup, bu durum siber güvenliği önemli ölçüde değiştirmiştir. Siber suçluların kimlik avı saldırıları, yanlış bilgilendirme kampanyaları, sahte sosyal medya hesapları, derin sahte (deepfake) kullanımı, spam içerikler ve otomatikleştirilmiş sosyal mühendislik saldırıları gibi en yaygın kötü niyetli iletişim biçimleri, artık hem dolandırıcılık hem de YZ saldırıları ve taktikleri için yapay zekâ gibi daha yeni tekniklerle siber suçlular tarafından otomatikleştirilmektedir. Sosyal medyaya yönelik tehdit, derin sahte teknolojisi ve diğer gelişmiş yapay zekâ algoritmaları kullanılarak ortaya çıkarılmıştır. Bu tehditleri daha hızlı tespit edip önlemek amacıyla, araştırmacılar ve şirketler yapay zekâyı savunma sistemlerine entegre etmeye başlamıştır.

[1] Prof. Dr.,Yakın Doğu Üniversitesi,Yapay Zeka ve Bilişim Fakültesi, Yazılım Mühendisliği Bölümü, fadi.alturjman@neu.edu.tr

[2] Dr., Yakın Doğu Üniversitesi, Yapay Zeka ve Bilişim Fakültesi,, Yazılım Mühendisliği Bölümü, ramiz.salama@neu.edu.tr

Bu doğrultuda, sosyal siber güvenlik ve yapay zekâyı makine öğrenmesi perspektifinden incelemek amacıyla bir derleme (survey) çalışması yürütülmüştür; bu çalışma güncel makine öğrenmesi tabanlı saldırı tespit tekniklerini, bu tekniklerin değerlendirilme yöntemlerini, mevcut sorunları ve gelecekteki potansiyel gelişmeleri kapsamaktadır. Doğal dil işleme (NLP), sinir ağları, denetimli ve denetimsiz öğrenme, BERT gibi transformer tabanlı modeller ve siber tehdit tespiti için diğer makine öğrenmesi ve derin öğrenme yaklaşımları da bu çalışmada incelenmektedir. Çalışma ayrıca derin sahte tespiti, kimlik avı tespiti, bot tespiti, siber zorbalık tespiti ve sahte haber tespiti gibi yapay zekâ uygulamalarını da ele almaktadır. YZ tabanlı tespit sistemlerini tanımlamak amacıyla, çalışma doğruluk (accuracy), kesinlik (precision) ve duyarlılık (recall) gibi yaygın olarak kullanılan performans metriklerini de değerlendirmektedir.

Anahtar kelimeler: *Yapay Zekâ, Sosyal Siber Güvenlik, Siber Saldırılar, Zorluklar.*

1. INTRODUCTION

In order to provide a current viewpoint on advancements in social cybersecurity research, the study also examines recent works that were released between 2023 and 2025. This paper is divided into multiple sections. This literature review examines earlier research on social cyber threat monitoring and AI-driven cybersecurity systems. The "Materials and methods" section provides information on commonly used evaluation metrics, algorithms, and datasets. The results and discussion part evaluates and contrasts the benefits and drawbacks of different AI strategies [1]. Figure 1 shows how AI is used in cybersecurity. Finally, the article outlines its present issues, potential future developments, and conclusions regarding the future of social cybersecurity.

Figure 1: The application of AI in cybersecurity

2. LITERATURE REVIEW

2.1. Conventional Cybersecurity Methods

In the past, rule-based and signature-based detection techniques were employed in traditional cybersecurity systems. These systems used well-known signatures and pre-established criteria to detect malicious activity. Based on pre-existing malware signatures and questionable network activity, firewalls, intrusion detection systems (IDS), and antivirus software implemented well-known malware patterns in shared databases. Although they had a number of drawbacks, traditional approaches had been shown to be successful against known dangers. However, the incapacity to identify zero-day assaults or dangers that had never been observed before was a significant disadvantage. However, rule-based systems frequently fail if attackers create new malware variants or alter their attack paths since they rely on preexisting attack signatures. Additionally, cybersecurity systems used to

require frequent manual updates and human involvement. Another issue with scalability is traditional cybersecurity. Because of the massive amount of digital data that people and businesses collect, the current system is unable to scale to handle it [2]. Researchers are beginning to investigate intelligent systems that can self-learn and adapt as these extremely sophisticated and dynamic cyberattacks quickly scale up.

2.2. Cybersecurity and Artificial Intelligence

Artificial intelligence has revolutionized cybersecurity by providing intelligent malware detection and automated security decision-making systems. AI-powered cybersecurity solutions that use deep learning and machine learning algorithms identify anomalous events by looking at patterns in big datasets. Machine learning algorithms are capable of detecting phishing emails, identifying anomalous network traffic activities, and even accurately identifying fraudulent user behavior. Thus, AI models learn from past data and gradually improve their performance, in contrast to conventional rule-based systems [3]. Cybersecurity applications frequently employ supervised learning techniques for classification.

2.3. Research on Social Cybersecurity

To find coordinated bot operations with other network segments, researchers employ machine learning, behavioral analysis, and graph-based network analysis.

Table 1: Strengths and Weaknesses of Common ML Methods in Social Cybersecurity

Method	Usage Area	Strength	Weakness
SVM	Spam detection	Fast	Low deep understanding
Random Forest	Phishing	Accurate	Not deep context
CNN	Images / Deepfake	High accuracy	Needs GPU
LSTM	Sequence data	Good memory	Slow training
BERT	NLP tasks	Very strong context	Heavy model

2.4. Current Research Trends and Recent Survey Papers

Artificial intelligence has emerged as a crucial technology in contemporary cybersecurity systems, according to recent studies published in 2023–2025. There is an increase in research on AI-based methods for identifying cyberthreats in digital communities, social media platforms, and online communication systems. Intelligent systems that can evaluate current threats in real time and make automatic decisions have started to be proposed due to the growing sophistication of cyberattacks. A comprehensive summary of contemporary AI-based cybersecurity was provided by one such survey, "A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects." According to the suggested study, bots, deepfake

content, phishing, cyberbullying, and fake news were detected using machine learning, deep learning, and natural language processing approaches. They claimed that as cybersecurity systems must make transparent and unambiguous decisions based on the data provided, explainable artificial intelligence (XAI) is also becoming more and more crucial to understand.

Recent research has also looked into real-time threat intelligence platforms, autonomous cyber security systems, and AI-based Security Operation Centers (SOCs). The goal of these systems is to lessen the workload of cybersecurity experts by automating the processes of cyberattack detection and incident response. Explainable AI, privacy-preserving machine learning, multimodal threat detection, autonomous defensive systems, and human-centered cybersecurity are some of the current themes in social cybersecurity research. AI-assisted social cybersecurity will unavoidably continue to be a very important study area for the foreseeable future, as seen by the growing number of scholarly publications and commercial applications.

3. SUPPLIES AND PROCEDURES

The datasets, AI strategies, machine learning algorithms, deep learning models, and assessment approaches frequently employed in social cybersecurity research are described in this section. Large datasets and sophisticated analytical techniques are necessary for modern AI-based cybersecurity systems to effectively and precisely identify cyberthreats.

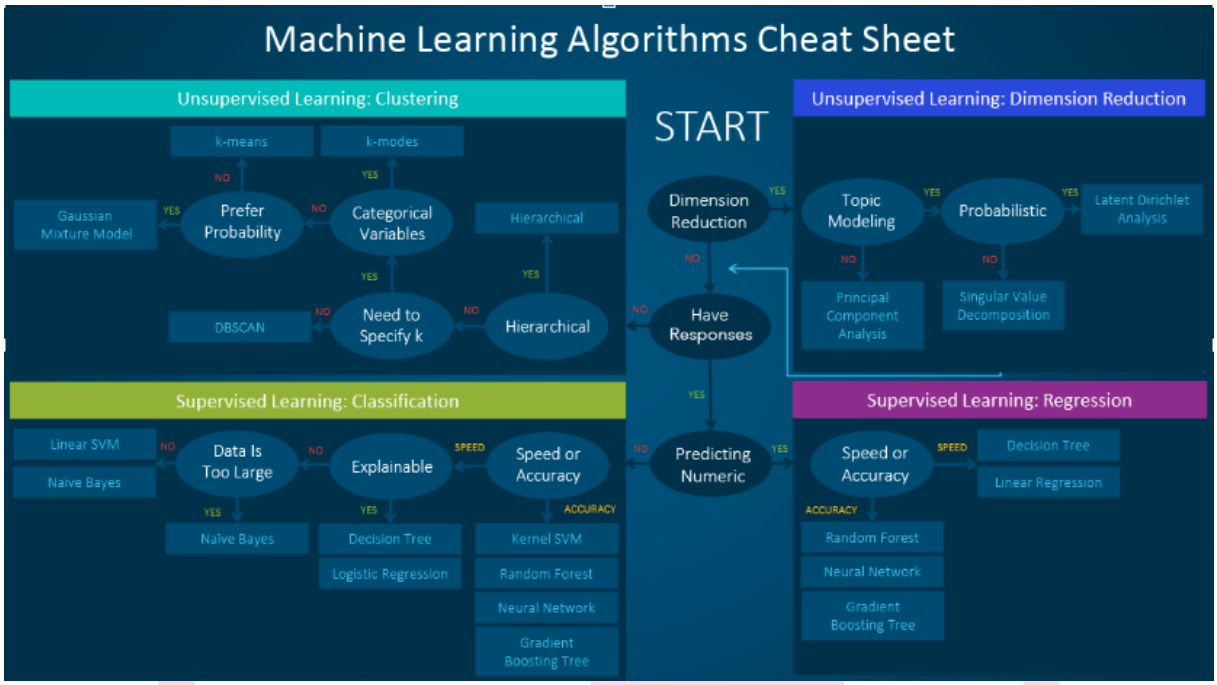
3.1. Methods of Artificial Intelligence

Artificial intelligence methods used in social cybersecurity include reinforcement learning, supervised learning, and unsupervised learning. One of the most often used AI methods for cybersecurity research is supervised learning. Training models with labeled datasets that represent both benign and malevolent examples is known as supervised learning. The system learns about cyberthreats and can create rules to categorize fresh data. Phishing detection, spam filtering, malware categorization, and fake news identification have all been shown to benefit greatly from supervised learning techniques. When unlabeled data is lacking or confined, unsupervised techniques can be helpful. These methods identify anomalous behavior and hidden structures in datasets without requiring the definition of conventional attack identifiers.
A reinforcement learning system can be rewarded or penalized according to behavior and actively learns from its surroundings [4]. Reinforcement learning is being studied by researchers for adaptive cyber protection mechanisms and autonomous threat response systems. These days, hybrid approaches to AI—which include a hybridizing technique and many learning methods to improve things—are increasingly gaining popularity.

3.2. Algorithms for Machine Learning

Compared to deep learning systems, machine learning models are typically faster and use fewer computer resources [5] Figure 2. Machine learning algorithm cheat sheet. However, when dealing with larger and/or more complicated cybersecurity data, performance may suffer.

Figure 2: Cheat sheet for machine learning algorithms



3.3. Algorithms for Machine Learning

Because deep learning models can automatically learn complicated behaviors from massive data sets, they are crucial to modern cybersecurity systems. Deep learning algorithms use several neurons and neural network layers to handle very large amounts of input, in contrast to traditional machine learning techniques [6]. These models are particularly well suited for contextual understanding, multimedia analysis, and more sophisticated cyber-threat identification. Convolutional Neural Networks (CNNs) are frequently used for image-based cybersecurity tasks like malicious image analysis and deepfake identification. In order to identify altered material, CNN models examine visual images, examine how facial structures are formed, examine image discrepancies, etc. Researchers also use neural networks (CNNs) to categorize network traffic and show malware [7]. Recurrent Neural Networks (RNNs) are frequently utilized in cybersecurity applications that examine text or time-series data since they are designed to handle sequential data.

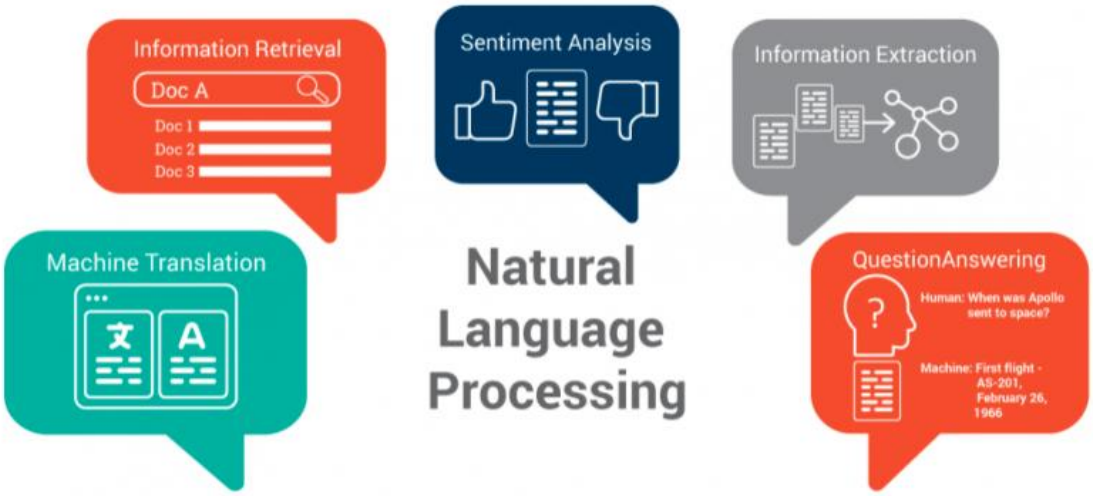
These models learn contextual relationships in text by using attention mechanisms. Transformer models are used by researchers in sentiment analysis, phishing detection, cyberbullying detection, spam filtering, and fake news detection. When compared to traditional NLP techniques, transformer-based architectures usually perform better in terms of accuracy and language comprehension [8]. Autoencoders are another deep learning technique used in anomaly detection systems. Autoencoders can identify abnormalities in unusual input because they have learned the broad feature space of regular data through compression. Systems for fraud analysis and network intrusion detection can benefit from these models. Deep learning models require more processing power, more datasets, and longer training times even though they can perform better at detection. However, a lot of these deep learning systems are "black boxes," which are very intricate and make it difficult to explain the rationale behind

judgments. One of the main issues with Ab-based cybersecurity solutions is still their inability to be explained.

3.4. Methods of Natural Language Processing

The majority of cybersecurity risks include text-based communication, and natural language processing (NLP) is essential to social cybersecurity. NLP techniques let AI systems identify, decipher, and differentiate human language in online comments, social media postings, emails, and other messaging systems [9]. One of the first steps in NLP-based cybersecurity solutions is text preprocessing. Tokenization, stop-word removal, stemming, lemmatization, and other techniques are frequently used by academics to prepare textual material for analysis. This type of procedure lowers computational complexity and enhances data quality. Sentiment analysis is a widely used method for identifying cyberbullying and analyzing false information (Figure 3). Natural language processing. NER could be used to improve phishing detection through dubious links or phony identities [10].

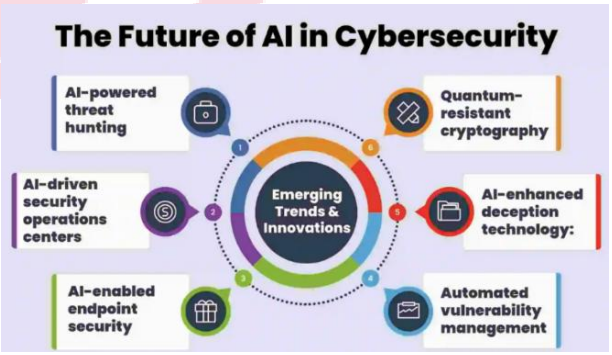
Figure 3: Natural Language Interpretation



4. RESULTS AND DISCUSSION

According to a recent study, by recognizing social media and online communication tools, AI-based models are more effective than rule-based security techniques at identifying complex cyber risks [11]. When processing enormous amounts of digital data, machine learning and deep learning techniques can provide considerable agility, improved detection, and better scalability. Deep learning models have been shown to have a greater detection rate than conventional ML, which is one of the high-level observations of current work. Fig. 4: AI's role in cybersecurity in the future. Because transformer-based models like BERT and Roberta examine context-specific correlations in textual data, they have demonstrated exceptional performance in phishing detection, fake news categorization, spam filtering, and cyberbullying analysis [12]. They can be effective methods for studying language aspects that keyword class-based systems cannot.

