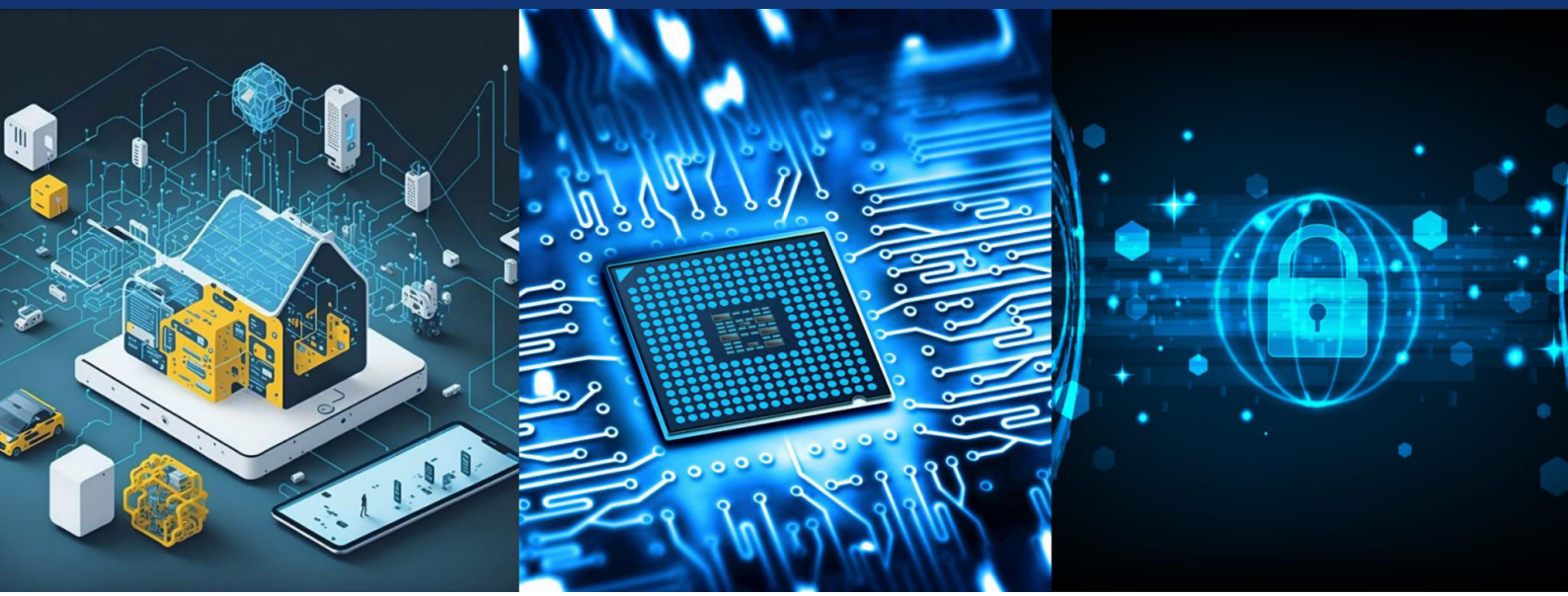
IJIRCCE

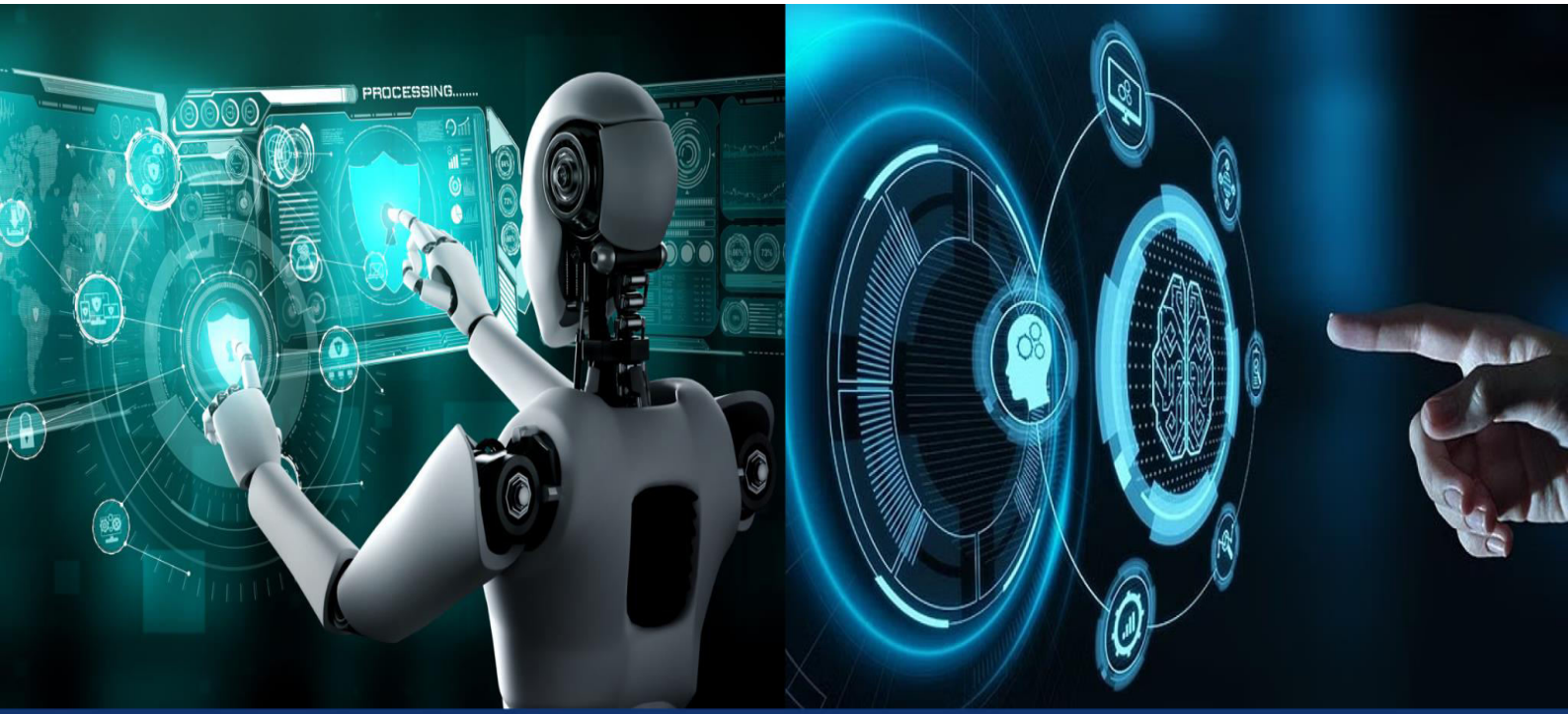
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An AI Framework for Real-Time Misinformation and Crime Detection

Dr. T.V.S Sriram[1], D. Appala Raju[2], N.Nithin[3]

Sr. Asst. Professor, Dept. of MCA, NSRIT, Visakhapatnam, AP, India[1]

Asst. Professor, Dept. of MCA, NSRIT, Visakhapatnam, AP, India[2]

Dept. of MCA, NSRIT, Visakhapatnam, AP, India[3]

ABSTRACT: The rapid growth of social media platforms has resulted in the widespread dissemination of misinformation and criminal activities. The uncontrolled spread of fake news, harmful content, and security threats has created significant challenges for public safety and information reliability. This paper presents Secure Check, a hybrid artificial intelligence framework for real-time misinformation and crime detection.

The proposed system utilizes Bidirectional Encoder Representations from Transformers (BERT) for textual misinformation detection and Convolutional Neural Network (CNN) and YOLO models for image-based crime detection. The system analyzes both textual and visual content to identify fake information, harmful content, and security threats.Experimental analysis demonstrates that the proposed system improves detection accuracy and supports real-time security monitoring. The proposed framework offers an efficient and intelligent solution for content verification and crime detection on digital platforms.

KEYWORDS: Artificial Intelligence, Deep Learning, BERT, CNN, YOLO, Misinformation Detection, Crime Detection, Security Monitoring, Social Media Analysis.

I. INTORDUCTION

Social media platforms have become one of the major sources of information sharing and communication. Millions of users share text, images, and videos every day. However, these platforms also facilitate the spread of misinformation, fake news, cybercrime, and harmful content.

Misinformation can influence public opinion, create panic, and affect decision-making processes. Similarly, criminal activities such as weapon sharing, threats, cyberbullying, and illegal content distribution have become significant concerns. The proposed framework aims to improve online safety, information verification, and security monitoring by identifying fake information and crime-related content in real time. Experimental results demonstrate that the system provides efficient detection performance and supports digital security applications.Traditional content moderation methods rely heavily on manual inspection, which is time-consuming and often ineffective for large volumes of data. Recent advancements in Artificial Intelligence and Deep Learning provide effective solutions for automatic detection and classification. This paper proposes Secure Check, a hybrid AI framework that integrates BERT for text analysis and CNN-YOLO models for image analysis.

