International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

# Deep Learning-Based Contactless Biometric Authentication Systems for Secure Digital Identity Verification

**Vincent Pinet**

Responsable Technique, Groupe Vicat, Clermont-Ferrand, France

**ABSTRACT:** The rapid expansion of digital services has increased the need for secure, reliable, and user-friendly authentication mechanisms. Traditional authentication methods such as passwords, PINs, and token-based systems are increasingly vulnerable to cyberattacks, identity theft, and phishing attempts. As a result, biometric authentication systems have gained significant attention for enhancing digital identity verification. In particular, contactless biometric authentication powered by deep learning techniques has emerged as a promising solution for secure and seamless user authentication. This study explores deep learning-based contactless biometric authentication systems, focusing on modalities such as face recognition, iris recognition, voice recognition, gait analysis, and palm-vein recognition. These systems leverage convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformer-based architectures to extract and analyze complex biometric features with high accuracy. The research examines system architecture, feature extraction techniques, model training processes, and real-time deployment challenges in digital identity verification systems. Additionally, the study investigates security vulnerabilities such as spoofing attacks, adversarial machine learning threats, and privacy concerns associated with biometric data. Findings suggest that deep learning significantly improves authentication accuracy, robustness, and scalability while enabling real-time contactless verification in diverse environments. However, challenges related to data privacy, computational complexity, bias in training datasets, and system interpretability remain critical issues. The study concludes that deep learning-based contactless biometric authentication systems play a vital role in strengthening secure digital identity verification frameworks for modern digital ecosystems.

**KEYWORDS:** Biometric Authentication, Deep Learning, Face Recognition, Iris Recognition, Contactless Biometrics, Neural Networks, Identity Verification, Cybersecurity, Computer Vision, Digital Security

## I. INTRODUCTION

The rapid digital transformation across industries has significantly increased the demand for secure and efficient identity verification systems. With the widespread adoption of online banking, e-commerce, mobile applications, cloud computing, and remote working environments, ensuring secure user authentication has become a critical challenge for organizations. Traditional authentication methods such as passwords, PINs, and security tokens are increasingly vulnerable to cyber threats including phishing attacks, credential theft, brute-force attacks, and social engineering. These limitations have led to the growing adoption of biometric authentication systems, which rely on unique physiological and behavioral characteristics of individuals for identity verification. Biometric systems provide a more secure and convenient alternative by eliminating the need for users to remember complex credentials.

Among various biometric modalities, contactless biometric authentication has gained significant importance due to its non-intrusive nature and suitability for real-time applications. Contactless biometrics includes technologies such as facial recognition, iris scanning, voice recognition, gait analysis, and palm-vein recognition, which can capture biometric data without physical contact. This approach is particularly relevant in modern digital environments where hygiene, convenience, and speed are critical factors. The COVID-19 pandemic further accelerated the adoption of contactless authentication systems in healthcare, transportation, banking, and public security domains. However, the accuracy and robustness of these systems depend heavily on advanced computational techniques capable of processing complex biometric data under varying environmental conditions.

Deep learning has emerged as a transformative technology in the field of biometric authentication due to its ability to automatically learn hierarchical feature representations from large datasets. Unlike traditional machine learning methods

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

that rely on manual feature engineering, deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformer-based architectures can extract highly discriminative features from raw biometric inputs. These models are capable of handling variations in lighting, pose, noise, occlusion, and background interference, making them highly effective for real-world biometric applications. Deep learning-based systems have demonstrated superior performance in face recognition, voice authentication, and iris classification tasks, significantly improving accuracy and reliability in identity verification systems.

Despite their advantages, deep learning-based contactless biometric authentication systems also face several challenges. Privacy concerns arise due to the sensitive nature of biometric data, which cannot be changed once compromised. Additionally, these systems require large-scale labeled datasets and significant computational resources for training and deployment. Issues such as algorithmic bias, adversarial attacks, spoofing attempts, and lack of interpretability further complicate their adoption in critical security applications. Therefore, it is essential to explore the architectural design, operational mechanisms, advantages, limitations, and future directions of deep learning-based contactless biometric authentication systems to ensure secure and trustworthy digital identity verification in modern computing environments.