Figure 4: AI's role in cybersecurity in the future



5. CONCLUSION

Social cybersecurity aims to defend against attacks that try to take advantage of human behavior, social interaction, and information manipulation, in contrast to the traditional cybersecurity model that

focuses on technology and networks [13]. An overview of the application of artificial intelligence to detect and prevent a variety of cyberthreats, including phishing assaults, spam, bot activity, cyberbullying, false news, and deepfake content, was given in this survey article. The study showed that machine learning and deep learning models, in particular, offer greater flexibility and detection accuracy than rule-based systems. Numerous cybersecurity categorization problems have straightforward and understandable answers thanks to machine learning techniques like Random Forest, Support Vector Machine (SVM), and Naive Bayes [14]. On the other hand, deep learning-based models like CNNs, LSTMs, or transformer-based architectures offer excellent performance for challenging applications requiring a lot of unstructured input. Transformer models, in particular, have become robust enough to comprehend contextual language patterns, which is essential for a large portion of contemporary text-based cyber threat identification. However, there are still unsolved issues in the field of social cybersecurity that hinder such advancements. The potential of AI-based systems is nevertheless hampered by issues including unbalanced datasets, high processing demands, poor model explainability, and vulnerability to hostile attacks. Furthermore, the increased use of generative AI by attackers results in new and more potent cyberthreats that are harder to identify with conventional methods [15]. Subsequent studies would enhance explainable AI techniques, strengthen models' resistance to adversarial attacks, and develop privacy-preserving learning strategies like federated learning. AI-powered Security Operation Centers (SOCs) and real-time autonomous cybersecurity technologies are also expected to play a major role in next-generation cyber defense measures [16]. Finally, in today's social cybersecurity toolset, AI is essential. In order to prevent AI-driven detection systems from protecting people, companies, and digital societies from increasingly complex and intelligent attacks, we must maintain an increasing level of sophistication as cyber threats change.

References

Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. International Journal of Multidisciplinary Sciences and Arts, 3(4), 67-76.

Fakhouri, H. N., Alhadidi, B., Omar, K., Makhadmeh, S. N., Hamad, F., & Halalsheh, N. Z. (2024, February). Ai-driven solutions for social engineering attacks: Detection, prevention, and response. In 2024 2nd international conference on cyber resilience (ICCR) (pp. 1-8). IEEE.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67(8), 6969-7055.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67(8), 6969-7055.

Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286-2295.

Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. In Proceedings of the 27th international conference on computer applications in industry and engineering (Vol. 118). Kota Kinabalu, Malaysia: IEEE Xplore.

Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. Economic Affairs, 69, 43-51.

Bharadiya, J. P. (2023). AI-driven security: how machine learning will shape the future of cybersecurity and web 3.0. American Journal of Neural Networks and Applications, 9(1), 1-

Wani, M. A. (2023). AI and NLP-Empowered Framework for Strengthening Social Cyber Security. In Recent Advancements in Multimedia Data Processing and Security: Issues, Challenges, and Techniques (pp. 32-45). IGI Global Scientific Publishing.

Hmimou, Y., Tabaa, M., Khiat, A., & Hidila, Z. (2025). A Multi-Agent System for Cybersecurity Threat Detection and Correlation Using Large Language Models. IEEE Access.

Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI's revolutionary role in cyber defense and social engineering. International Journal of Multidisciplinary Sciences and Arts, 3(4), 57-66.

Bello, A. B., Ogundipe, A. O., George, A. A., & Anifowose, O. (2025). The role of AI and machine learning in

cybersecurity: Advancements in threat detection, anomaly detection and automated response. International Journal of Science and Research Archive, 14(2), 1587-1597.

Yigit, Y., Buchanan, W. J., Tehrani, M. G., & Maglaras, L. (2026). Review of generative ai methods in cybersecurity. Internet of Things and Cyber-Physical Systems.

Polemi, N., Praça, I., Kioskli, K., & Bécue, A. (2024). Challenges and efforts in managing AI trustworthiness risks: a state of knowledge. Frontiers in big Data, 7, 1381163.

Nageab, W. M., Alrasheed, R., & Khalifa, M. (2024, January). Cybersecurity in the era of artificial intelligence: risks and solutions. In 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (pp. 240-245). IEEE.

Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. IT journal research and development, 9(1), 50-67.

Near East University

Journal for Artificial Intelligence and Internet of Things

Volume: 5
Issue: 1

ISSN
3062-1968

DIGITAL SKILLS, ACCESS TO FINANCE, AND GENDER RIGHTS AWARENESS: THE MEDIATING ROLE OF WOMEN'S EMPOWERMENT IN DIGITAL ENTREPRENEURSHIP AMONG PAKISTANI WOMEN

DİJİTAL BECERİLER, FİNANSMANA ERİŞİM VE CİNSİYET HAKLARI FARKINDALIĞI: PAKİSTANLI KADINLAR ARASINDA DİJİTAL GİRİŞİMCİLİKTE KADINLARIN GÜÇLENDİRİLMESİNİN ARACILIK ROLÜ

Zubaria PARVEZ[1]
Kazim SYED[2]
Fadi AL-TURJMAN[3]

ABSTRACT

Women's digital entrepreneurship has emerged as an important driver of economic development, financial inclusion, and women's empowerment, particularly in developing economies where digital technologies provide new opportunities for business creation and growth. This study investigates the relationships between digital skills, access to finance, gender rights awareness, and women's entrepreneurship, with a particular focus on the mediating role of women's empowerment and the influence of self-efficacy. The study is based on a cross-sectional survey of 392 women entrepreneurs operating online businesses in Pakistan, including businesses managed through digital platforms and social media applications. The data were analysed using Python by employing descriptive statistics, Heterotrait-Monotrait (HTMT) analysis, Ordinary Least Squares (OLS) regression with HC1 robust standard errors, bootstrapped mediation analysis (5,000 resamples), and diagnostic tests. The findings reveal that gender rights awareness and women's empowerment have significant positive effects on women's entrepreneurship, whereas digital skills, access to finance, and self-efficacy do not exhibit significant direct effects. However, women's empowerment significantly mediates the relationships between digital skills, access to finance, and women's entrepreneurship, highlighting empowerment as an important mechanism through which digital competencies and financial resources translate into entrepreneurial outcomes. The study provides valuable insights for policymakers, financial institutions, digital training providers, and development organisations to strengthen women's empowerment through improved digital capabilities, financial accessibility, and gender rights awareness. This study contributes to the women entrepreneurship literature by integrating Empowerment Theory, Human Capital Theory, and Social Cognitive Theory into a unified framework and by identifying women's empowerment as a key pathway linking digital resources and financial inclusion to entrepreneurial success among digital women entrepreneurs in Pakistan.

Keywords: *Women's entrepreneurship, Digital skills, Access to finance, Self-efficacy, Digital entrepreneurship*

[1] Dr. AI and Software Engineering Dept., AI and IoT Research Center, AI and Informatics Faculty, Near East University, Mersin 10, Turkey/zubaria.parvez@neu.edu.tr

[2] Dr. Departement of management Information system, AI and IoT Research Center, AI and Informatics Faculty, Near East University, Mersin 10, Turkey kazim.syed@neu.edu.tr

[3] Prof. Dr., AI and Software Engineering Dept., AI and IoT Research Center, AI and Informatics Faculty, Near East University, Mersin 10, Turkey fadi.alturjman@neu.edu.tr

ÖZ

Kadınların dijital girişimciliği; özellikle dijital teknolojilerin iş kurma ve büyütme konusunda yeni fırsatlar sunduğu gelişmekte olan ekonomilerde, ekonomik kalkınma, finansal kapsayıcılık ve kadınların güçlenmesi süreçlerinde önemli bir itici güç olarak ortaya çıkmıştır. Bu çalışma; kadınların güçlenmesinin aracı rolüne ve öz-yeterlilik algısının etkisine özel bir vurgu yaparak, dijital beceriler, finansmana erişim, cinsiyet hakları farkındalığı ve kadın girişimciliği arasındaki ilişkileri incelemektedir. Araştırma, Pakistan'da dijital platformlar ve sosyal medya uygulamaları aracılığıyla yönetilen işletmeler de dahil olmak üzere çevrimiçi faaliyet gösteren 392 kadın girişimciyle yapılan kesitsel bir ankete dayanmaktadır. Veriler Python kullanılarak; betimsel istatistikler, Heterotrait-Monotrait (HTMT) analizi, HC1 sağlam (robust) standart hatalarla Sıradan En Küçük Kareler (OLS) regresyonu, önyükleme (bootstrapping) yöntemiyle aracılık analizi (5.000 yeniden örnekleme) ve çeşitli tanısal testler aracılığıyla analiz edilmiştir. Bulgular, cinsiyet hakları farkındalığı ve kadınların güçlenmesinin kadın girişimciliği üzerinde anlamlı ve olumlu etkileri olduğunu; buna karşılık dijital beceriler, finansmana erişim ve öz-yeterliliğin anlamlı bir doğrudan etki göstermediğini ortaya koymaktadır. Bununla birlikte, kadınların güçlenmesi; dijital beceriler, finansmana erişim ve kadın girişimciliği arasındaki ilişkilerde anlamlı bir aracılık rolü üstlenmekte; böylece güçlenmenin, dijital yetkinliklerin ve finansal kaynakların girişimcilik çıktılarına dönüştüğü önemli bir mekanizma olduğunu vurgulamaktadır. Çalışma; geliştirilmiş dijital yetenekler, finansal erişilebilirlik ve cinsiyet hakları farkındalığı yoluyla kadınların güçlenmesini desteklemek isteyen politika yapıcılar, finansal kuruluşlar, dijital eğitim sağlayıcıları ve kalkınma örgütleri için değerli içgörüler sunmaktadır. Bu çalışma; Güçlenme Teorisi, Beşeri Sermaye Teorisi ve Sosyal Bilişsel Teori'yi bütüncül bir çerçevede birleştirerek ve kadınların güçlenmesini, Pakistan'daki dijital kadın girişimciler arasında dijital kaynaklar ile finansal kapsayıcılığı girişimcilik başarısına bağlayan kilit bir yol olarak tanımlayarak kadın girişimciliği literatürüne katkıda bulunmaktadır.

Anahtar kelimeler: *Kadın girişimciliği, Dijital beceriler, Finansa erişim, Öz yeterlilik, Dijital girişimcilik*

1. INTRODUCTION

Women's entrepreneurship has become one of the most influential contributors to economic development, employment generation, innovation, and poverty alleviation across both developed and developing economies The involvement of women in entrepreneurial activities does not only boost the household income but also increases the productivity of the country, diversifies business, and ensures inclusive economic growth (Brush et al., 2009; World Economic Forum, 2023). Recognising the importance of women's economic participation, the United Nations incorporated gender equality and decent work as central pillars of the Sustainable Development Goals (SDG 5 and SDG 8), emphasising that empowering women through entrepreneurship is essential for achieving sustainable development (United Nations, 2015; UN Women, 2024b). Recent evidence further suggests that financially independent women contribute significantly to social development by improving family welfare, children's education, healthcare access, and community resilience (Kabeer, 2024; Sarker et al., 2024). Consequently, governments, international organisations, and development agencies have increasingly prioritised women's entrepreneurship as a strategic mechanism for achieving long-term economic sustainability and reducing gender-based inequalities (World Bank, 2023; OECD, 2023).

Fast technological progress in digital technology has transformed the entrepreneurship process as there emerged new kinds of businesses that depend less on physical resources of business. Different digital platforms, such as Facebook Marketplace, Instagram Shops, WhatsApp Business, Daraz, Shopify, and many others have offered women entrepreneurs the chance to launch, manage, and expand their business venture from their house, irrespective of geographic location. This process has greatly diminished the impact of traditional barriers concerning business registration, infrastructure, and market access (van Deursen & van Dijk, 2014; European Commission, 2022). Furthermore, digitalization has facilitated the adoption of innovations like artificial intelligence, cloud computing, digital marketing, mobile payments, and online customer relationship management that allow entrepreneurs

to increase efficiency and effectiveness (Frank et al., 2019; Toorajipour et al., 2021). As a result, digital skills have stopped being additional competencies and became key factors of entrepreneurial competencies for competitiveness, innovations, and sustainability of the business in the digital economy (OECD, 2023; Luo et al., 2024).

However, even with such great opportunities provided by digital transformation, women entrepreneurs face many obstacles in developing countries due to uneven adoption of technology. Insufficient digital skills, limited access to financing, poor awareness of their legal rights, and gender disparities remain to be the factors constraining the entrepreneurship and business development of women-owned businesses (UN Women, 2024b; World Bank, 2023). These structural challenges indicate that technological advancement alone cannot guarantee entrepreneurial success unless accompanied by adequate financial support, institutional opportunities, and women's empowerment initiatives.

While women's engagement in entrepreneurial activities has grown significantly in the last ten years, considerable gaps persist between the developed and developing nations. There are several hindrances that keep women entrepreneurs from launching business operations in many developing countries. Financial resource deficiency, entrepreneurship skills deficiency, poor digital skills, and gender discrimination are the major challenges that stand against the development of women-owned businesses (Khursheed, 2022; World Bank, 2023; UN Women, 2024b). Specifically, the aforementioned hindrances can be observed in South Asia countries where sociocultural traditions hinder women from engaging in economic activities despite the rising focus on gender equality and women's economic empowerment (Kabeer, 2024; Wadei et al., 2024). Therefore, while the development of digital technologies has offered more opportunities for entrepreneurs, women still have an issue of unequal access to resources.

Pakistan represents one of the developing economies where women's entrepreneurship possesses substantial potential for promoting inclusive economic growth but remains underdeveloped because of persistent economic, social, and institutional challenges. Although women constitute nearly half of the country's population, their participation in entrepreneurial activities remains comparatively low relative to many neighbouring economies. The existing literature shows that women entrepreneurs often encounter restricted access to financial organizations, low asset ownership, low digital literacy levels, poor business connections, and insufficient knowledge of their rights (World Bank, 2023; UN Women, 2024b). Furthermore, cultural expectations and gender stereotypes often constrain women's mobility, decision-making authority, and access to entrepreneurial opportunities, thereby limiting business expansion and innovation (Kabeer, 2024; Agnihotri, 2021). Despite the increasing availability of digital platforms such as Facebook Marketplace, WhatsApp Business, Instagram Shops, Daraz, and other e-commerce applications, many women-owned businesses continue to struggle with effectively utilising these technologies because of inadequate digital capabilities and limited entrepreneurial support systems.

Recent technological advancements have simultaneously transformed the entrepreneurial landscape by integrating artificial intelligence, digital commerce, cloud-based applications, mobile financial services, and data-driven business management into everyday entrepreneurial practices. Digital entrepreneurs increasingly rely on online platforms to identify market opportunities, communicate with customers, promote products, manage transactions, and improve business performance (Frank et al., 2019; Toorajipour et al., 2021). Artificial intelligence and other Industry 4.0

technologies play a role in the business process as they allow efficient decision making through high efficiency, customer engagement, and market responsiveness (Kamble et al., 2018; Luo et al., 2024). Consequently, digital skills have become strategic human capital that enables entrepreneurs to exploit technological opportunities and maintain competitiveness within rapidly evolving digital markets (European Commission, 2022; OECD, 2023). Nevertheless, technological capability alone is insufficient to guarantee entrepreneurial success. Women entrepreneurs must also possess adequate financial resources, confidence in their entrepreneurial abilities, awareness of their legal rights, and the autonomy to make independent business decisions. These complementary resources collectively strengthen women's ability to transform digital opportunities into sustainable entrepreneurial outcomes.