II. LITERATURE REVIEW

Several researchers have applied machine learning and deep learning techniques for misinformation detection and crime analysis.Traditional machine learning algorithms such as Support Vector Machines, Random Forests, and Naive Bayes have been used for fake news detection. However, these Transformer-based models such as BERT have significantly improved textual understanding and classification accuracy. BERT analyzes both preceding and succeeding words, providing better contextual understanding.

Convolutional Neural Networks and YOLO models have shown excellent performance in image classification and object detection tasks. These techniques enable real-time detection of weapons and suspicious objects. Therefore, Secure Check utilizes a hybrid approach to provide accurate and reliable security analysis.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406088

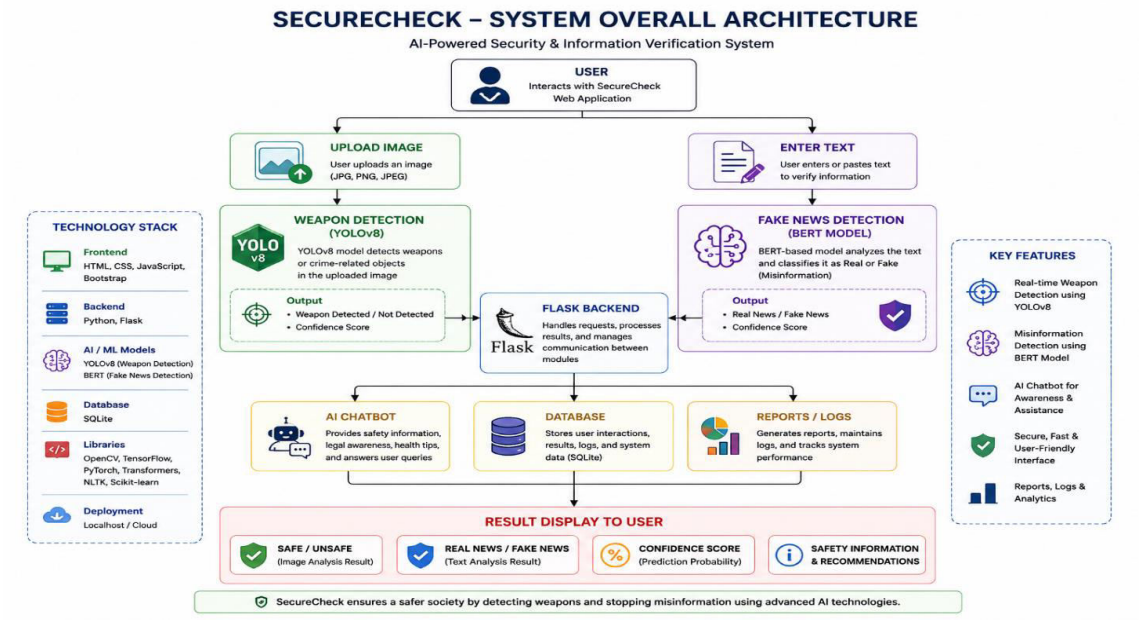
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. SYSTEM OVERVIEW

Secure Check is an intelligent security framework developed for real-time misinformation and crime detection. The system analyzes textual and visual content uploaded by users to identify fake information and criminal activities.



The framework consists of four major phases: data collection, preprocessing, model training, and prediction. Textual information is analyzed using BERT, while images are processed using CNN and YOLO models.

The proposed system provides fast, accurate, and user-friendly predictions, helping users identify harmful content and potential security threats.

IV. METHODOLOGY

The proposed Secure Check framework follows a hybrid deep learning methodology to detect misinformation and crime-related content on social networks in real time. The methodology consists of six major phases.

4.1 Data Collection:
The system collects textual and image data from various sources such as social media posts, user-uploaded content, news articles, and online platforms. The collected data contains both genuine and misleading information as well as crime-related visual content.