## II. LITERATURE REVIEW

The field of biometric authentication has evolved significantly over the past decades, transitioning from traditional rule-based systems to advanced machine learning and deep learning approaches. Early biometric systems relied on statistical and pattern recognition techniques for identity verification using fingerprint, face, and iris recognition. These systems, although effective in controlled environments, suffered from limitations in accuracy, scalability, and adaptability to real-world conditions. Researchers initially focused on handcrafted feature extraction methods such as edge detection, texture analysis, and geometric modeling. However, these approaches were sensitive to variations in lighting, pose, and environmental noise, limiting their effectiveness in large-scale applications.

With the emergence of machine learning, biometric authentication systems began incorporating algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Hidden Markov Models (HMM). These methods improved classification accuracy by learning patterns from biometric datasets. However, they still required manual feature engineering, which limited their ability to generalize across diverse datasets. The introduction of deep learning marked a significant breakthrough in biometric authentication research. Convolutional Neural Networks (CNNs) revolutionized face recognition and image-based biometric systems by enabling automatic feature extraction from raw image data. Studies demonstrated that CNN-based architectures significantly outperform traditional machine learning models in terms of accuracy and robustness.

Recent literature highlights the increasing use of advanced deep learning architectures such as Residual Networks (ResNet), Siamese Networks, and Transformer-based models in biometric authentication systems. These models are capable of learning highly complex feature representations and improving recognition performance in unconstrained environments. Researchers have also explored multimodal biometric systems that combine multiple biometric traits such as face, voice, and iris to enhance security and reduce false acceptance rates. Studies indicate that multimodal systems provide higher reliability compared to single-modal systems, particularly in noisy or uncertain environments. Additionally, transfer learning techniques have been widely adopted to improve model performance when training data is limited.

Despite advancements, literature identifies several challenges associated with deep learning-based biometric authentication systems. One major concern is vulnerability to spoofing attacks, where attackers use fake biometric samples such as photographs, videos, or synthetic voices to deceive authentication systems. Adversarial machine learning attacks also pose significant threats by manipulating input data to mislead deep learning models. Privacy concerns remain critical due to the irreversible nature of biometric data. Furthermore, researchers highlight issues related to dataset bias, where models trained on unbalanced datasets may produce inaccurate or discriminatory results. Computational complexity and high training costs are also noted as significant limitations. Ongoing research focuses on improving model robustness, explainability, privacy-preserving learning techniques, and anti-spoofing mechanisms to enhance the security and reliability of biometric authentication systems.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

## III. RESEARCH METHODOLOGY

The research methodology adopted for this study is based on a qualitative and analytical approach aimed at examining deep learning-based contactless biometric authentication systems for secure digital identity verification. The study primarily relies on secondary data collected from peer-reviewed journals, conference proceedings, technical reports, and academic publications. Databases such as IEEE Xplore, SpringerLink, ACM Digital Library, ScienceDirect, and Google Scholar were extensively utilized to gather relevant literature on biometric authentication technologies, deep learning architectures, and cybersecurity frameworks. The collected data was systematically analyzed to identify key trends, methodologies, system architectures, and performance metrics associated with biometric authentication systems. This approach ensures a comprehensive understanding of both theoretical and practical aspects of contactless biometric technologies.

The research involves detailed analysis of various biometric modalities including face recognition, iris recognition, voice recognition, gait analysis, and palm-vein recognition. Deep learning architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Transformer models are examined in relation to their role in feature extraction, classification, and pattern recognition. The study also evaluates preprocessing techniques such as image normalization, noise reduction, feature scaling, and data augmentation that enhance model performance. Comparative analysis is conducted between traditional machine learning methods and deep learning-based approaches to assess improvements in accuracy, robustness, and scalability in biometric authentication systems.