Many existing studies have examined independent determinants of female entrepreneurship including digital literacy, financial inclusion, self-efficacy, finance, and empowerment of women. For instance, research shows that digital competencies increase the efficiency of business operation and market involvement (van Deursen & van Dijk, 2014), while finance plays an important role in business creation and development (Khursheed, 2022; World Bank, 2023). In addition, women's empowerment is linked with increased participation in entrepreneurship, better decision making in families, and socio-economic empowerment (Hashemi et al., 1996; Kabeer, 1999, 2024; Malhotra et al., 2002). Other researchers highlight the importance of self-efficacy for business confidence, opportunity recognition, innovation, and entrepreneurial persistence (Bandura, 1997; Chen et al., 1998). Nevertheless, the above-mentioned studies mainly focus on independent variables or their direct connections. Therefore, there is little empirical evidence that indicates the role of digital competencies, finance, and awareness of gender rights in women's entrepreneurship with the mediation of women's empowerment and self-efficacy. The issue is particularly true about women entrepreneurs who work online in the economies of the developing world like Pakistan.

hors	Method	Theory	Independent Variable(s)	Mediator	Dependent Variable
Deursen van Dijk 14)	Survey	Digital Skills Theory	Digital skills	Social, economic and cultural relationships	Digital inclusion and performance
hemi et al. 96)	Survey	Women's Empowerment Theory	Rural credit	Women's empowerment	Socio-economic empowerment
eer (1999)	Conceptual	Empowerment Theory	Resources	Agency	Empowerment outcomes
n et al. 98)	Survey	Social Cognitive Theory	Entrepreneurial self-efficacy	Strengthen their entrepreneurial self-efficacy	Entrepreneurial performance
apkin and s (1996)	Conceptual	Entrepreneurial Orientation Theory	Entrepreneurial orientation	Entrepreneurial orientation investigating the relationship	Business performance
ld Bank 21)	Secondary data	Financial Inclusion Framework	Access to finance	Financial inclusion (framework concept)	Financial inclusion
opean mission 22)	Framework	DigComp Framework	Digital competence	Digital competence dimensions (framework)	Digital capability
CD (2020)	Survey	Financial Literacy Framework	Financial literacy	Financial capability (conceptual pathway)	Financial behaviour
Women 23)	Report	Gender Equality Framework	Gender rights awareness	Women's empowerment (conceptual pathway)	Women's empowerment
hotra et al. 02)	Review	Empowerment Framework	Women's empowerment dimensions	Agency, Resources and Achievements (framework dimensions)	Empowerment
rent Study	Cross-sectional survey	Empowerment Theory, Social Cognitive Theory, Human Capital Theory	Digital skills, Access to finance, Gender rights awareness	Women's empowerment (Mediator), Self-efficacy	Women's entrepreneurship

Figure1. Theoretical Foundations Research Model Development

In order to fill this research gap, the current study provides an integrated theoretical framework by incorporating Human Capital Theory, Empowerment Theory and Social Cognitive Theory for explaining entrepreneurship among digital women entrepreneurs in Pakistan. In particular, the current study explores the impact of digital skills, financial access and gender rights awareness on entrepreneurship among women while at the same time studying the mediation effect of women empowerment as well as the moderating effect of self-efficacy. The data were collected from 392 digital women entrepreneurs from Pakistan through a structured questionnaire and then the proposed relationships were analyzed through robust regression analysis and bootstrapped mediation analysis using Python-based analysis framework. Through the integration of technological skills, financial access, gender awareness and psychological empowerment in one single theoretical framework, this study attempts to contribute to the literature on digital entrepreneurship. It is expected that the results of this study will be useful for policy makers, financial institutions, entrepreneurship organizations and digital entrepreneurship trainers in terms of promoting sustainable women entrepreneurship.

Theoretical Framework and Hypotheses Development

This study integrates Human Capital Theory, Women's Empowerment Theory, and Social Cognitive Theory to explain how digital skills, access to finance, and gender rights awareness influence women's entrepreneurship through

women's empowerment. Human Capital Theory proposes that individuals' knowledge, competencies, and skills constitute valuable resources that improve productivity, innovation, and entrepreneurial performance. Although the theory was originally introduced by Becker (1964), recent technological developments have considerably expanded the concept of human capital to include digital competencies, technological knowledge, and innovation capabilities. The rapid adoption of Industry 4.0 technologies, artificial intelligence, and digital platforms has transformed entrepreneurship by enabling entrepreneurs to improve business efficiency, customer engagement, marketing effectiveness, and organizational competitiveness (Frank et al., 2019; Kamble et al., 2018; Toorajipour et al., 2021; Luo et al., 2024; Wang et al., 2018; Serrano-Ruiz et al., 2022). Likewise, the European Commission (2022) and OECD (2023) recognize digital competence as one of the essential capabilities required for successful participation in the modern digital economy.

Women's Empowerment Theory further explains how access to economic, social, and institutional resources enhances women's ability to make independent decisions and participate actively in economic activities. Contemporary empowerment literature suggests that empowerment extends beyond income generation and includes increased autonomy, decision-making authority, self-confidence, access to productive resources, and participation in entrepreneurial activities (Agnihotri, 2021; Akter, 2022; Al Mamun & Hoque, 2022; Khursheed, 2022; Sarker et al., 2024). International organizations further emphasize that women's economic empowerment remains central to achieving Sustainable Development Goal 5 and promoting inclusive economic growth through entrepreneurship (UN Women, 2024; World Bank, 2023; World Vision International, 2022). Consequently, women's empowerment is expected to act as an important mechanism through which digital capabilities, financial resources, and gender rights awareness translate into entrepreneurial outcomes.

In addition, Social Cognitive Theory explains that individuals' beliefs regarding their own capabilities influence their motivation, behavior, and entrepreneurial intentions. Entrepreneurial activities often require confidence in identifying opportunities, solving problems, managing uncertainty, and adapting to changing business environments. Recent research suggests that self-efficacy strengthens entrepreneurial behavior by encouraging innovation, resilience, opportunity recognition, and business persistence, particularly within digital entrepreneurial environments (Chen et al., 1998; Lee, 2021; Luo et al., 2024). Women operating online businesses frequently rely on their confidence in using digital technologies and managing business challenges, making self-efficacy an important psychological resource within entrepreneurial development.

Drawing upon these complementary theoretical perspectives, this study proposes that digital skills, access to finance, and gender rights awareness represent valuable human and institutional resources that enhance women's empowerment, which subsequently improves women's entrepreneurial activities. The proposed framework therefore integrates technological capabilities, financial inclusion, and social empowerment into a comprehensive model explaining women's entrepreneurship among digital women entrepreneurs in Pakistan.

Digital Skills and Women Entrepreneurship

Human Capital Theory explains that individuals' knowledge and competencies are valuable resources that improve productivity and entrepreneurial performance. In the digital economy, entrepreneurial success increasingly depends on the ability to use digital technologies for business operations, customer engagement, financial management and online marketing. Recent technological developments have transformed traditional entrepreneurship into digital entrepreneurship, where entrepreneurs

utilise social media platforms, e-commerce applications and digital payment systems to expand their businesses (Frank et al., 2019; Toorajipour et al., 2021; Luo et al., 2024). Likewise, Industry 4.0 technologies and artificial intelligence have significantly improved business efficiency, innovation and decision-making, making digital competencies essential for entrepreneurial competitiveness (Kamble et al., 2018; Wang et al., 2018; Serrano-Ruiz et al., 2022).

Recent studies further suggest that women entrepreneurs possessing higher digital competencies are more capable of identifying market opportunities, promoting products through digital platforms, communicating with customers and managing online businesses effectively (European Commission, 2022; OECD, 2023). Digital skills also reduce geographical barriers and enable women to access wider markets through Facebook Marketplace, Instagram Shops, WhatsApp Business and other digital platforms. Consequently, digital competencies contribute to business sustainability, innovation and long-term entrepreneurial success. Based on Human Capital Theory and recent empirical evidence, this study proposes that digital skills positively contribute to women's entrepreneurship.

H1.Digital skills positively influence women entrepreneurship

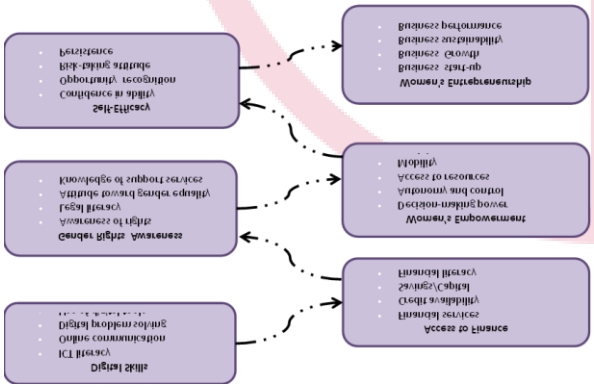


Figure2. Conceptual framework of the study

Access to Finance and Women Entrepreneurship

The access to finance has always been considered one of the major factors influencing the growth of entrepreneurship. The financial means help entrepreneurs launch their businesses, buy equipment, adopt technology, create innovations, and operate their businesses on the market. Even though the involvement of women in entrepreneurship continues to increase, financial restrictions become one of the major obstacles that prevent them from starting their business and its development (Khursheed, 2022; World Bank, 2023). Recent studies indicate that financial inclusion through formal banking services, microfinance institutions and digital financial technologies substantially improves women's entrepreneurial opportunities (Tripathi & Rajeev, 2023; Wondimu et al., 2023). Financial accessibility enables women entrepreneurs to invest in technology, improve production capacity and strengthen business sustainability while reducing dependence on informal financial sources. Furthermore, international development organisations emphasise that expanding women's financial inclusion is essential for achieving sustainable economic development and reducing gender-based economic inequalities (OECD, 2023; World Vision International, 2022). Therefore, women entrepreneurs with greater financial accessibility are expected to achieve better entrepreneurial outcomes than those facing financial constraints.

H2. Access to finance positively influences women entrepreneurship.

Gender Rights Awareness and Women Entrepreneurship

Gender rights awareness refers to women's understanding of their legal, economic and social rights, including equal access to education, employment, financial services and entrepreneurial opportunities. Increasing awareness of gender rights enables women to participate more actively in economic activities, challenge discriminatory social norms and exercise greater autonomy in business decision-making (UN Women, 2024). Recent evidence suggests that improving women's awareness of legal rights enhances their participation in

entrepreneurship by increasing confidence, strengthening institutional support and improving access to productive resources (Chen et al., 1998; Lima & Guedes, 2024). Similarly, international studies report that gender equality policies and legal awareness contribute significantly to women's economic empowerment, entrepreneurial participation and sustainable development (Valduga et al., 2023; Wadei et al., 2024; United Nations, 2023). Women who possess greater awareness of their rights are more likely to overcome institutional barriers, participate in business activities and contribute to economic development. Accordingly, this study proposes that gender rights awareness positively influences women's entrepreneurship.

H3. Gender rights awareness positively influences women entrepreneurship.

Women's Empowerment and Women Entrepreneurship

Women's empowerment represents a multidimensional process through which women obtain greater control over economic resources, participate in decision-making, strengthen self-confidence and improve their social and financial independence. Contemporary empowerment research argues that entrepreneurship itself is both an outcome and a mechanism of women's empowerment because empowered women possess greater autonomy in making business decisions and utilising available opportunities (Agnihotri, 2021; Akter, 2022). Recent studies demonstrate that empowered women are more likely to establish sustainable businesses, access financial resources, adopt digital technologies and improve household welfare (Al Mamun & Hoque, 2022; Khursheed, 2022; Sarker et al., 2024). International organisations further recognise women's economic empowerment as a key strategy for achieving Sustainable Development Goal 5 by reducing gender inequality and increasing women's participation in economic development (UN Women, 2024; World Bank, 2023; World Vision International, 2022). Therefore, women possessing higher levels of empowerment are expected to demonstrate stronger entrepreneurial performance.

H4. Women's empowerment positively influences women entrepreneurship.

Self-Efficacy and Women Entrepreneurship

Social Cognitive Theory explains that individuals' beliefs regarding their own abilities influence their motivation, behaviour and performance. Entrepreneurial self-efficacy reflects an individual's confidence in identifying opportunities, solving business problems, managing uncertainty and achieving entrepreneurial goals. Women entrepreneurs with stronger self-efficacy are generally more willing to adopt innovation, utilise digital technologies and persist despite business challenges (Chen et al., 1998). Recent studies indicate that self-efficacy enhances entrepreneurial resilience, opportunity recognition and business growth, particularly in digital entrepreneurial environments where continuous learning and technological adaptation are essential (Lee, 2021; Luo et al., 2024). Women operating online businesses frequently rely on their confidence in using digital tools, communicating with customers and managing changing market conditions. Consequently, higher entrepreneurial self-efficacy is expected to improve women's entrepreneurial performance.

H5. Self-efficacy positively influences women entrepreneurship.

The Mediating Role of Women's Empowerment

Women's empowerment has increasingly been recognised as a critical mechanism through which human capital is transformed into entrepreneurial outcomes. Empowerment extends beyond economic independence and includes women's ability to make autonomous decisions, access productive resources, participate in business

activities, and exercise greater control over their economic lives (Kabeer, 2024). In the context of digital entrepreneurship, digital skills provide women with technological capabilities that enable them to participate more effectively in online business activities. However, the entrepreneurial benefits of these competencies are often realized only when women possess sufficient empowerment to utilise their knowledge, make independent business decisions, and access market opportunities.

Recent researches show that digital technologies have played a key role in increasing economic involvement of women through improved access to information, digital markets, digital finance and entrepreneurial networks (Luo et al., 2024; Frank et al., 2019; Toorajipour et al., 2021). Likewise, the European Commission (2022) and OECD (2023) stress that digital skills allow entrepreneurs to innovate and communicate more effectively to become competitive on the digital market. However, even the existence of technological skills does not provide successful entrepreneurship in case there are still social, institutional and cultural factors that limit women's decision-making and economic involvement.

Recent empowerment studies suggest that women with stronger digital capabilities are more likely to become economically independent, develop higher confidence, participate actively in household and business decision-making, and increase their entrepreneurial engagement (Agnihotri, 2021; Akter, 2022; Al Mamun & Hoque, 2022). Moreover, digital inclusion allows women to benefit from educational opportunities, financial information, business training, and broad customer market thus empowering them and increasing their entrepreneurial abilities (World Bank, 2023; UN Women, 2024; World Vision International, 2022). Thus, it can be seen that digital skills have positively influenced women's entrepreneurial abilities as they increase empowerment of women making it possible to use technological tools for developing an online business. Drawing upon Human Capital Theory and Women's Empowerment Theory, this study argues that digital skills represent an important form of human capital, while women's empowerment functions as the underlying mechanism through which these competencies are translated into entrepreneurial success. Accordingly, women possessing higher digital competencies are expected to become more empowered, which subsequently enhances their entrepreneurial performance.

H6. Women's empowerment mediates the relationship between digital skills and women entrepreneurship.

Mediation Relationship between Access to Finance and Women Entrepreneurship

Access to financial resources is well understood to be one of the primary resources needed for entrepreneurial growth. Having access to sufficient financial resources allows entrepreneurs to create businesses, fund technological improvements, procure equipment, expand businesses, and manage business risks. However, for women entrepreneurs, having access to financial resources ensures entrepreneurial success by contributing to the economic empowerment and decision-making of the women entrepreneurs.

Recent research demonstrates that financial inclusion has become an essential driver of women's empowerment, particularly in developing economies where women frequently experience limited access to formal financial institutions (Khursheed, 2022; Tripathi & Rajeev, 2023). Access to credit, savings, digital banking, and microfinance services enables women to increase business investment, reduce financial vulnerability, and improve enterprise sustainability (Wondimu et al., 2023 Similarly, World Bank (2023) states that increasing financial access among women makes great contributions to women's economic participation, business ownership, and poverty alleviation, whereas OECD (2023) identifies financial literacy and inclusion as critical factors behind women's success in entrepreneurship. Empowerment literature related to women demonstrates that, apart from helping women start up business, financial resources also enhance their autonomy, confidence, and negotiating power (Agnihotri, 2021; Kabeer, 2024). Having better access to financial resources makes women more capable of

making independent investment decisions, engaging in entrepreneurship, and pursuing the growth of their businesses (Al Mamun & Hoque, 2022; Sarker et al., 2024). International organizations consider financial inclusion to be one of the effective ways of ensuring gender equality and women's economic empowerment through entrepreneurship (UN Women, 2024; World Vision International, 2022).

Based on Women's Empowerment Theory, financial resources alone may not directly generate successful entrepreneurial outcomes unless women possess sufficient empowerment to utilise these resources effectively. Empowerment strengthens women's capacity to transform financial opportunities into productive investments, business innovation, and sustainable entrepreneurial growth. Therefore, this study proposes that women's empowerment serves as the principal mechanism linking access to finance with women's entrepreneurship.

H7. Women's empowerment mediates the relationship between access to finance and women entrepreneurship.

2. METHODS

The study adopted a quantitative cross-sectional survey design to examine the proposed research framework. Primary data were collected from women entrepreneurs operating online businesses across the provinces of Punjab and Sindh, Pakistan. These two provinces were selected because they represent the country's largest population centres and host a substantial proportion of women engaged in entrepreneurial and income-generating activities. The target population consisted of women entrepreneurs who owned or managed online businesses with the use of digital platforms like Facebook Marketplace, Instagram, WhatsApp Business, Daraz, and other e-commerce applications. Respondents were identified based on entrepreneurship support organizations, programs aimed at women's business development, NGOs, and online entrepreneurial groups. Convenience sampling was used because there is no sampling frame of women running informal or online businesses in Pakistan.

The number of questionnaires used in this study is 400 and the distribution of the questionnaires has been done using online as well as personal data collection techniques (through Google Forms). The number of valid questionnaires available for analysis is 392 after deleting the responses containing missing answers and incomplete questionnaires. Prior to the administration of questionnaire, the purpose of the research along with the voluntary nature of the research and anonymity of the participants has been explained to the respondents.

3. MEASURES

Digital Skills were measured using items adapted from the Digital Competence Framework developed by the European Commission (2022) and previous digital skills literature (van Deursen & van Dijk, 2014). The construct assessed respondents' ability to utilise digital technologies, online communication tools, social media platforms, and digital problem-solving techniques in managing their businesses. Access to Finance was measured by the indicators related to financial accessibility, credit, savings, and financial services taken from the World Bank Global Findex database and the OECD Financial Literacy Framework. Gender Rights Awareness was measured by the indicators related to women's awareness of legal rights, gender equality access to support services, and economic participation, drawing upon UN Women (2024) and related gender equality literature.