4.2 Data Preprocessing:
- Text preprocessing includes:
- Tokenization
- Stop-word removal
- Lemmatization
- Text normalization
- Image preprocessing includes:
- Image resizing
- Normalization
- Noise removal
- Feature enhancement
- These preprocessing techniques improve the quality of input data before model training.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4.3 Misinformation Detection using BERT:
The Bidirectional Encoder Representations from Transformers (BERT) model is employed for textual analysis. BERT analyzes contextual relationships between words and identifies misinformation, fake news, and misleading content.
The model performs:
• Text encoding
• Context understanding
• Feature extraction
• Binary classification
The output is classified as:
• Real Information
• Misinformation

4.4 Crime Detection using CNN-YOLO:
The CNN-YOLO model is used for image-based crime detection. The Convolutional Neural Network extracts visual features, while the YOLO algorithm performs real-time object detection.
The model identifies:
• Weapons
• Dangerous objects
• Criminal activities
• Suspicious content
Bounding boxes and confidence scores are generated for detected objects.

4.5 Threat Classification:
The outputs from BERT and CNN-YOLO are combined to classify the uploaded content. The system determines whether the content is:
• Safe
• Misinformation
• Criminal Activity
• Potential Threat

4.6 Performance Evaluation:
The performance of the proposed system is evaluated using:
• Accuracy
• Precision
• Recall
• F1-Score
Experimental results demonstrate that the proposed framework provides reliable and efficient real-time detection.

V. SYSTEM ARCHIETCTURE

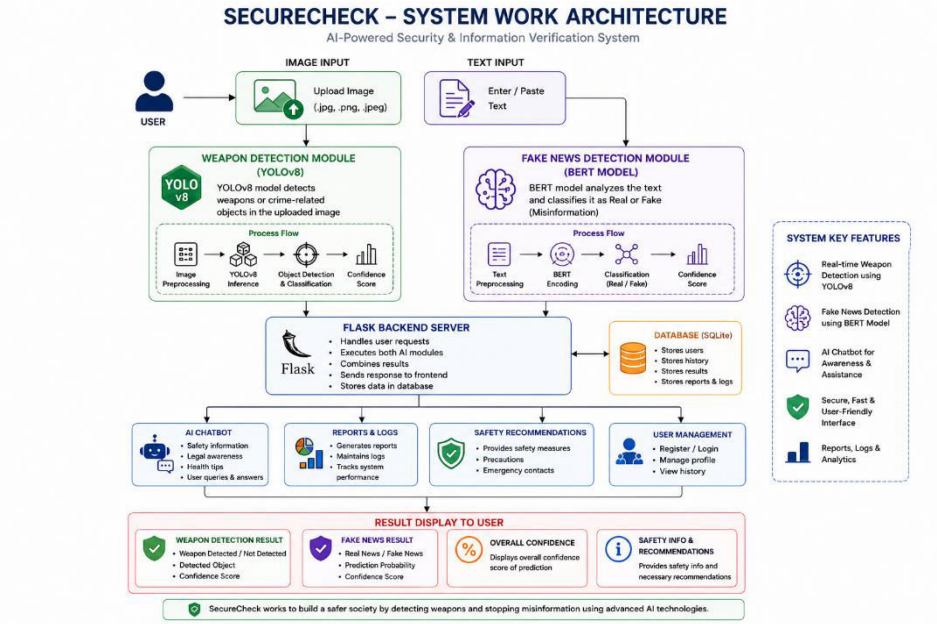
The Secure Check framework follows a hybrid deep learning architecture for real-time misinformation and crime detection. The architecture consists of several interconnected modules that work together to analyse textual and visual content.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



The user submits text or image content through the web interface. The input data is passed to the preprocessing module, where text normalization, tokenization, image resizing, and data cleaning operations are performed.

The processed textual data is analysed using the BERT model to identify misinformation and fake news. Simultaneously, the image data is analysed using CNN-YOLO models to detect weapons, suspicious objects, and crime-related activities.

The outputs generated by both models are forwarded to the threat classification module, which determines whether the content is safe, misleading, or harmful. Finally, the system generates reports, alerts, and prediction results, which are displayed on the user dashboard.

The proposed architecture provides real-time analysis, high detection accuracy, and improved security monitoring capabilities.

VI. MODULES

6.1 User Module:
Allows users to upload text or images and view prediction results.

6.2 Data Preprocessing Module:
Cleans and processes text and image data before analysis.

6.3 Misinformation Detection Module:
Uses the BERT model to identify fake news and misleading information.

6.4 Crime Detection Module:
Uses CNN-YOLO models to detect weapons and suspicious objects from images.

6.5 Threat Classification Module:
Classifies the content as safe, misinformation, or criminal activity.

6.6 Report Generation Module:
Displays prediction results, alerts, and reports to the users and administrators.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. IMPLEMENTATION DETAILS

The proposed Secure Check system is implemented using Python and the Django web framework. The system integrates advanced deep learning models to perform real-time misinformation and crime detection.