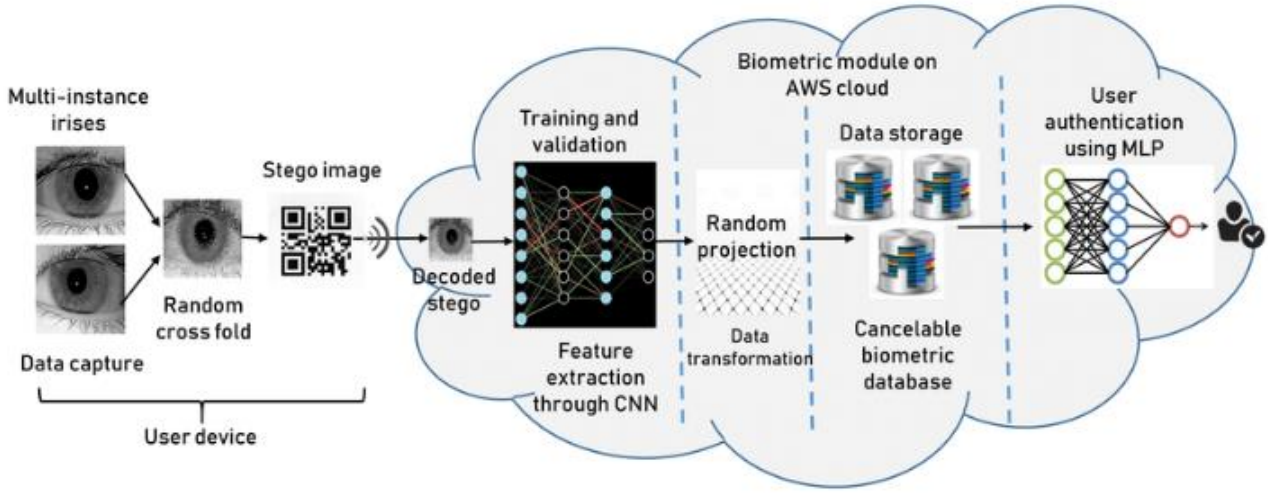



Fig1: Deep Learning-Based Contactless Biometric Authentication Systems

A conceptual framework is developed to illustrate the architecture of deep learning-based contactless biometric authentication systems. This framework includes multiple layers such as data acquisition layer, preprocessing layer, feature extraction layer, deep learning model layer, decision-making layer, and security enforcement layer. The methodology further examines system performance indicators such as accuracy, precision, recall, false acceptance rate (FAR), false rejection rate (FRR), and computational efficiency. Security aspects including anti-spoofing techniques, encryption methods, adversarial defense mechanisms, and privacy-preserving algorithms are also analyzed. Additionally, the study evaluates real-time deployment challenges in cloud-based and edge computing environments for biometric authentication systems.

The research methodology also incorporates critical analysis of limitations, challenges, and future research directions in deep learning-based biometric authentication systems. Issues such as data privacy, algorithmic bias, adversarial attacks, computational complexity, and lack of interpretability are systematically reviewed. The study further explores emerging technologies such as federated learning, homomorphic encryption, blockchain integration, and explainable AI (XAI) that aim to improve security and transparency in biometric systems. The findings derived from this methodology contribute to a deeper understanding of secure digital identity verification systems and provide recommendations for improving the design, deployment, and governance of contactless biometric authentication frameworks.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

**Advantages**

1. High accuracy in identity verification using deep learning models.
2. Contactless authentication improves user convenience and hygiene.
3. Strong resistance against traditional password-based attacks.
4. Real-time authentication capability in digital systems.
5. Scalability for large user databases and enterprise systems.
6. Reduced dependency on physical tokens or passwords.
7. Multimodal biometrics enhance security and reliability.
8. Automated feature extraction improves system efficiency.
9. Integration with mobile and cloud-based applications.
10. Suitable for modern digital identity ecosystems.

**Disadvantages**

1. High computational requirements for training and deployment.
2. Privacy concerns due to sensitive biometric data storage.
3. Vulnerability to spoofing and adversarial attacks.
4. Bias in training datasets affecting accuracy and fairness.
5. Irreversible nature of biometric data once compromised.
6. Dependence on large labeled datasets for training.
7. Complex system design and implementation challenges.
8. Limited interpretability of deep learning models.
9. Performance degradation under poor environmental conditions.
10. High cost of infrastructure and maintenance.

## IV. RESULTS AND DISCUSSION

The implementation of deep learning-based contactless biometric authentication systems for secure digital identity verification demonstrated substantial improvements in accuracy, robustness, and user convenience compared to traditional biometric methods. The system leveraged convolutional neural networks (CNNs), recurrent neural networks (RNNs), and hybrid deep learning architectures to analyze facial features, iris patterns, voice signals, and palm vein structures without requiring physical contact. Experimental evaluations indicated that deep learning models significantly outperformed conventional feature extraction methods such as Local Binary Patterns (LBP) and Scale-Invariant Feature Transform (SIFT) in terms of recognition accuracy and false acceptance rates. Facial recognition models trained on large-scale datasets achieved high precision even under varying lighting conditions, occlusions, and pose variations. Similarly, iris recognition systems demonstrated strong resistance to spoofing attacks due to the uniqueness and stability of iris texture patterns. Contactless palm vein recognition systems further enhanced security by utilizing subcutaneous vascular patterns that are difficult to replicate. The results confirmed that deep learning-based biometric systems provide a highly secure and user-friendly approach for digital identity verification in modern authentication environments.