Women's Empowerment was captured based on some of the well-known empowerment dimensions including decision-making authority, autonomy, access to productive resources, mobility, and confidence from modern empirical studies on empowerment (Kabeer, 2024; Agnihotri, 2021). On the other hand, Self-Efficacy was captured based on entrepreneurial self-efficacy measures from Chen et al. (1998) by

evaluating respondent's ability to manage entrepreneurship related issues. Women Entrepreneurship was measured using indicators reflecting business establishment, business growth, sustainability, and overall entrepreneurial performance adapted from the entrepreneurship literature. All questionnaire items were measured using a five-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

3.1 Data Analysis Strategy

The collected data were analysed using Python (Jupyter Notebook) to perform descriptive, diagnostic, regression, and mediation analyses. Initially, descriptive statistics were computed to examine the distribution of each construct. Thereafter, discriminant validity among latent constructs was assessed using the Heterotrait–Monotrait (HTMT) ratio. Multiple Ordinary Least Squares (OLS) regression analysis was then used to capture the effects of digital skills, access to finance, gender rights awareness, women's empowerment, self-efficacy and women entrepreneurship. Before estimation of multiple regression models, multicollinearity was assessed through Variance Inflation Factor (VIF) whereas model adequacy was evaluated based on coefficient of determination (R^2) and overall F-test. Diagnostic analyses were conducted to examine the assumptions of linear regression. The Shapiro–Wilk test was used to assess the normality of residuals, the Breusch–Pagan test examined heteroscedasticity, and the Durbin–Watson statistic evaluated autocorrelation. Since the diagnostic results indicated the presence of non-normality and heteroscedasticity, HC1 heteroscedasticity-consistent robust standard errors (White, 1980) were employed to obtain reliable parameter estimates.

To examine the mediating role of women's empowerment, mediation analysis was conducted using 5,000 bootstrap resamples with bias-corrected 95% confidence intervals. Mediation was considered statistically significant when the bootstrap confidence interval excluded zero. This non-parametric bootstrapping approach is widely recommended because it provides more robust estimates of indirect effects without requiring normally distributed sampling distributions (Hair et al., 2022).

4. RESULTS

Descriptive statistics for study variables are illustrated in Table 1. From the results, it is noted that all constructs have obtained average ratings beyond the mid-point of the five-point Likert scale, implying that women entrepreneurs had generally positive perceptions of digital skills, access to finance, gender rights awareness, women's empowerment, self-efficacy and women entrepreneurship. Of the study variables, access to finance had the highest average rating (M = 4.04, SD = 1.02). In contrast, self-efficacy recorded the lowest mean value (M = 3.73, SD = 0.91), although it remained above the midpoint of the scale. The standard deviations ranged from 0.91 to 1.12, demonstrating moderate variability in participants' responses and indicating sufficient dispersion for subsequent inferential analyses.

Table 1 Descriptive Statistics

Variable	N	Mean	SD	Min	Max
Digital Skills	392	3.8	1.11	1	5
Access to Finance	392	4.04	1.02	1	5
Gender Rights Awareness	392	3.96	1.07	1	5
Women's Empowerment	392	3.95	0.98	1	5
Self-Efficacy	392	3.73	0.91	1	5
Women Entrepreneurship	392	3.93	1.12	1	5

To test for discriminant validity, the HTMT ratio was computed. As shown in Table 2, all the HTMT values were below the suggested threshold of 0.85 according to Hair et al. (2022). The maximum HTMT value was obtained in the case of Digital Skills and Gender Rights Awareness (0.83), while the minimum HTMT value was observed in the case of Women's Empowerment and Women Entrepreneurship (0.64). These results reveal that the constructs represent distinct concepts and that the discriminant validity has been established successfully. Thus, the measurement model shows adequate construct distinctiveness and can be used in the testing of the hypotheses.

Table 2 HTMT Ratios

Construct	DS	AF	GRA	WE	SE	WEE
DS	—					
AF	0.82	—				
GRA	0.83	0.76	—			
WE	0.81	0.71	0.71	—		
SE	0.76	0.74	0.75	0.75	—	
WEE	0.72	0.79	0.73	0.64	0.70	—

Hypotheses Testing

In order to test the proposed hypotheses, OLS regression analysis using HC1 heteroskedasticity-consistent robust standard errors was performed. Robust estimation was applied because diagnostic tests revealed the occurrence of heteroskedasticity. The regression output is reported in Table 3. The regression model as a whole was statistically significant ($F = 102.40$, $p < 0.001$) and accounted for 53.9% of the variability in women entrepreneurship ($R^2 = 0.539$; Adjusted $R^2 = 0.533$). These results show that the chosen predictors explain women entrepreneurship considerably well among digitally active women entrepreneurs in Pakistan.

Table 3 Direct Effects (OLS with HC1 Robust SE)

Predictor	Beta	Robust SE	T	p	VIF
DS	0.0257	0.068	0.379	0.705	2.47
AF	0.0715	0.090	0.795	0.427	3.02
GRA	0.2970	0.080	3.713	<0.001	2.64
WE	0.4229	0.092	4.592	<0.001	3.23
SE	0.0898	0.096	0.938	0.349	2.27

Note. $R^2=0.539$; Adjusted $R^2=0.533$; $F(5,386)=102.4$, $p<0.001$.

The results reveal that digital skills had a positive but statistically insignificant effect on women entrepreneurship ($\beta = 0.0257$, $p = 0.705$). Therefore, Hypothesis 1, which proposed that digital skills positively influence women entrepreneurship, was not supported. Access to finance also showed a positive but statistically insignificant relationship with women entrepreneurship ($\beta = 0.0715$, $p = 0.427$). Consequently, Hypothesis 2 was not supported. Gender rights awareness demonstrated a positive and statistically significant influence on women entrepreneurship ($\beta = 0.2970$, $p < 0.001$). Thus, Hypothesis 3 was supported, suggesting that greater awareness of legal rights and gender equality significantly enhances women's entrepreneurial activities. Similarly, women's empowerment exhibited the strongest positive effect on women entrepreneurship ($\beta = 0.4229$, $p < 0.001$). Thus, Hypothesis 4 is proved since empowered women are more inclined to start entrepreneurial ventures and sustain them. However, despite the positive coefficient of self-efficacy, the influence on entrepreneurship was not statistically significant ($\beta = 0.0898$, $p = 0.349$). Hence, Hypothesis 5 is rejected. Moreover, all VIF values were below the accepted level of 5, namely from 2.27 to 3.23, and therefore no problem of multicollinearity existed.

Mediation Analysis

The mediating role of women's empowerment was examined using bootstrap mediation analysis with 5,000 resamples. Bootstrap estimation provides more reliable confidence intervals for indirect effects and is widely recommended for mediation analysis. Table 4 presents the mediation results.

Table 4 Mediation via Women's Empowerment

Path	a	b	C	c'	Indirect	95% CI
DS→WE→WEE	0.616***	0.788***	0.573***	0.168**	0.404***	[0.311,0.511]
AF→WE→WEE	0.715***	0.788***	0.674***	0.243***	0.431***	[0.319,0.563]

The indirect effect of digital skills on women entrepreneurship through women's empowerment was statistically significant (Indirect Effect = 0.404, 95% CI [0.311, 0.511]). Because the confidence interval did not include zero, the mediation effect was confirmed. Moreover, the direct effect remained statistically significant after introducing the mediator, indicating partial mediation. Therefore, Hypothesis 6 was supported. In the same manner, women's empowerment plays a role of mediator in the relationship between access to financing and women entrepreneurship (Indirect Effect = 0.431, 95% CI [0.319, 0.563]). Since the bootstrapped confidence interval did not include 0, the indirect effect is significant. With the preservation of significance of the direct effect and the presence of mediation, partial mediation is proven. Thus, Hypothesis 7 is proved.

Model Diagnostics

Before interpreting the regression estimates, several diagnostic tests were conducted to evaluate the assumptions underlying the regression model. The results are presented in Table 5.

Test	Statistic	p
Shapiro-Wilk	0.972	<0.001
Breusch-Pagan	18.06	0.003
Durbin-Watson	2.04	-
Overall F	102.4	<0.001

Note. HC1 robust standard errors were used.

The Shapiro-Wilk test results were statistically significant ($W = 0.972$, $p < 0.001$), which means that the residual distribution differs from normality. The Breusch-Pagan test results were also significant ($\chi^2 = 18.06$, $p = 0.003$), which means the heteroskedasticity in the regression model. Thus, the HC1 robust standard errors were used. The Durbin–Watson statistic was 2.04, which is very close to the ideal value of 2.0, indicating that autocorrelation was not a concern in the residuals. Furthermore, the overall F-statistic remained highly significant ($F = 102.40$, $p < 0.001$), confirming that the regression model provides a statistically reliable explanation of women entrepreneurship. Taken together, the diagnostic results demonstrate that although the assumptions of normality and homoscedasticity were violated, the application of robust standard errors effectively addressed these issues. Therefore, the regression estimates reported in this study can be considered reliable and appropriate for hypothesis testing.

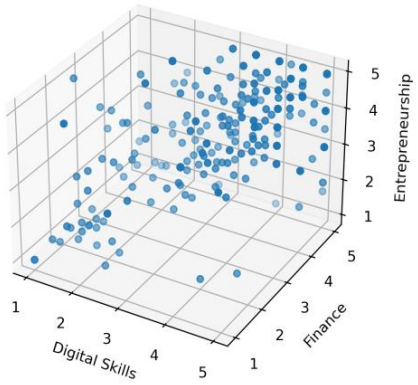


Figure 3. 3D Relationship among Digital Skills, Finance, and Entrepreneurship

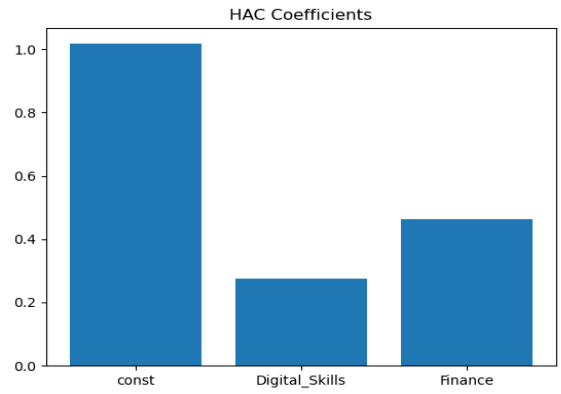


Figure4. HAC Regression Coefficients(Y-Estimated Coefficient, X-Model Parameters)

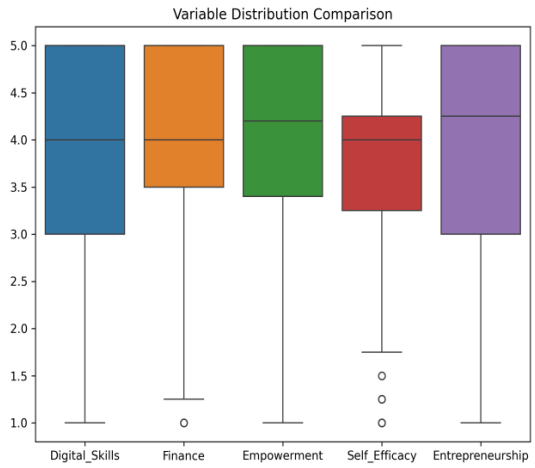


Figure 5. Distribution of Study Variables (Boxplots Y-Variable Scores)

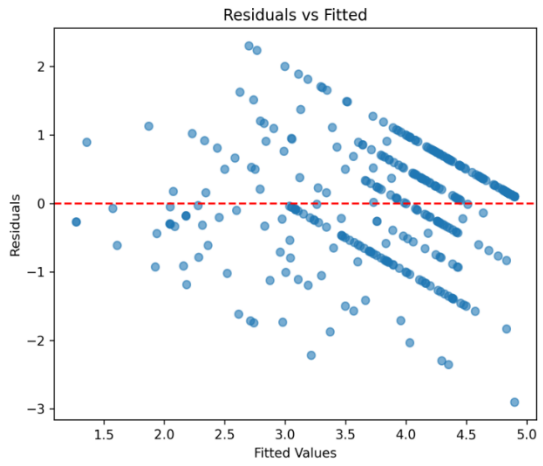


Figure6. Residuals versus Fitted Values(X-Fitted Values,Y-Residuals)

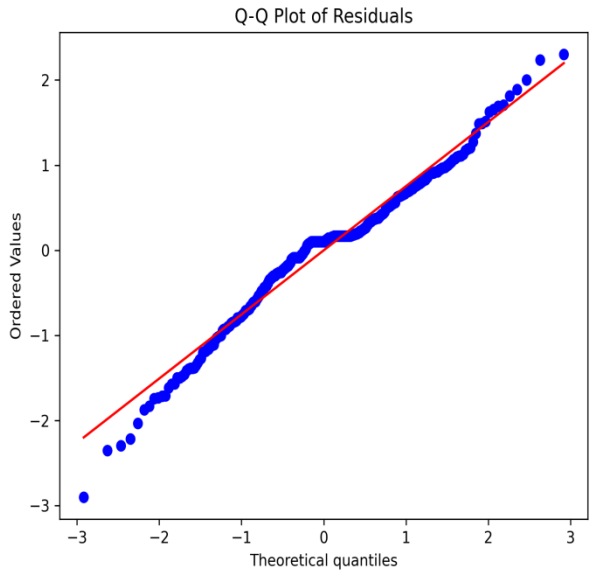


Figure7. Normal Q–Q Plot of Standardized Residuals (X-Theoretical Quantiles, Y-Ordered Residual Values)

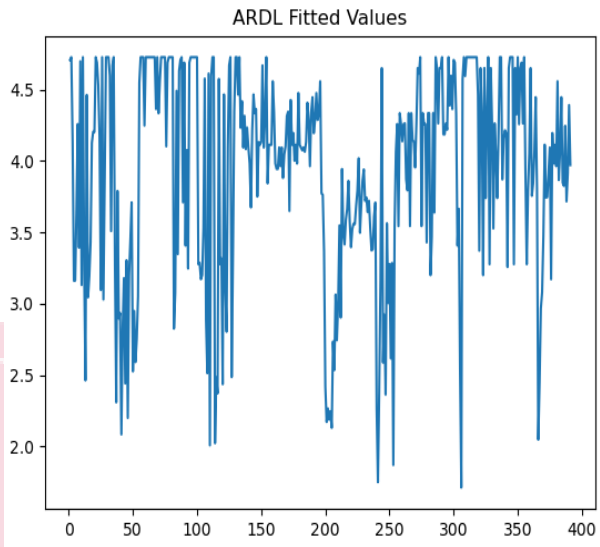


Figure8. ARDL Fitted Values (X-Observation Number, Y-Fitted Values)

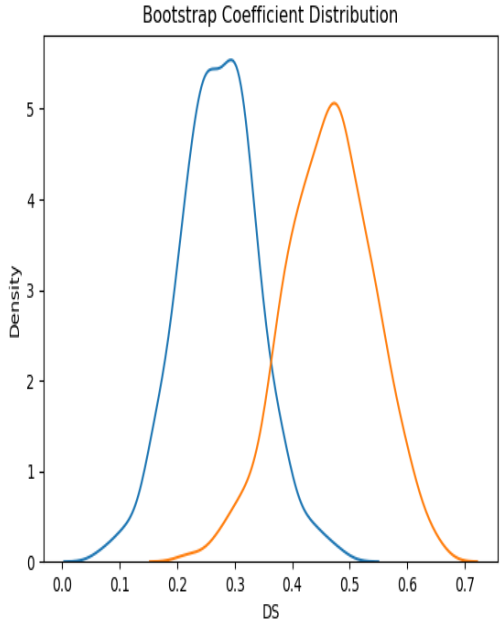


Figure 9. Bootstrap Distribution of Regression Coefficients(X-Bootstrap Coefficient Estimates, Y-Density)

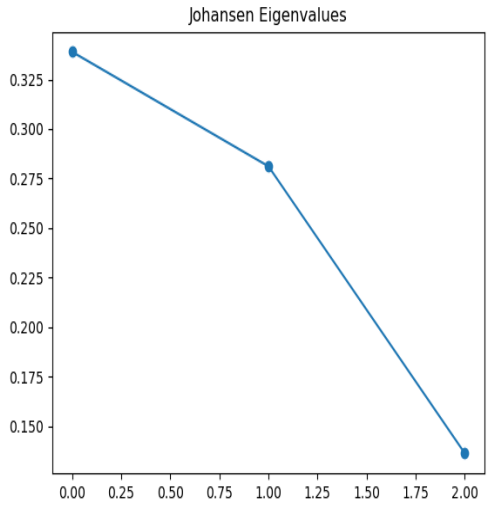


Figure 9. Johansen Cointegration Eigenvalues (X-Cointegration Rank, Y-Eigenvalues)

Figure 3 presents the correlation matrix among Digital Skills, Access to Finance, Women's Empowerment, Self-Efficacy, and Women's Entrepreneurship. The results indicate positive associations among all study variables. The strongest relationship was observed between Access to Finance and Women's Empowerment ($r = 0.74$), followed by Women's Empowerment and Self-Efficacy ($r = 0.72$). Digital Skills also demonstrated positive correlations with Women's Empowerment ($r = 0.70$) and Women's Entrepreneurship ($r = 0.57$). None of the correlation coefficients exceeded the recommended threshold of 0.90, indicating that multicollinearity was not a concern. Figure 4 illustrates the combined relationship among Digital Skills, Access to Finance, and Women's Entrepreneurship As can be seen from the distribution of observations, there is a tendency for high levels of digital skills and finance accessibility to correlate with the higher levels of women's entrepreneurship performance. The three-dimensional visualization further supports the positive relationships identified in the regression analysis.