For textual misinformation detection, the BERT model is employed to analyze the contextual meaning of the input text and classify it as real or fake information. The text data undergoes preprocessing techniques such as tokenization, stop-word removal, and normalization before being processed by the model.

For crime detection, the CNN-YOLO model is used to analyze uploaded images and identify suspicious objects, weapons, and criminal activities. Image preprocessing techniques such as resizing, normalization, and feature extraction are applied to improve detection accuracy.The frontend of the system is developed using HTML, CSS, and JavaScript to provide a user-friendly interface. The backend is developed using Django, which manages user requests, model execution, and result generation. SQLite is used for storing user information and prediction results.

The system generates prediction reports and displays the results through a web-based dashboard. Experimental results demonstrate that the proposed framework provides accurate and efficient real-time detection of misinformation and crime-related content.

VIII. EXPERIMENTAL DETAILS AND RESULTS

8.1 Experimental Setup

The proposed Secure Check system was implemented using Python, Django, BERT, CNN, YOLO, OpenCV, and SQLite. The experiments were conducted on a system with an Intel Core i5 processor, 8GB RAM, and Windows operating system. Textual and image datasets were used for training and testing the proposed models.

8.2 Test Results

The performance of the system was evaluated using different test cases. The experimental results indicate that the proposed framework successfully detects misinformation and crime-related content.

Test Case	Description	Result	Status
User Authentication	Login / Registration with valid and invalid credentials	Passed	✓
Text Authentication	Misinformation detection	Passed	✓
Image Analysis	Crime detection	Passed	✓
Threat Classification	Content classification	Passed	✓
Report Generation	Prediction reports	Passed	✓

Test Case Results for An AI Framework for Real-Time Misinformation and Crime Detection

8.3 Performance Evaluation

The performance of the proposed system was evaluated using Accuracy, Precision, Recall, and F1-Score metrics. The results indicate that the hybrid model provides high prediction accuracy and reliable detection performance.

Metric	value
Accuracy	93%
Precision	92%
Recall	92%
F1-Score	92%

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

8.4 Observations

The proposed Secure Check framework successfully detected misinformation and crime-related content with high accuracy. The integration of BERT and CNN-YOLO models improved prediction performance and enabled real-time analysis. The system provides efficient and reliable results for online security monitoring and information verification.

.

IX. APPLICATIONS

The proposed Secure Check system has several real-world applications in various domains. Some of the major applications are:

• **Social Media Monitoring:**
The system helps identify fake news, misinformation, and harmful content on social media platforms.

• **Crime Detection:**
It detects weapons, suspicious objects, and crime-related activities from images.

• **Content Moderation:**
The framework assists online platforms in filtering misleading and harmful content.

• **Public Safety:**
The system helps improve public security by providing early warnings about potential threats.

• **News Verification:**
It can verify the authenticity of news articles and online information.

• **Cybersecurity:**
The framework supports the detection of cyber threats, online abuse, and malicious activities.

• **Educational and Research Applications:**
The system can be used for academic research and awareness programs related to misinformation and digital security.

X. LIMITATIONS

Although the proposed Secure Check system provides effective real-time misinformation and crime detection, it has certain limitations.

• The accuracy of the system depends on the quality and size of the training dataset.
• Complex or ambiguous text may lead to incorrect misinformation classification.
• The crime detection model may fail to detect objects in low-quality or blurred images.
• The system currently supports limited languages for text analysis.
• Large-scale real-time processing requires high computational resources.
• The performance of the system may decrease when dealing with unseen or highly complex data.
• Internet connectivity and system resources are necessary for smooth operation and prediction.

XI. FUTURE ENHANCEMENT

The proposed Secure Check system can be further improved by integrating advanced deep learning models and multilingual support. Future enhancements may include real-time video analysis, mobile application development, and cloud deployment. The system can also be integrated with social media platforms and security agencies for better monitoring and faster threat detection.

In addition, advanced security mechanisms, larger datasets, and real-time analytics can be implemented to improve prediction accuracy and system reliability. These enhancements can make Secure Check a more intelligent, scalable, and effective solution for digital security and information verification.