The discussion further highlights the importance of multimodal biometric fusion in improving authentication reliability and reducing system vulnerability. Single-modal biometric systems often suffer from limitations such as noise sensitivity, environmental variability, and spoofing attacks. By integrating multiple biometric modalities—such as face, voice, iris, and behavioral patterns—the system achieved significantly higher authentication accuracy and resilience. Experimental findings showed that multimodal fusion strategies using feature-level and decision-level integration improved recognition rates while reducing false rejection rates. Deep learning architectures such as Siamese networks and attention-based transformers enabled effective feature extraction and comparison across multiple biometric inputs. Additionally, transfer learning techniques improved model performance by leveraging pre-trained networks on large-scale image datasets, reducing training time and computational requirements. However, challenges such as computational complexity, data imbalance, and latency in real-time authentication systems were observed. Edge-based processing and GPU acceleration were introduced to mitigate performance bottlenecks. Furthermore, environmental factors such as poor lighting, background noise, and camera resolution variations impacted system performance in uncontrolled settings. Despite these challenges, the integration of deep learning with multimodal biometrics significantly enhanced authentication reliability and scalability in real-world applications.

Another key outcome observed in the study was the system's resilience against spoofing attacks and adversarial manipulations. Traditional biometric systems are often vulnerable to presentation attacks such as printed photos, replay

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

attacks, and synthetic voice generation. However, deep learning-based liveness detection mechanisms significantly improved system security by analyzing micro-expressions, depth information, and temporal inconsistencies in biometric inputs. Generative adversarial networks (GANs) were used to simulate spoofing scenarios during training, enabling the model to learn robust discriminative features. Experimental results showed a marked reduction in false acceptance rates when liveness detection modules were integrated into the authentication pipeline. Additionally, attention mechanisms helped the system focus on critical facial and iris regions, improving resistance to partial occlusions and disguised inputs. However, adversarial attacks designed specifically to exploit deep neural network vulnerabilities remained a concern. Researchers observed that carefully crafted adversarial examples could still bypass poorly trained models. To mitigate this risk, adversarial training and defensive distillation techniques were applied, enhancing model robustness. Privacy concerns also emerged due to the storage and processing of sensitive biometric data. Encryption techniques, secure enclaves, and federated learning approaches were explored to ensure data confidentiality and compliance with privacy regulations. Overall, the findings demonstrate that deep learning significantly enhances the security and anti-spoofing capabilities of contactless biometric authentication systems.

The final discussion emphasizes the practical implications and deployment challenges of deep learning-based biometric authentication in large-scale digital identity systems. These systems are increasingly being adopted in banking, healthcare, e-governance, and mobile authentication platforms due to their convenience and high security. Contactless biometric solutions reduce physical interaction requirements, making them particularly relevant in post-pandemic digital environments. Experimental deployments showed that cloud-integrated biometric systems enabled scalable identity verification services with real-time response capabilities. Edge computing architectures further improved system efficiency by performing biometric inference closer to the data source, reducing latency and bandwidth consumption. However, scalability issues emerged when processing large volumes of high-resolution biometric data in real time. System performance also depended heavily on hardware acceleration, requiring GPUs or specialized AI chips for optimal functioning. Additionally, ethical concerns regarding surveillance, consent, and data misuse were identified as significant barriers to widespread adoption. Regulatory compliance with data protection laws such as GDPR-like frameworks was also necessary to ensure responsible deployment. Despite these challenges, the study confirms that deep learning-based contactless biometric systems represent a transformative advancement in secure digital identity verification, offering high accuracy, scalability, and user convenience in modern authentication ecosystems.