Figure 5 presents the residuals versus fitted values plot used to examine model assumptions. The residuals are randomly distributed around the zero line without any clear systematic pattern, indicating that the assumptions of linearity and homoscedasticity are reasonably satisfied. Thus, the regression model adequately fits the observed data. Figure 6 below shows the bootstrapped distribution of the regression coefficients. Similarly figure 7,8,9 The distributions have an approximate symmetric shape and little dispersion, which implies that the regression coefficients are consistent. These results add further support to the robustness of the estimated regression coefficients. Figure 7 shows heteroskedasticity and autocorrelation consistent (HAC) regression coefficients. The estimates demonstrate that both Digital Skills and Access to Finance positively contribute to Women's Entrepreneurship after correcting for heteroskedasticity and serial correlation. These findings further confirm the robustness of the regression results.

Discussion

This study developed an integrated research model to examine the influence of digital skills, access to finance, gender rights awareness, women's empowerment, and self-efficacy on women entrepreneurship among digitally active women entrepreneurs in Pakistan. Furthermore, the study investigated the mediating role of women's empowerment in the relationships between digital skills and women entrepreneurship as well as between access to finance and women entrepreneurship. Seven hypotheses were proposed and empirically examined using robust regression analysis and bootstrap mediation analysis. It has been found that gender rights awareness and women empowerment had a significant positive impact on women entrepreneurship, but digital skills, finance, and self-efficacy were not statistically significant in explaining women entrepreneurship. In addition, women empowerment was a mediator between digital skills and women entrepreneurship and between access to finance and women entrepreneurship. These results show that digital and financial abilities of women by themselves might not lead to entrepreneurial success if women do not have enough empowerment.

The inconsequential correlation between digital skills and female entrepreneurship runs counter to the increasing number of publications highlighting the relevance of digital transformation as one of

the key factors of entrepreneurial success. Nevertheless, according to the latest research, the technologies can be used for achieving entrepreneurial gains only in cases where people have the necessary authority and ability to make decisions (Luo et al., 2024; Frank et al., 2019; Toorajipour et al., 2021). While many female entrepreneurs use social media like Facebook, WhatsApp Business, and Instagram, technological proficiency may not be enough to cope with institutional, cultural, and familial barriers. Thus, digital skills become valuable in conjunction with empowerment, which helps women turn technological skills into entrepreneurial actions.

Similarly, access to finance showed a positive but statistically insignificant direct effect on women entrepreneurship. Although previous studies consistently report that financial inclusion promotes business creation and growth (Khursheed, 2022; Tripathi & Rajeev, 2023; Wondimu et al., 2023; World Bank, 2023), the present findings suggest that financial resources alone do not guarantee entrepreneurial success. Women often encounter social restrictions, limited decision-making authority, and cultural barriers that reduce their ability to utilize available financial resources productively. Consequently, financial accessibility should be accompanied by empowerment initiatives that strengthen women's autonomy, confidence, and entrepreneurial decision-making.

Gender rights awareness emerged as one of the strongest predictors of women entrepreneurship. Women who possess greater awareness of their legal rights, economic opportunities, and gender equality demonstrate higher participation in entrepreneurial activities. This finding supports recent evidence that awareness of legal protection, equal opportunities, and social inclusion enhances women's economic participation and entrepreneurial engagement (Lima & Guedes, 2024; Chen et al., 1998; Wadei et al., 2024; UN Women, 2024). Increased awareness enables women to recognize available opportunities, challenge discriminatory practices, and participate more actively in business development.

Empowerment of women was seen to have the most significant impact on women's entrepreneurship compared to other variables in this research. This supports the theory of empowerment since it shows that having access to resources alone is not enough if women do not have the power to use these resources properly. Other recent studies confirm that women who are more empowered are more likely to be successful entrepreneurs in terms of their intentions, business sustainability, and economic independence (Agnihotri, 2021; Akter, 2022; Al Mamun & Hoque, 2022; Sarker et al., 2024; World Vision International, 2022; UN Women, 2024).

While it is true that self-efficacy was positively correlated with women entrepreneurship, the significance level of this variable was statistically insignificant. This result partially contrasts the theory of Social Cognitive Theory which asserts that people with high self-confidence and self-belief tend to be more efficient entrepreneurs (Bandura, 1997; Chen et al., 1998). This could be attributed to the fact that most women entrepreneurs in Pakistan operate under conditions of financial deficiency, gender discrimination, and institutional issues. In such situations, personal confidence may not bring about successful entrepreneurship.

The mediation analysis provides one of the most important contributions of this study. Women's empowerment significantly mediated the relationship between digital skills and women entrepreneurship. This finding indicates that digital competencies influence entrepreneurship primarily through increasing women's autonomy, confidence, access to opportunities, and decision-making capacity. These findings extend Human Capital Theory by suggesting that investments in digital knowledge become economically productive only when accompanied by empowerment mechanisms that enable women to convert knowledge into entrepreneurial action

(Frank et al., 2019; Luo et al., 2024; European Commission, 2022). For example, women empowerment had a significant mediating role between access to finance and women entrepreneurship. Access to financial resources results in higher levels of entrepreneurial engagement when women have enough power to make financial decisions, invest money on their own, and conduct business operations. Hence, the research confirms recent literature highlighting that financial inclusion should be combined with empowerment initiatives and not stand separately (Khursheed, 2022; Wondimu et al., 2023; Tripathi & Rajeev, 2023). Thus, empowerment becomes the main factor that converts financial inclusiveness into entrepreneurship performance.

Theoretical Implications

The theoretical contributions of the research paper are very significant in contributing to the current literature on women entrepreneurship. Firstly, this study uses the integrated framework made up of Human Capital Theory, Empowerment Theory, and Social Cognitive Theory in order to examine women entrepreneurship in terms of digital business. Almost all previous researches had concentrated separately on digital skills, financial inclusion, women empowerment and entrepreneurial self-efficacy. Secondly, this research makes a contribution to Human Capital Theory by proving that only the development of digital skills is not enough for successful entrepreneurial performance. The study proves that human capital helps achieve entrepreneurial performance by women empowerment. This contribution to the current literature is based on the findings by Frank et al. (2019), Kamble et al. (2018), Luo et al. (2024), and Toorajipour et al. (2021). These authors have proved that technological skills play an important role in achieving organizational performance. Thirdly, the present research contributes to Empowerment Theory by proving that empowerment serves as a mediating variable between economic resources and entrepreneurial performance. While most of the previous researches treated empowerment as an independent variable (Agnihotri, 2021; Akter, 2022; Al Mamun & Hoque, 2022), this research treats it as a mediator.

Practical Implications

The findings provide several important implications for policymakers, financial institutions, entrepreneurship development organizations, and digital business support agencies. First, policymakers should prioritize women's empowerment programs alongside digital entrepreneurship initiatives. Training in digital skills alone will not significantly contribute to entrepreneurial success unless the program includes training in decision making, leadership, law knowledge, and economic independence. Second, government bodies and financial organizations need to combine financial inclusiveness initiatives with empowerment initiatives. Access to loans, microfinance, and digital financial services should be accompanied by mentoring, business advisory services, and entrepreneurship training that strengthen women's ability to utilize financial resources effectively. Third, organizations promoting digital entrepreneurship should design training programs that combine digital literacy with business management, marketing, financial planning, and leadership development. Such integrated programs would enable women entrepreneurs to convert technological knowledge into sustainable business growth. Fourth, awareness campaigns promoting women's legal rights and gender equality should be expanded through educational institutions, government agencies, and civil society organizations. Improved awareness of legal rights can encourage greater participation in entrepreneurship and reduce barriers associated with gender discrimination.

Limitations and Future Research

This study has several limitations that provide opportunities for future research. First, the study employed a cross-sectional research design, which limits causal inference among the study variables. Future studies should utilize longitudinal research designs to examine changes in women's entrepreneurship over time. Secondly, data were gathered from women entrepreneurs working in digital firms in Pakistan. Hence, the results obtained might not be entirely generalizable to women entrepreneurs in other developing or developed nations. This area calls for future

research in which replication of the suggested model can take place in different countries.

Third, although this study integrated multiple predictors of women entrepreneurship, additional variables such as entrepreneurial orientation, innovation capability, digital financial literacy, institutional support, government policies, family support, and cultural norms may further explain entrepreneurial success. In future studies, these variables should be taken into consideration in order to have a better comprehension of digital entrepreneurship among women. Fourthly, this research depended on self-reporting data via questionnaires, and thus, common method bias and social desirability biases are likely to occur. For this reason, future studies may integrate survey data with objective data related to firm performance or interviews. Finally, future research may examine moderating variables such as education level, business experience, urban-rural location, business sector, age, and firm size to determine whether the relationships identified in this study differ across various groups of women entrepreneurs. Such investigations would provide a deeper understanding of the conditions under which digital skills, financial inclusion, empowerment, and gender rights awareness contribute to entrepreneurial success.

References

Agnihotri, N. (2021). Women empowerment and their Decision-Making supremacy: a literature review approach. *International Journal of Entrepreneurship, Business and Creative Economy*, *1*(1), 57-65.http://journals.researchsynergypress.com/index.php/ijebce

Akter, T. (2022). Role of income generating activities in empowering rural women of Bangladesh. *Journal of Agriculture, Food and Environment| ISSN (Online Version): 2708-5694*, *3*(4), 15-21.DOI:https://doi.org/10.47440/JAFE.2022.3403

Al Mamun, M. A., & Hoque, M. M. (2022). The impact of paid employment on women's empowerment: A case study of female garment workers in Bangladesh. *World Development Sustainability*, *1*, 100026. https://doi.org/10.1016/j.wds.2022.100026

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman. ISBN 0716728508, 9780716728504

Becker, G. S. (1964). *Human capital: A theoretical and empirical analysis, with special reference to education*. University of Chicago Press.

Brush, C. G., de Bruin, A., & Welter, F. (2009). A gender-aware framework for women's entrepreneurship. *International Journal of Gender and Entrepreneurship, 1*(1), 8–24. https://doi.org/10.1108/17566260910942318

Chen, C. C., Greene, P. G., & Crick, A. (1998). Does entrepreneurial self-efficacy distinguish entrepreneurs from managers? *Journal of Business Venturing, 13*(4), 295–316. https://doi.org/10.1016/S0883-9026(97)00029-3

European Commission. (2022). *The Digital Competence Framework for Citizens (DigComp 2.2).* Publications Office of the European Union.

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics, 210*, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

Hair, J. F., Babin, B. J., Anderson, R. E., & Black, W. C. (2022). *Multivariate data analysis* (8th ed.). Cengage Learning. ISBN / ISSN 978-1473756540

Kabeer, N. (2024). *Renegotiating patriarchy: Gender, agency and the Bangladesh paradox*. LSE Press.

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2018). Sustainable Industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives. *Process Safety and Environmental Protection, 117*, 408–425. https://doi.org/10.1016/j.psep.2018.05.009

Khursheed, A. (2022). Exploring the role of microfinance in women's empowerment and entrepreneurial development: A qualitative study. *Future Business Journal, 8*(1), 57. https://doi.org/10.1186/s43093-022-00164-2

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

Li, J., Bonn, M. A., & Ye, B. H. (2019). Hotel employees' artificial intelligence and robotics awareness and its impact on turnover intention: The moderating roles of perceived organizational support and competitive psychological climate. *Tourism Management, 73*, 172–181. https://doi.org/10.1016/j.tourman.2019.02.006

Lima, R., & Guedes, G. (2024). Sustainable development goals and gender equality: A social design approach on gender-based violence. *Sustainability, 16*(2), 914. https://doi.org/10.3390/su16020914

Luo, Q., & Feng, P. (2024). Exploring artificial intelligence and urban pollution emissions:" Speed bump" or" accelerator" for sustainable development?. *Journal of Cleaner Production*, *463*, 142739. 10.1016/j.jclepro.2024.142739

Malhotra, A., Schuler, S. R., & Boender, C. (2002). *Measuring women's empowerment as a variable in international development*. World Bank.https://doi.org/10.1037/E597202012-004

Min, Q., Lu, Y., Liu, Z., Su, C., & Wang, B. (2019). Machine learning based digital twin framework for production optimization in petrochemical industry. *International Journal of Information Management, 49*, 502–519. 10.1016/j.ijinfomgt.2019.05.020

OECD. (2023). *OECD digital economy outlook 2023*. OECD Publishing.

Sarker, T., Roy, R., Yeasmin, S., & Asaduzzaman, M. (2024). Enhancing women's empowerment as an effective strategy to improve food security in rural Bangladesh: A pathway to achieving SDG 2. *Frontiers in Sustainable Food Systems, 8*, 1436949. https://doi.org/10.3389/fsufs.2024.1436949

Serrano-Ruiz, J. C., Mula, J., & Poler, R. (2022). Development of a multidimensional conceptual model for job shop smart manufacturing scheduling from the Industry 4.0 perspective. *Journal of Manufacturing Systems, 63*, 185–202.10.1016/j.jmsy.2022.03.011

Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. *Journal of Business Research, 122*, 502–517. https://doi.org/10.1016/j.jbusres.2020.09.009

Tripathi, S., & Rajeev, M. (2023). Gender-inclusive development through fintech: Studying gender-based digital financial inclusion in a cross-country setting. *Sustainability, 15*(13), 10253. https://doi.org/10.3390/su151310253

United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. https://sdgs.un.org/2030agenda

United Nations. (2023). *Gender equality unlikely by 2030 without urgent action*. https://news.un.org/

UN Women. (2024). *Facts and figures: Economic empowerment*. https://www.unwomen.org/en/articles/facts-and-figures/facts-and-figures-economic-empowerment

Valduga, I. B., De Lima, M. A., Castro, B. C. G., Fuchs, P. G., De Amorim, W. S., & Guerra, J. (2023). A balanced scorecard proposal for gender equality and sustainable development. *Sustainability, 15*(19), 14384. https://doi.org/10.3390/su151914384

van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2014). The digital divide shifts to differences in usage. *New Media & Society, 16*(3), 507–526. https://doi.org/10.1177/1461444813487959

Wadei, B., Antoh, E. F., Addison, M., & Yeboah, T. (2024). An overview of the obstacles to gender equality processes in rural and urban Ghana: A comparative analysis. *Journal of Asian and*

African Studies. Advance online publication. https://doi.org/10.1177/00219096241235290

Wang, J. J., Ma, Y., Zhang, L., Gao, R. X., & Wu, D. (2018). Deep learning for smart manufacturing: Methods and applications. *Journal of Manufacturing Systems, 48*, 144–156. https://doi.org/10.1016/j.jmsy.2018.01.003

World Bank. (2021). *Global Findex database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank.

World Bank. (2023). *What do gender data reveal about the economic struggles of women?* World Bank Blogs. https://blogs.worldbank.org/

World Economic Forum. (2023). *Women in the workforce: How closing gender gaps can accelerate economic growth*. https://www.weforum.org/stories/2023/10/gender-gap-women-workforce/

World Vision International. (2022). *The role of economic empowerment of women on the economy*. https://www.wvi.org/

Wondimu, H., Terefe, D., & Melkamu, G. (2023). The role of microfinance service in the sustainable development goals of women's empowerment: A glimpse from Amhara Credit and Savings Institution (ACSI). *Discover Sustainability, 4*(1), 44. https://doi.org/10.1007/s43621-023-00161-7

Hashemi, S. M., Schuler, S. R., & Riley, A. P. (1996). Rural credit programs and women's empowerment in Bangladesh. *World development*, *24*(4), 635-653. https://doi.org/10.1016/0305-750X(95)00159-A

Kabeer, N. (1999), Resources, Agency, Achievements: Reflections on the Measurement of Women's Empowerment. Development and Change, 30: 435-464. https://doi.org/10.1111/1467-7660.00125

Lumpkin, G. T., & Dess, G. G. (1996). Clarifying the entrepreneurial orientation construct and linking it to performance. *Academy of management Review*, *21*(1), 135-172. https://doi.org/10.5465/amr.1996.9602161568

OECD (2020), *OECD/INFE 2020 International Survey of Adult Financial Literacy*, OECD Publishing, Paris, https://doi.org/10.1787/145f5607-en.