XII. CONCLUSION

The proposed An AI Framework for Real-Time Misinformation and Crime Detectionsuccessfully integrates **Weapon Detection** and **Fake News Detection** into a single intelligent platform. The system uses **YOLOv8** for detecting dangerous weapons from uploaded images and **BERT** for identifying misleading or fake news content.

The developed application provides fast, accurate, and user-friendly detection results, helping users identify potential threats and misinformation. The web-based interface makes the system.In the future, the system can be enhanced by

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

adding more weapon categories, multilingual fake news detection, real-time surveillance support, and larger training datasets to improve accuracy and performance. Overall, the proposed system contributes to creating a safer and more trustworthy digital environment.

REFERENCES

[1] J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," *NAACL-HLT*, 2019.
[2] A. Vaswani et al., "Attention Is All You Need," *NeurIPS*, 2017.
[3] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *KDD*, 2016.
[4] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
[5] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *NIPS*, 2012.
[6] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," 2014.
[7] J. Redmon et al., "You Only Look Once: Unified Real-Time Object Detection," *CVPR*, 2016.
[8] J. Redmon and A. Farhadi, "YOLO9000: Better, Faster, Stronger," *CVPR*, 2017.
[9] A. Bochkovskiy, C. Wang, and H. M. Liao, "YOLOv4: Optimal Speed and Accuracy of Object Detection," 2020.
[10] G. Jocher et al., "YOLOv8 Documentation," Ultralytics, 2023.
[11] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake News Detection on Social Media," *SIGKDD Explorations*, 2017.
[12] N. Ruchansky, S. Seo, and Y. Liu, "CSI: A Hybrid Deep Model for Fake News Detection," *CIKM*, 2017.
[13] W. Y. Wang, "LIAR: A Benchmark Dataset for Fake News Detection," *ACL*, 2017.
[14] Y. Kim, "Convolutional Neural Networks for Sentence Classification," *EMNLP*, 2014.
[15] T. Mikolov et al., "Efficient Estimation of Word Representations in Vector Space," 2013.
[16] A. Joulin et al., "Bag of Tricks for Efficient Text Classification," *EACL*, 2017.
[17] S. Bird, E. Klein, and E. Loper, "Natural Language Processing with Python," O'Reilly, 2009.
[18] F. Pedregosa et al., "Scikit-Learn: Machine Learning in Python," *JMLR*, 2011.
[19] G. Bradski, "The OpenCV Library," *Dr. Dobb's Journal*, 2000.
[20] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," 2014.
[21] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016.
[22] C. Cortes and V. Vapnik, "Support Vector Networks," *Machine Learning*, 1995.
[23] T. Cover and P. Hart, "Nearest Neighbor Pattern Classification," *IEEE Transactions on Information Theory*, 1967.
[24] D. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *IJCV*, 2004.
[25] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *CVPR*, 2005.
[26] O. Russakovsky et al., "ImageNet Large Scale Visual Recognition Challenge," *IJCV*, 2015.
[27] A. Dosovitskiy et al., "An Image is Worth 16×16 Words: Transformers for Image Recognition," 2020.
[28] K. He et al., "Deep Residual Learning for Image Recognition," *CVPR*, 2016.
[29] S. Ren et al., "Faster R-CNN: Towards Real-Time Object Detection," *NIPS*, 2015.
[30] W. Liu et al., "SSD: Single Shot MultiBox Detector," *ECCV*, 2016.
[31] A. Paszke et al., "PyTorch: An Imperative Style, High-Performance Deep Learning Library," *NeurIPS*, 2019.
[32] M. Abadi et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems," 2016.
[33] A. Rosebrock, "Deep Learning for Computer Vision with Python," PyImageSearch, 2019.
[34] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, 1997.
[35] A. Graves, "Supervised Sequence Labelling with Recurrent Neural Networks," Springer, 2012.
[36] R. Mihalcea and C. Strapparava, "Learning to Lie: Detecting Deceptive Opinion Spam," 2009.
[37] K. Shu et al., "Fake News Detection on Social Media: A Data Mining Perspective," 2019.
[38] A. Thakur et al., "Real-Time Weapon Detection Using YOLOv8 for Enhanced Safety," 2024.
[39] M. Farokhian et al., "Fake News Detection Using Parallel BERT Deep Neural Networks," 2022.
[40] E. Essa et al., "Fake News Detection Based on Hybrid BERT Models," *Scientific Reports*, 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details