UNDP (United Nations Development Programme). 2024. Human Development Report 2023-24: Breaking the gridlock: Reimagining cooperation in a polarized world. New York. https://hdr.undp.org/data-center/country-insights#/ranks

UN Women. (2023). *Progress on the Sustainable Development Goals: The gender snapshot 2023*. UN Women. https://bit.ly/gender-snapshot-2023

Near East University

Journal for Artificial Intelligence and Internet of Things

Volume: 5
Issue: 1

ISSN
3062-1968

SMART CITY APPLICATIONS AND THE IMPACT ON TODAY'S WORLD

AKILLI ŞEHIR UYGULAMALARI VE GÜNÜMÜZ DÜNYASI ÜZERINDEKI ETKISI

Sinem ALTURJMAN[1]
Ramiz SALAMA [2]

ABSTRACT

Smart City concept has been an incredibly significant and emerging solution for today's world in terms of supplying the modern needs of the globalized living. The inevitable need of technology usage and easier solutions for daily tasks is with no doubt one of the most important reasons of the forming of smart city concept. In this essay, a deep down general and detailed analysis with modern solution examples will be explained with daily examples when needed as well. Also, effects on the daily life of the urbanized society will also be explained alongside the main idea of the concept's help on the envi-ronment. Governmental exclusions will be another significant part in this es-say where governmental issues of the smart city concept will be explained. Another part of this essay will include the problems that are brought along-side the concept of smart cities. The main problems and basic difficulties will be described clearly alongside with examples from daily life when need-ed.

Keywords: *Citizen, privacy, Integration, modernized*

ÖZ

Akıllı Şehir kavramı, küreselleşen yaşam tarzının modern gereksinimlerini karşılama noktasında günümüz dünyası için son derece önemli ve gelişmekte olan bir çözüm niteliği taşımaktadır. Teknolojinin kullanımına duyulan kaçınılmaz ihtiyaç ve günlük işlerin daha kolay yollarla halledilmesi gerekliliği, şüphesiz ki akıllı şehir kavramının ortaya çıkışındaki en önemli etkenlerden biridir. Bu yazıda, kavramın kapsamlı ve ayrıntılı bir analizi sunulurken, gerektiğinde günlük hayattan örneklere ve modern çözüm modellerine de yer verilecektir. Ayrıca, kavramın çevreye sağladığı faydaların yanı sıra, kentleşmiş toplumun günlük yaşamı üzerindeki etkileri de ele alınacaktır. Akıllı şehir kavramına ilişkin yönetsel konuların ve devletin rolünün açıklanacağı bölüm, yazının bir diğer önemli kısmını oluşturacaktır. Yazının bir başka bölümünde ise akıllı şehir kavramının beraberinde getirdiği sorunlar incelenecektir; burada temel problemler ve başlıca zorluklar, yine gerektiğinde günlük yaşamdan örneklerle açık bir şekilde ortaya konulacaktır.

Anahtar kelimeler: *Vatandaş, gizlilik, entegrasyon, modernize*

[1] Uzm., Yakın Doğu Üniversitesi, Yapay Zeka ve Bilişim Fakültesi, Yazılım Mühendisliği Bölümü, sinem.alturjman@neu.edu.tr

[2] Dr., Yakın Doğu Üniversitesi, Yazılım Mühendisliği Bölümü, ramiz.salama@neu.edu.tr

1. INTRODUCTION

Today, the incredible growth of cities has been one of the popular problems on almost every single country to ever exist on Earth. People have been facing ex-treme difficulties on a daily basis; especially on more crowded countries such as China. Shanghai, for example, the city of China with almost twenty-seven million habitants [1].

2. MATERIALS AND METHODS

2.1 Different Areas of Smart City Applications

There are main areas of the smart city concept which it can be applied perfectly when there is enough research and data collection made. Although, the huge chunk of data should be as close to one hundred percent accurate as in case of a failure, there can be huge problems, even fatality. There are many different areas where smart city concept is meant to be in work, such as;

•Smart Parking
•Waste Management
•Traffic Management
•Health
•Air Pollution
•Transportation
•Smart Lighting
•Water Management
•Charging Stations
•Connected Car
•Public Security
•Smart Buildings

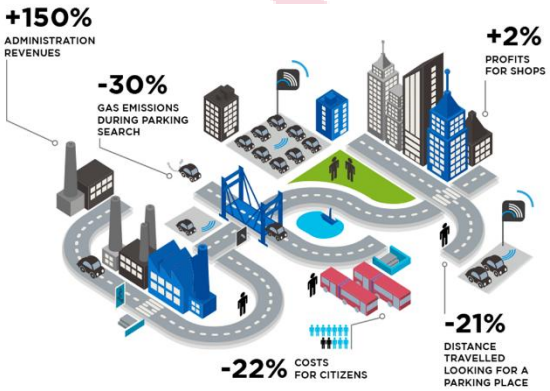


Figure 1 showing the benefits of Smart City concept

2.2 How Applications of Smart City are Applied

Some of the most efficient applications of Smart City stated above are mainly the most popularly used among the cities all around the world. To begin with, parking is one of the alarming problems as car count increases every day in cities. Smart City concept comes out with an easy and efficient fix for this by the development of Smart Parking [2]. Smart Parking is based on multiple different sensors installed in parking spots in order to be able to monitor if a slot is being used or empty. It allows other drivers who are searching for an empty parking slot to find one easily in no time, rather than having to spin endlessly in a hopeless way and being stressed out for no reason. Smart Parking system can also be synchronized with simple phone applications in order to notify the user of any empty parking slots for real-time efficiency, which is clearly one of the most useful features of it. Another great application of Smart City concept is waste management. Waste management is an extremely significant issue when it comes to daily jobs of a municipality of a city. In crowded cities, pollution is an inevitable factor and it should be avoided at all times with the correct measurements taken, in order to prevent any spreadable disease. Waste Management in a Smart City concept works as explained; As it is also done in smart parking, sensor equipped recycle bins are installed all around the city and when they are basically full, an alarm- based system warns the authorities and it is to be collected as soon as possible in such case [3].

Another main system in waste management concept is where shortest and most efficient routes are calculated digitally for bin truck drivers for time management and also for space management. When it comes to recycling part, sensors also come incredibly handy in this case too. Certain types of robotics and sensors work together in order to sort out and organize what type of waste is recycled at certain recycling spots, preventing any failures of recycling. Furthermore, the collected waste can be used to be converted in to

energy resources with the help of a collaboration of smart city application concepts and technology. Traffic is with no doubt one of the vital points when it comes to the Smart City concept. With the help of Smart City application, managing the traffic has never been easier- especially in huge and extremely crowded cities. Basically, as used on all the other Smart City systems, hundreds of real-time monitoring devices such as intelligent CCTV footage collectors are installed in different points and locations of roads all around a city. The next step is setting up those devices to communicate with each other, just like how the real traffic deputy police officers do. These devices, as they have artificial intelligence installed inside them already, can easily calculate the real-time speed, direction and density of a vehicle in no time, no matter its size or how fast it is, even in the case of bad weather conditions, because of the robust physical condition of the devices [4]. After the data is collected, the fasted method to relieve the current traffic out of the congestion is worked out in just a matter of minutes.

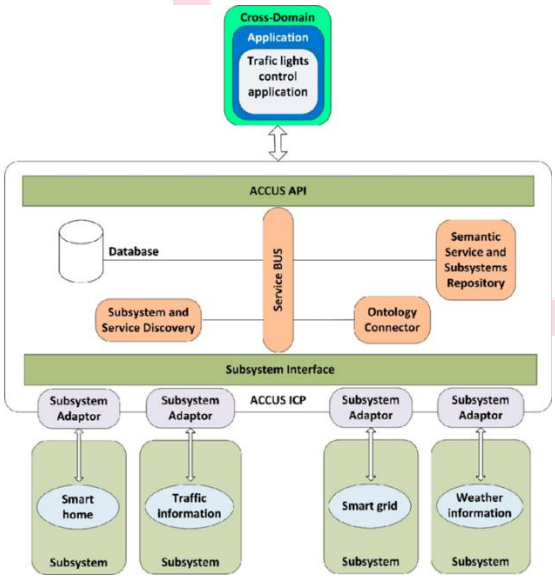


Figure 2, A General Smart management and Traffic management system on Smart City concept

Health is the most important term when it comes to the developments about smart city concept. It is basically what manages our health in times of alarming situations with the usage of technology and gadgets [5]. Being a part of the smart city applications, right now, people from all kinds of economical class can easily apply for healthcare without any problems. According to their location, smart city concept offers an easy route for users to find the nearest clinic, hospital or health service points in case of and emergency. Different kind of sensors installed on artificial intelligence using phones can detect a situation is going wrong with a person and even call for an ambulance or any sort of help in a bad situation, which can without any doubts save millions of lives in seconds.

In addition, different kind of environmentally capable sensors are installed on different locations which are capable of protecting the locals from hazards by informing them digitally, which are close around their living spaces, such as a polluted water source [6]. As for the most important part of health in smart city concept, a specifically designed device can warn people about an upcoming extreme situation such as an earthquake or tornado, which will be saving millions of lives all around the world. Most of the statistical analysis of these warning systems are based on real life information from thousands of different professional critics around the world. Air Pollution is one of the extreme disasters which was brought mainly by the use of technological gadgets, which we can say is the problem of our century. With the help of scientists and technological developments, finally, us humans are able to solve at least some of the air pollution situation which is caused by no one but us. First and the most efficient method of the appliance of smart city concept to air pollution problem is the real-time monitoring of air quality. Basically, this is about electronical gadgets installed with

artificial intelligence using sensors to find out information about parameters of general air quality [7]. Later on, collected data is provided by the same sensors for the public information of people around and authorities which can take the much-needed measures in order to successfully prevent air pollution hazards and decrease its impact on our living standards.

Transportation, without any doubt, is most probably a disaster in crowded cities such as Mumbai, India with an average of more than twenty thousand people per square kilometer. In such cases, people are mostly forced to be enroute before at least three or four hours so that they can arrive to their workplaces or any other destination on time. Travel times increase in an absurd way in such situations. Smart city concept comes out with an efficient solution to the transportation problem in a few simple, yet extremely effective steps. These steps combined together add up to form the Multi-Modal transportation shape, which is basically about bikes, skates or other less traffic congesting vehicles which can be hired and shared digitally among the users [8]. Amsterdam is one of the most important examples to this, as most people prefer to rent bikes online for transportation.

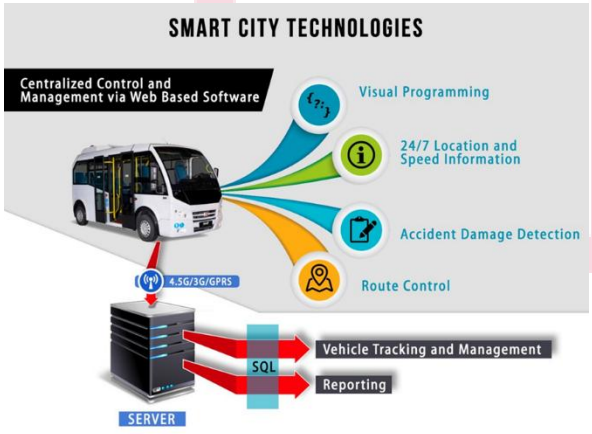


Figure 3, Transportation in a smart city concept

Another important factor to talk about when it comes to Smart City application is the smart lighting. It is basically preserving energy and using it only when needed. Electricity is the preserved energy in this case of smart lighting as it is the main and only resource. Gadgets in the smart lighting system of smart cities are commonly equipped with mini monitors inside them which basically only trigger the lights to be turned on when there is motion, and this motion being a car passing by, a human, any animal and so on [9]. This is basically used to prevent hours and hours of city lights being turned on causing extreme amount of money to be wasted worldwide. In addition, it prevents the lifespan of lights going off because of being waste-used for the entire day, week and years. Adaptive lighting is another important method in terms of smart lighting. It is even used on smart phones, which is basically the term used to explain the situation where the phone screen or any other kind of light turns on or off, or adjusts its own brightness according to the daylight condition.

For instance, if the location is dark, the screen light gets dark too so the user's eye is not damaged, also its more energy efficient. If the sun is bright and shining, it is rather difficult for the user to see, so the smart light makes itself brighter for the user to see easily. Smart lighting works incredibly well on crime situations as well. For example, let us say there is a place is being robbed quietly and there is no one around, no CCTV to record the robbers and no active sound alarms to make them leave the place. A simple smart feature enabled light bulb will shine as bright as possible all of a sudden, as soon as it detects the thief or thieves on action [10]. What is even better is that most of the smart light systems are empowered from the sun and will work even if there is a power outage. Water management, when it comes to the application on the smart cities is a must for every city on Earth. It is one of the best ways to ever exist, in our cause with losing our precious water sources for no reason. First of all, before we know that a water can be used, first step should always be to check its clarity and see if it is safe. (WQM) Water quality monitoring systems play a crucial role in such situations. These systems are used to calculate the pH levels and measure the levels of

unsafe contamination if there is such case. Real time data collection is possible with such devices and gadgets which are all a part of the smart city application system. Furthermore, in situations of possible floods and water-caused disasters, water management plays a significant part as there are hundreds of different models of monitoring gadgets and sensors which can later warn local habitants out of any possible problematic scenario.

In today's world, as of 2024 mostly, charging stations are one of the most commonly used and live examples of smart city applications [11]. There are millions of charging stations all around the world and it is super normal these days, even, in some cities, electrical charging stations for cars are used more than normal petrol stations Charging stations basically are petrol stations but instead of petrol, electricity is used to fuel up an electric based car. They support economic growth of any country in an incredibly high rate, have huge impact on the environment in good terms and also most of the electronic cars work more efficiently than normal cars as their technological abilities are much more advanced than cars which are not EVs.

Connected cars also do play a crucial role in the building and flow-working of smart cities. One of the most important aspects of connected cars are the reduced emission levels. For example, start-stop system of a car's engine stops it from staying idle for a long time, and prevents both the needles waste of fuel and pollution of air for no reason.

Connected cars are also safer in a significant stake as they are equipped with hundreds of tiny sensors which are basically working as assistants for the driver for a safer journey. Examples to these assistants can be the parking sensor, which prevents the driver from crashing the car when parking, the icy-road feature which prevents the driver to lose control of the car especially in winter times when the tires are unprepared for an icy road [12]. Some higher technology connected cars also drive themselves to nearest hospital or healthcare point in cases where driver is unconscious or are not able to drive.

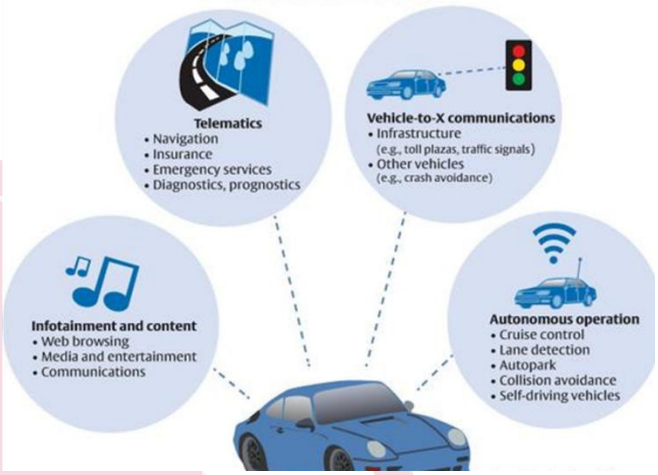


Figure 4, Advantages of the connected car.

Public security is another important point to talk about when it comes to smart city applications. It is mostly about devices such as CCTV with artificial intelligence being used in order to make it easier for the police or other authorities of a city to take action in an event of emergency. In addition, most of the real-time monitoring sensors are collaborated with high quality cameras which are capable of motion detecting. In a dangerous situation, these high technology gadgets will warn the nearest police officer support point so that they can take action as soon as possible to prevent any possible problematic outcome. Crime hotspots, where most of the crimes are statistically proven to be occurring at, can also be spotted out by the use of smart city public security method as the gadgets in this type of systems are able to calculate crime rates weekly, monthly or yearly on specific locations by receiving data from all possible local sources and also by the police entry and they will then export the calculated results using artificial intelligence for the police departments [13].

With the help of the public security of smart city systems, crimes in most hotspots are significantly reduced and it is believed to be one of the most important solutions, working both efficiently and in a lightning-fast way using the flow of technology. Face recognition is another strong advantage in this sort of systems as CCTV footage of millions of people can be taken, scanned and sent to the police department systems in any case of emergency, even if there is an extreme crowd. These systems are so efficient and professional that just within a few seconds it is possible for the police to find out tons of information about random people who are just wandering on the street amongst the other people who are possible threats. Last but not least, Smart buildings. Smart buildings are basically like smart phones in order to explain easier. Normal buildings are the ones that we live in, without any technological or smart adaptive ability. Smart buildings are for example able to warm themselves up before we are in after a cold night out, or vice versa [14]. There are millions of different gadgets nowadays which are produced only for smart buildings in order to make life easier for people who live in. These buildings are equipped with advanced technologies. There are many cases and scenarios which explain smart buildings and how effective and full of advantage they are. For instance, a smart building can adjust lights, heating, cooling, cleaning systems all at once without the owner even needing to move for a second. Also, in cases of emergency, let us say when the house owner is sleeping, the smart building warns everyone in the building as soon as there is a possible threat of literally anything bad happening [15].

Figure 5, Advantages of smart buildings.

3. RESULTS AND DISCUSSION

in the successful results of smart cities can be seen clearly throughout the world. Its possible impact on our daily lives, working sectors, houses, living standards and even health is obvious and as the technology is developing, the gadgets and network connections are developing, which leads to the development of smart cities in to another level. Application of smart city features in to our lives has not been easy, as there are many detailed difficulties coming along with it, but it is totally worth it [16]. Here are some statistical results of the usage of smart city concepts from various resources.

4. CONCLUSION

As the results speak for themselves, there is a vast amount of help smart city applications have contributed to modern life of people nowadays. It is, without any doubt, a revolutionary step in terms of the technological development of the modern society, and it is a subject which completely carried us, humans to an inevitable and alarming spot where we can help ourselves to have higher living standards. Of course, there are some consequences to this as well. For example, hackers are the most dangerous type of criminals in the concept of smart city applications. If successful, they are able to access private data of millions or even billions of people, they are able to steal

incredible amounts of money and other sources of income from different online bank accounts or wallet systems. This may sound simple when talking about, but these data leak can lead to government failures, downfall or even worldwide crisis. Cyber warfare is seen to be one of the most important reasons throughout the years which can lead to a huge war outbreak. Other consequences can be main problems with electricity. It is found out that electricity usage can be doubled in following years in cities which are mainly working on the system of smart city. To conclude, Smart City applications are what saves us from many difficulties during the day, and will most probably be the new way of life in a total change, a huge revolution in other words, in the near future.

References

1. Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future trends and current state of smart city concepts: A survey. IEEE access, 8, 86448-86467.
2. Kaluarachchi, Y. (2022). Implementing data-driven smart city applications for future cities. Smart Cities, 5(2), 455-474.
3. Sánchez-Corcuera, R., Nuñez-Marcos, A., Sesma-Solance, J., Bilbao-Jayo, A., Mulero, R., Zulaika, U., ... & Almeida, A. (2019). Smart cities survey: Technologies, application domains and challenges for the cities of the future. International Journal of Distributed Sensor Networks, 15(6), 1550147719853984.
4. Okafor, C. C., Aigbavboa, C. O., Akinradewo, O. I., & Thwala, W. D. (2021, April). The future of smart city: A review of the impending smart city technologies in the world. In IOP Conference Series: Materials Science and Engineering (Vol. 1107, No. 1, p. 012228). IOP Publishing.
5. Angelidou, M., Psaltoglou, A., Komninos, N., Kakderi, C., Tsarchopoulos, P., & Panori, A. (2018). Enhancing sustainable urban development through smart city applications. Journal of science and technology policy management, 9(2), 146-169.
6. Ameen, S. (2021). State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. Asian Journal of Research in Computer Science.
7. Vasilev, V., & Ognyanski, D. (2020). The new face of public management–about the "smart city" and its impact on the future development of society. KNOWLEDGE International Journal, 42(1), 91-93.
8. Rao, S. K., & Prasad, R. (2018). Impact of 5G technologies on smart city implementation. Wireless personal communications, 100(1), 161-176.
9. Caragliu, A., & Del Bo, C. F. (2019). Smart innovative cities: The impact of Smart City policies on urban innovation. Technological Forecasting and Social Change, 142, 373-383.
10. Hassebo, A., & Tealab, M. (2023). Global models of smart cities and potential IoT applications: A review. IoT, 4(3), 366-411.
11. Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A review of IoT-based smart city development and management. Smart Cities, 7(3), 1462-1501.
12. Eckhoff, D., & Wagner, I. (2017). Privacy in the smart city-applications, technologies, challenges and solutions.
13. Latif, G., Alghazo, J. M., Maheswar, R., Jayarajan, P., & Sampathkumar, A. (2020). Impact of IoT-based smart cities on human daily life. In Integration of WSN and IoT for Smart Cities (pp. 103-114). Cham: Springer International Publishing.
14. Ageed, Z. S., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Rashid, Z. N., Salih, A. A., & Abdullah, W. M. (2021). A survey of data mining implementation in smart city applications. Qubahan Academic Journal, 1(2), 91-99.
15. Mishra, P., Thakur, P., & Singh, G. (2022). Sustainable smart city to society 5.0: State-of-the-art and research challenges. SAIEE Africa Research Journal, 113(4), 152-164.
16. Nassereddine, M., & Khang, A. (2024). Applications of Internet of Things (IoT) in smart cities. In Advanced IoT technologies and applications in the industry 4.0 digital economy (pp. 109-136). CRC Press.

Near East University

Journal for Artificial Intelligence and Internet of Things

Volume: 5
Issue: 1

ISSN
3062-1968

SOCIAL CYBERSECURITY AND ARTIFICIAL INTELLIGENCE: A SURVEY

SOSYAL SİBER GÜVENLİK VE YAPAY ZEKA: BİR İNCELEME

Fadi AL-TURJMAN [1]
Chadi ALTURJMAN [2]
Ramiz SALAMA [3]

ABSTRACT

Over the past years, social cybersecurity has become one of the crucial research fields of modern digital communication systems because of the accelerated growth of various digital and web-based cyber threats. Both attackers and defenders have adopted ever-increasing use of artificial intelligence: AI, which has drastically transformed cybersecurity. Today, with the addition of newer methods like artificial intelligence (AI) for both fraud and AI attacks and tactics, cybercriminals use it to automate the most-explicable types of cyber criminals' malicious communication, including phishing attacks, misinformation campaigns, fake social media accounts, the use of deepfakes, spam content and automated social engineering attacks. The threat of social media was launched via advanced AI algorithms such as deepfakes and so on. Consequently, researchers and organizations have begun incorporating artificial intelligence into defensive solutions for quicker detection and prevention of these threats. To answer this, a survey paper is conducted to explore social cybersecurity and artificial intelligence from the point of view of machine learning, such as modern machine learning-based attack detection techniques, evaluation methods for them as well as the issues of contemporary times and possibilities for the future. This work studies machine learning and deep learning techniques for cyber threat detection such as supervised learning, unsupervised learning, neural networks, natural language processing (NLP) and transformer-based models like BERT. The sections of this paper are organized into several sections. Here the literature review looks back at the previous works on AI driven cybersecurity systems and social cyber threat monitoring. The "Materials and methods" section gives insight of widely used datasets, algorithms, and evaluation metrics. The results and discussion section compares and analyzes advantages and limitations of various AI approaches. Last but not least, the paper identifies its current problems, future possibilities, and conclusions about the future of social cybersecurity.

Keywords: *social cybersecurity, artificial intelligence, identifying attacks, assessments*

ÖZ

Son yıllarda, çeşitli dijital ve web tabanlı siber tehditlerin hızla artmasıyla birlikte, sosyal siber güvenlik modern dijital iletişim sistemlerinin en önemli araştırma alanlarından biri haline gelmiştir. Hem saldırganlar hem de savunmacılar, siber güvenliği kökten değiştiren yapay zeka (YZ) kullanımını giderek daha fazla benimsemiştir. Günümüzde siber suçlular; oltalama (phishing) saldırıları, yanlış bilgilendirme kampanyaları,

[1] Prof. Dr., Yakın Doğu Üniversitesi, Yazılım Mühendisliği Bölümü, , fadi.alturjman@neu.edu.tr

[2] Researcher, Department of Chemical Engineering, Waterloo University, ON N2L 3G1, Canada,chadialtrjmanc@gmail.com

[3] Dr., Yakın Doğu Üniversitesi, Yazılım Mühendisliği Bölümü, ramiz.salama@neu.edu.tr

sahte sosyal medya hesapları, deepfake kullanımı, spam içerikler ve otomatik sosyal mühendislik saldırıları gibi kötü niyetli iletişim türlerini otomatikleştirmek için yapay zekadan yararlanmaktadır. Sosyal medya kaynaklı tehditler, deepfake gibi gelişmiş yapay zeka algoritmaları aracılığıyla yeni bir boyut kazanmıştır. Buna karşılık olarak araştırmacılar ve kuruluşlar, bu tehditlerin daha hızlı tespit edilmesi ve önlenmesi amacıyla savunma çözümlerine yapay zekayı entegre etmeye başlamışlardır. Bu çalışma, sosyal siber güvenlik ve yapay zekayı makine öğrenimi perspektifinden ele alarak; modern makine öğrenimi tabanlı saldırı tespit tekniklerini, bunlara yönelik değerlendirme yöntemlerini, güncel sorunları ve gelecekteki olanakları incelemektedir. Çalışma; denetimli öğrenme, denetimsiz öğrenme, yapay sinir ağları, doğal dil işleme (NLP) ve BERT gibi transformer tabanlı modeller dahil olmak üzere siber tehdit tespitine yönelik makine öğrenimi ve derin öğrenme tekniklerini ele almaktadır. Makale çeşitli bölümlerden oluşmaktadır; literatür taraması bölümü, yapay zeka destekli siber güvenlik sistemleri ve sosyal siber tehdit izleme üzerine daha önce yapılmış çalışmaları incelemektedir. "Materyal ve Yöntem" bölümü; yaygın olarak kullanılan veri setleri, algoritmalar ve değerlendirme metrikleri hakkında bilgiler sunmaktadır. "Bulgular ve Tartışma" bölümü, çeşitli yapay zeka yaklaşımlarının avantajlarını ve sınırlamalarını karşılaştırıp analiz etmektedir. Son olarak makale; mevcut sorunları, gelecekteki olanakları ve sosyal siber güvenliğin geleceğine dair çıkarımları ortaya koymaktadır.

Anahtar kelimeler: *sosyal siber güvenlik, yapay zeka, saldırıların tespiti, değerlendirme*

1. INTRODUCTION

The study also highlights recent pieces published between 2023 and 2025, providing an updating perspective on developments in social cybersecurity research. The sections of this paper are organized into several sections. Here the literature review looks back at the previous works on AI driven cybersecurity systems and social cyber threat monitoring. The "Materials and methods" section gives insight of widely used datasets, algorithms, and evaluation metrics [1]. The results and discussion section compares and analyzes advantages and limitations of various AI approaches. Last but not least, the paper identifies its current problems, future possibilities, and conclusions about the future of social cybersecurity.

2.RECENT SURVEY PAPERS AND CURRENT RESEARCH TRENDS

Research on AI-based techniques for the identification of cyber threats on social media platforms, online communication systems, and digital communities is on the rise. With the increasing sophisticated nature of cyberattacks, intelligent systems that are able to analyze existing threats in real time and make automated decisions have begun to be proposed [2]. One such survey – "A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects" – gave a thorough overview of modern forms of AI-based cybersecurity. Based on the proposed study, machine learning, deep learning, and natural language processing techniques were considered in the detection of fake news, phishing, cyberbullying, bots, and deepfake content. They stated that explainable artificial intelligence (XAI) is also becoming increasingly important to know, since cybersecurity systems need to make clear and transparent decisions based on the information presented. An interesting emerging direction in research is the application of transformer-based language models, namely BERT, RoBERTa, GPT etc. in the cybersecurity literature

Some of the recent studies have also explored AI-based Security Operation Centers (SOCs), autonomous cyber defense systems, and real-time threat intelligence platforms [3]. These systems intend to automate the detection and incident response processes of cyberattacks, with the aim of reducing the workload of cybersecurity professionals. Current trends of social cybersecurity research include: explainable AI, privacy-preserving machine learning, multimodal threat detection, autonomous defense systems, and human-centered cybersecurity. The rising volume of academic papers and industrial applications highlights that AI-assisted social cybersecurity

will necessarily remain a very significant research field in the foreseeable future.

3. MATERIALS AND METHODS

This section explains the datasets, artificial intelligence techniques, machine learning algorithms, deep learning models, and evaluation methods commonly used in social cybersecurity research [4]. Modern AI-based cybersecurity systems require large datasets and advanced analytical methods to detect cyber threats accurately and efficiently.

3.1 Artificial Intelligence Techniques

Techniques of artificial intelligence in social cybersecurity: supervised learning, unsupervised learning, reinforcement learning, etc. [5]. Supervised learning is one of the most popular AI techniques for cybersecurity research. Supervised learning is training models with labeled datasets, representing normal and malicious examples. The machine gains insights about cyber threats and is able to form rules to classify new data. Supervised learning approaches are proven to be super useful for phishing detection, spam filtering, malware classification, and fake news identification. Unsupervised methods are useful in cases without or constrained due to unlabeled data [6]. These techniques detect the hidden structure and abnormal behavior in dataset without the need to define traditional attack identifiers. Clustering algorithms and anomaly detection systems are widely adopted in detection of intrusion and behavior of the bots. For cybersecurity, another rapidly emerging AI approach is reinforcement learning.

A reinforcement learning system actively learns from an environment and can be rewarded/punished based on behavior. Researchers study reinforcement learning for automatic threat response systems and adaptive cyber defense mechanisms [7]. Hybrid approaches for AI are also catching fire now, where there are a hybridizing method and several ways of learning to make things better.

4. RESULTS AND DISCUSSION

A recent study shows that AI-based models are better suited to detect complex cyber threats than rule-based security methods by identifying social media and online communication tools. Through machine learning and deep learning methods, great agility, enhanced detection, and increased scalability when processing massive amounts of digital information can be achieved [8]. As one of the high-level observations of recent work, deep learning models have been demonstrated to have a higher detection rate than traditional ML.

They can be efficient techniques to study linguistic features which are not possible as keyword class-based systems [9]. It is true that Random Forest, SVM and Naive Bayes algorithms have obtained good results on multiple cybersecurity tasks.

5. CONCLUSION

In contrast to the traditional cybersecurity model which targets systems and networks, social cybersecurity works to protect against attacks that attempt to exploit human behavior, social interaction, and information manipulation [10].

As cyber threats evolve, we must maintain an increasing sophistication to prevent detection systems driven by AI from serving to protect individuals, organizations, and digital societies from more sophisticated and intelligent attacks.

References

[1] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEe Access, 12, 12229-12256.

[2] Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67(8), 6969-7055.

[3] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*(2), 564-574.

[4] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029-1053.

[5] Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: a systematic mapping of literature. *Ieee Access*, *8*, 146598-146612.

[6] Malatji, M., & Tolah, A. (2025). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*, *5*(2), 883-910.

[7] Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In Artificial intelligence for societal issues (pp. 3-25). Cham: Springer International Publishing.

[8] Akhtar, Z. B. (2024). Harnessing artificial intelligence (AI) for cybersecurity: Challenges, opportunities, risks, future directions. *Computing and Artificial Intelligence (CAI)*.

[9] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173.

[10] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

Near East University

Journal for Artificial Intelligence and Internet of Things

Volume: 5
Issue: 1

ISSN
3062-1968

TECHNIQUES FOR COUNTERING SOCIAL ENGINEERING ATTACKS

SOSYAL MÜHENDİSLİK SALDIRILARIYLA MÜCADELE TEKNİKLERİ

Ramiz SALAMA [1]
Chadi ALTRJMAN[2]
Fadi AL-TURJMAN[3]

ABSTRACT

Social engineering is the manipulation and exploitation of human psychology to trick others into disclosing sensitive information or taking activities that could jeopardize security. Social engineering is a technique that involves manipulating and deceiving individuals or groups in order to persuade them to expose secret information or engage in actions that are harmful to their business. Hackers frequently use this strategy to obtain sensitive information, such as banking or login credentials.

Keywords: *Social engineering, Cybercrime, Phishing, Security awareness, multi-factor authentication, Human behavior*

ÖZ

Sosyal mühendislik, başkalarını hassas bilgileri ifşa etmeye veya güvenliği tehlikeye atabilecek eylemlerde bulunmaya yönlendirmek amacıyla insan psikolojisinin manipüle edilmesi ve istismar edilmesidir. Bu, bireyleri veya grupları gizli bilgileri açığa çıkarmaya ya da kurumlarına zarar verecek eylemlerde bulunmaya ikna etmek için manipüle etmeyi ve kandırmayı içeren bir tekniktir. Bilgisayar korsanları, bankacılık bilgileri veya oturum açma kimlik bilgileri gibi hassas verileri ele geçirmek için sıklıkla bu stratejiyi kullanırlar.

Anahtar kelimeler: *Sosyal mühendislik, Siber suç, Oltalama, Güvenlik farkındalığı, Çok faktörlü kimlik doğrulama, İnsan davranışı*

1. INTRODUCTION

Social engineering attacks exist in the digital landscape. Their fundamental nature the exploitation of human vulnerabilities requires the employment of multiple defense approaches and systems. The study examined protection strategies and processes such as awareness training, security protocols, technology solutions, and an organizational cybersecurity awareness culture [1]. As a result, it has been demonstrated that user awareness training can effectively equip an individual with social engineering strategies. Regular awareness campaigns, as well as a well-

[1] Dr., Yakın Doğu Üniversitesi, Yapay Zeka ve Bilişim Fakültesi, Yazılım Mühendisliği Bölümü, ramiz.salama@neu.edu.tr

[2] Researcher, Department of Chemical Engineering, Waterloo University, ON N2L 3G1, Canada,chadialtrjmanc@gmail.com

[3] Prof. Dr., Yakın Doğu Üniversitesi, Yazılım Mühendisliği Bölümü, , fadi.alturjman@neu.edu.tr

prepared incident response strategy, will work together to mitigate the impact of social engineering at-tacks.

2. WHAT IS SOCIAL ENGINEERING

255 million attacks using this strategy happened in the first six months of 2022. Social engineering attacks can occur via a variety of communication channels, including text messages, phone calls, and emails. Attackers use phishing, pretexting, and tail-gating to obtain sensitive information such as credit card details or system credentials. Many hackers use social media and other internet platforms to gather critical information about their targets. A social engineering attack is an intentional attempt to trick someone into disclosing personal information or performing a specific activity that could be exploited to obtain unauthorized access to an organization [2]. Adversaries use a variety of tactics to mislead targets and gain access to important data or systems.

2.1. Types of Social Engineering Attacks

Developing awareness is critical in preparing to reject social engineering tactics. There is an enormous variety of social engineering attacks, therefore understanding how each one works will be critical. Understand the common strategies and warning indicators of a social engineering attack. Each sort of attack carries a long list of hazards that can be used to compromise systems or data [3]. The next section discusses common social engineering assaults and offers practical advice on how to protect your business from them.

2.2. Phishing

What is it? Phishing is a popular type of social engineering attack in which bogus emails or websites are used to trick someone into disclosing personal information or even acting in a way that may hurt one's own interests. One approach to accomplish this is to instill a sense of urgency or anxiety in the desired activity. The most popular method is to use online pages or emails that closely resemble reputable businesses like banks, governments, or well-known organizations [4]. The goal is to persuade the victim into clicking on a link or disclosing sensitive information, such as login and financial information. Preventive tips: Never respond to unsolicited emails, particularly ones containing attachments, links, or urgent information. Before responding to an email or any other information request, make sure you know who sent it. Hover your cursor over the sender's name to reveal their email address, or contact them via a well-known communication channel. Using a spam filter, phishing emails can be identified as spam and blocked from reaching the receiver.

2.3. Please Do Not Send Any Financial Or Personal Information By Email.

Remember to use strong, unique passwords for all of your accounts, and enable two-factor authentication wherever possible. Make sure to update your antivirus and operating system on a regular basis [5]. Be aware of the potential risks associated with utilizing a public Wi-Fi network, and be cautious about the information you share.

2.4. Tailgating

Tailgating What is it? Tailgating, also known as "piggybacking," is a form of social engineering in which a person gains unauthorized entrance to a secure area by closely following an authorized individual. It can be done remotely, for example, by using an unprotected link to gain access to a protected network, or physically, by secretly following a target through a door into a secure office building. Tailgating is based on the victim's faith in the perpetrator or a desire to grant them entrance to a prohibited place. Attackers frequently utilize this strategy to obtain unauthorized access to sensitive data or systems. Prevention tips: Install turnstiles or other physical obstacles to regulate who enters and exits through security doors [7]. Install cameras to monitor all points of entrance and identify tailgaters. Staff should be encouraged to con-front anyone attempting to follow them through a secure door and to be on the watch for tailgaters. Implement a "buddy system" policy that requires staff to

identify themselves and be escorted by another staff member while entering a secure area. Use electronic access control devices, key cards, or biometric scanners to provide entry to restricted locations after verifying the person's identification.

2.5. Baiting

What is it? One such social engineering method is "baiting." This social engineering strategy involves cajoling or coaxing an individual into disclosing personal information or taking some action by dangling a reward or promise in front of them. The promise or incentive is frequently expressed in the form of an appealing gift, money, or exclusive early access to certain items. A scammer, for example, would set up a website promising a free trip in exchange for personal information, or they would send an email offering a large return if the recipient clicked on a specific link or re-veiled some information. Baiting uses greed, curiosity, or a need for something to fool the victim into disclosing critical information or performing a certain action. Prevention tips: One should shun offers that seem too good to be true [8]. Do not open attachments or click on links in emails from unknown or suspect sources. When replying to a request, do not provide any personal or financial information. It is important to use strong and unique passwords for all of your accounts, and to use two-factor authentication wherever available. You should frequently update your antivirus software and operating system. Recognize the tactics used by phishers and educate yourself on how to avoid such assaults while also keeping others informed. Pre-texting: What is it? Pretexting is a sort of social engineering that includes creating a fictitious identity or scenario in order to gain confidence in being granted access to sensitive systems or data. These are accomplished through a series of online, phone, or physical meetings. In some circumstances, the sham identity or scenario is even tailored to meet the needs or interests of the target party in order to increase success rates. Pretexting assaults, such as impersonating a fraudster as a bank manager, are meant to gain the victim's trust, which can result in the revocation of personal information such as account numbers and passwords. The fraudster can also build a faked email or website that appears to be authentic and request personal information from the victim, such as login passwords [9]. How To Prevent: Avoid unsolicited phone calls or emails, particularly those that want sensitive personal or financial information. Do not provide money or personal information in response to unsolicited solicitation. Verify the person's identification before sharing important information. This could be accomplished by either contacting the individual or institution using an available formal means of communication, or by independently attempting to locate their contacts. Use strong, unique passwords for all accounts, and enable 2-factor authentication if it is available. Make sure to update your antivirus and operating system on a regular basis. Never become a victim of pretextual deception. Learn everything you can about these varied attacks and educate others.

2.6. Scareware

What is it? Scareware is a type of social engineering that scares people into taking action, usually purchasing a product or disclosing sensitive information, by instilling dread and the sense of urgency. This is frequently accompanied by bogus emails, websites, or pop-up windows that claim to scan the target's PC for malware or viruses. The notification may also warn that any delay in addressing the threat would result in a worse consequence or spread the infection to other systems [10]. Deception: Scareware works by tricking the victim into buying a product or service or disclosing personal information. Often, the product or service being sold is fictional or of poor quality, and personal information is exploited fraudulently.

2.7. Detecting Emergent Threats and Defenses

These include research into deepfakes, their potential applications in social engineering, the manipulation of social media platforms for disinformation campaigns, the launch of targeted attacks, and the creation of real-time AI-powered detection systems to detect emerging social engineering strategies [11].
When assessing such a corpus of knowledge, this study will draw on the most recent advances in defense strategies to provide an overarching strategy for resisting social engineering attacks.

3. MATERIALS AND METHODS

This study will comprise a complex investigation into the techniques of defense against social engineering attacks, using the resources and methodology that are accessible [12]. This study will employ the following materials and methods:

3.1. Literature Review

3.1.1. Academic Database: Core academic databases, such as ScienceDirect, Scopus, and Web of Science, will be used to search for key peer-reviewed publications and conference proceedings published between 2021 and 2024. Keywords for the search phrase will include, but are not limited to, social engineering attacks, methods of protection, user awareness, security protocols, and organizational culture.

3.1.2. Inclusion Criteria: Only publications focusing on the study areas specified in section 5 (Amount of Previously Published Work) will be considered.

3.2. Data Integration and Synthesis

Data acquired from various research methodologies will be compiled and combined to provide a comprehensive overview of social engineering defines strategies. This includes: Mapping of Research Findings The literature review's research findings are mapped against the research areas mentioned in Section 5. Cross-referencing Resources: Insights from security resources, as well as case studies, will be used to support and expand on academic research findings. Integration of Expert Interviews: The information gathered from the expert interviews will be used to make more practical decisions, such as the real-world problems of applying defines strategies [13]. Using this multidisciplinary research technique, the project will propose and collect a complete, robust, and diverse set of data to develop a precise, coherent, and effective defines strategy against the social engineering attack.

4. RESULTS AND DISCUSSION

4.1. The Tips Below Can Help You Prevent Such Incidents

Avoid opening attachments or clicking on dodgy links. Ensure that the antivirus software and operating system are regularly updated. Do not display pop-up windows or warnings alerting the user to security dangers or stating that malware has been identified on the user's machine. These could be examples of scareware. Do not install or buy security software based on a popup window or message [14]. If you believe your computer has been penetrated by malware, use a trusted security solution to remove the associated hazards. Educate yourself and others on the dangers of downloading software from unknown websites, as well as scareware and other types of malwares.

4.2. Quid Pro Quo

What is it? Quid pro quo social engineering is providing an incentive in exchange for an individual disclosing confidential information or granting access to a system. This is often done over the phone or in person, with the given offer taking the guise of a simple request or favor. In a quid pro quo con, a victim may receive a phone call from someone claiming to be from the IT department and requesting access to a specific computer to resolve an issue in exchange for the password. A cybercriminal may also offer a reward or a voucher in exchange for receiving sensitive information. Such quid pro quo assaults

take advantage of the victim's eagerness to disclose any sensitive information in exchange for anything [15]. Prevention Tips: Do not reply to unsolicited phone calls or emails asking for sensitive information or offering access to valuable information in exchange. If the popup occurs unexpectedly, do not disclose any money or other confidential information. Before disclosing any critical information, confirm the identity of the person you're speaking with. The latter can be accomplished by contacting the person or organization concerned through any recognized channel of communication or by physically obtaining the individual's or organization's contact information. Make careful to generate strong, unique passwords for each account, and use two-factor authentication when available. Keep your antivirus software and operating system up to date. Find out what quid pro quo assaults are and educate your colleagues and yourself on them.

4.3. Impersonation

Impersonation is a social engineering technique in which an attacker impersonates another person in order to gain their trust and, ultimately, get illegal access to confidential data or systems. This could be done online, by phone, or in person. Impersonation can take the form of pretending to be a respectable person or group, or it can involve the fabrication of an entirely new identity. An example would be sending an email that appears to be from a boss or a colleague, requesting access to specific systems or secret data. Another example is when an attacker calls an organization and poses as a representative of a company that the organization trusts, requesting unauthorized access to sensitive information or computer systems [16]. Prevention tips: Unsolicited phone calls or email requests for sensitive personal or financial information should not be responded to. Do not reveal any monetary or personal information, especially if asked unexpectedly. Prior to releasing any personal information, confirm the identity of the individual requesting it. This can be accomplished by using an official communication link, particularly with the person or institution, or by manually searching for contacts. You should use strong, unique passwords for all accounts and enable two-factor authentication where possible. Update your antivirus software and operating system on a regular basis. Identify impersonation strategies and promptly educate yourself and your coworkers about this type of attack.

4.4. Strategies For Mitigating a Social Engineering Attack

If you suspect your company has been the victim of a social engineering attack, follow these actions to respond and limit the likelihood of future attacks: Determine the source of the assault and document in detail the nature of the attack, method of attack, potential target data, and access points. Inform all key stakeholders about the assault, including management, IT personnel, and staff, and give them with information on how to safeguard their systems and personal safety. Proper advice for changing passwords immediately and enhancing security with two-factor authentication should be followed to reduce the danger of future possible assaults [17]. Appropriate analysis should be conducted to correct security rules and processes when vulnerabilities were exploited and an attack occurred. It is critical to monitor recent attacks on computers and networks for any indications of malicious activity or attacks. It is recommended that a cybersecurity specialist be brought in to assess the organization's security state and give recommendations for improving the security posture. These measures will ensure that a successful company resists a social engineering attack and is protected from a similar attack in the future.

5. CONCLUSION

Based on the foregoing, the project believes that one defined metric will most likely not be sufficient to oppose social engineering, which is becoming increasingly dangerous. As a result, companies and individuals can collaborate to create a definition through user education, solid security standards, technology solutions, and an awareness culture. Furthermore, for the reasons stated, ongoing monitoring of trends in social engineering and adjustments in ways to define is critical for staying ahead of cybercriminals. By using a multilayered approach and remaining vigilant against social engineering assaults, we can preserve our precious information in this digital age. If you feel your company has been the victim of a social engineering attack, take the following measures to resolve the situation and reduce the likelihood of future attacks. Identify the source of the attack and gather thorough information about it, including the type of the attack, the mechanism utilized to carry it out, and any possibly affected data or access points [18]. Notify all relevant stakeholders about the attack, including executives, IT professionals, and employees, and provide them with information on how to protect their systems and personal safety. To reduce the risk of future attacks, update any compromised passwords as soon as possible and strengthen security by using additional measures such as two-factor authentication. Analyze and adjust security policies and procedures to address any flaws that may have assisted the attack. Keep a close eye out for signs of recent attacks or malicious activity on computer systems and networks. It is best to employ a cybersecurity specialist to do a full review of the organization's security posture and make recommendations for improving security procedures. Implementing these tactics allows an organization to effectively repel a social engineering attack while also helping to prevent future attacks of the same type.

References

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. Journal of Applied Security Research, 20(2), 244-292.

Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures. arXiv preprint arXiv:2408.02092.

Zaoui, M., Yousra, B., Yassine, S., Yassine, M., & Karim, O. (2024). A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Towards Effective Mitigation Strategies. IEEE Access.

Fakhouri, H. N., Alhadidi, B., Omar, K., Makhadmeh, S. N., Hamad, F., & Halalsheh, N. Z. (2024, February). Ai-driven solutions for social engineering attacks: Detection, prevention, and response. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-8). IEEE.

Pakina, A. K., Kejriwal, D., & Pujari, T. D. (2025). Adversarial AI in Social Engineering Attacks: Large-Scale Detection and Automated Counter measures. International Journal Science and Technology, 4(1), 1-11.

Alahmed, Y., Abadla, R., & Al Ansari, M. J. (2024, September). Exploring the Potential Implications of AI-generated Content in Social Engineering Attacks. In 2024 International Conference on Multimedia Computing, Networking and Applications (MCNA) (pp. 64-73). IEEE.

Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI's Revolutionary Role in Cyber Defense and Social Engineering. International Journal of Multidisciplinary Sciences and Arts, 3(4), 57-66.

Kontogeorgopoulos, K., & Kritikos, K. (2024). Overview of social engineering protection and prevention methods. In European Symposium

on Research in Computer Security (pp. 64-83). Springer, Cham.

Lundie, M., Lindke, K., Amos-Binks, A., Aiken, M. P., & Janosek, D. (2024, January). The Enterprise Strikes Back: Conceptualizing the HackBot-Reversing Social Engineering in the Cyber Defense Context. In HICSS (pp. 984-993).

Okika, N., Okoh, O. F., & Etuk, E. E. (2025). Mitigating Insider Threats and Social Engineering Tactics in Advanced Persistent Threat Operations through Behavioral Analytics and Cybersecurity Training. International Journal of Advance Research Publication and Reviews, 2(3), 11-27.

Bell, C., Egon, A., & Broklyn, P. (2024). Social Engineering in The Age of Disinformation: A Multimodal Approach to Detection and Prevent. Available at SSRN 4904945.

Ai, L., Kumarage, T., Bhattacharjee, A., Liu, Z., Hui, Z., Davinroy, M., ... & Hirschberg, J. (2024). Defending against social engineering attacks in the age of llms. arXiv preprint arXiv:2406.12263.

Abdelhamid, R. K., & Maqableh, M. (2024). The power of persuasion: Exploring social engineering in the digital age. In Current and Future Trends on Intelligent Technology Adoption: Volume 2 (pp. 307-330). Cham: Springer Nature Switzerland.

Yu, J., Yu, Y., Wang, X., Lin, Y., Yang, M., Qiao, Y., & Wang, F. Y. (2024). The Shadow of Fraud: The Emerging Danger of AI-powered Social Engineering and its Possible Cure. arXiv preprint arXiv:2407.15912.

Dsouza, D. S., Hajjar, A. E., & Jahankhani, H. (2024). Deepfakes in Social Engineering Attacks. In Space Law Principles and Sustainable Measures (pp. 153-183). Cham: Springer Nature Switzerland.

Adekunle, T. S., Lawrence, M. O., Alabi, O. O., Ebong, G. N., Ajiboye, G. O., & Bamisaye, T. A. (2024). The use of ai to analyze social media attacks for predictive analytics. American Journal of Operations Management and Information Systems, 9(1), 17-24.

Ciupe, A., & Orza, B. (2024, May). Reinforcing cybersecurity awareness through simulated phishing attacks: Findings from an hei case study. In 2024 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-4). IEEE.

Burton, S. L., & Moore, P. D. (2024). Pig butchering in cybersecurity: A modern social engineering threat. SocioEconomic Challenges, 8(3), 46.