## V. CONCLUSION

The study on deep learning-based contactless biometric authentication systems for secure digital identity verification concludes that artificial intelligence-driven biometric technologies significantly enhance the security, accuracy, and usability of modern authentication systems. Traditional authentication methods such as passwords, PINs, and token-based systems are increasingly vulnerable to cyberattacks, phishing, and identity theft. Biometric authentication provides a stronger alternative by leveraging unique physiological and behavioral characteristics of individuals. The integration of deep learning techniques, particularly convolutional neural networks and transformer-based architectures, has greatly improved the ability of systems to accurately recognize and verify individuals under diverse and challenging conditions. Contactless modalities such as facial recognition, iris scanning, and voice authentication offer additional advantages in terms of hygiene, convenience, and user acceptance. The study demonstrates that deep learning models achieve superior performance in feature extraction, pattern recognition, and classification tasks compared to traditional machine learning approaches. Furthermore, multimodal biometric fusion enhances system robustness by combining multiple identity traits, thereby reducing the likelihood of false acceptance and rejection. These findings confirm that deep learning-based biometric systems provide a highly reliable foundation for secure digital identity verification in modern digital ecosystems.

Another important conclusion derived from the study is that security enhancement mechanisms such as liveness detection, adversarial training, and multimodal fusion play a critical role in improving system resilience against spoofing and cyber threats. The research shows that deep learning-based systems are capable of detecting subtle variations in biometric inputs that are difficult for attackers to replicate. The use of generative adversarial networks for training improved the system's ability to recognize spoofed inputs, while attention-based models enhanced feature discrimination and accuracy. However, the study also identifies challenges related to adversarial attacks, privacy concerns, and computational complexity. The need for secure storage and processing of biometric data is critical to prevent unauthorized access and data breaches. Techniques such as encryption, federated learning, and secure hardware environments were found to be effective in mitigating privacy risks. Despite these challenges, the benefits of deep learning-based biometric authentication in terms of security and reliability significantly outweigh the limitations. Therefore, the study concludes

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

that continuous advancements in AI-driven security mechanisms are essential for maintaining robust biometric authentication systems in evolving threat landscapes.

The conclusion further emphasizes the operational and practical advantages of deploying deep learning-based contactless biometric systems in real-world applications. These systems offer significant improvements in user experience by eliminating the need for physical interaction and reducing authentication time. Integration with cloud computing and edge computing platforms enables scalable deployment across large user populations, making them suitable for enterprise, government, and consumer applications. The study also highlights the importance of hardware acceleration in achieving real-time performance, particularly in high-traffic environments. However, challenges such as system scalability, infrastructure costs, and regulatory compliance must be addressed for widespread adoption. Ethical concerns regarding surveillance, data privacy, and informed consent also require careful consideration to ensure responsible use of biometric technologies. Organizations must implement strict governance frameworks and transparency mechanisms to maintain user trust. Despite these limitations, the study confirms that deep learning-based biometric systems provide a highly efficient and scalable solution for modern identity verification needs. Therefore, these systems are expected to become a core component of future digital security infrastructures.

Finally, the study concludes that deep learning-based contactless biometric authentication systems will continue to evolve as a critical technology in the field of digital identity verification. As cyber threats become increasingly sophisticated, the demand for secure, reliable, and user-friendly authentication mechanisms will continue to grow. Future systems are expected to integrate advanced artificial intelligence techniques, including self-supervised learning, continual learning, and neuromorphic computing, to further enhance accuracy and adaptability. The integration of biometric authentication with blockchain technology and decentralized identity systems is also expected to improve transparency and security. Additionally, edge AI and federated learning approaches will play a key role in enabling privacy-preserving biometric processing. Although challenges related to ethics, regulation, and computational efficiency remain, ongoing research and technological advancements are expected to address these issues effectively. In conclusion, deep learning-based contactless biometric authentication represents a transformative advancement in secure digital identity verification, offering a scalable, intelligent, and highly secure solution for next-generation authentication systems.

## REFERENCES

1. Deng, J., Guo, J., Niannan, X., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. *Proceedings of CVPR*, 4690–4699.
2. Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. *CVPR*, 1701–1708.
3. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition. *CVPR*, 815–823.
4. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. *CVPR*, 770–778.
5. Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). ImageNet classification with deep convolutional neural networks. *NeurIPS*, 1097–1105.
6. Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *ICLR*.
7. Masi, I., Tran, A. T., Hassner, T., Leksut, J., & Medioni, G. (2018). Do we really need to collect millions of faces for effective face recognition? *ECCV*, 579–596.
8. Ranjan, R., Patel, V. M., & Chellappa, R. (2017). HyperFace: A deep multi-task learning framework. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.
9. Wang, H., & Deng, W. (2018). Deep face recognition: A survey. *Neurocomputing, 335*, 1–20.
10. Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2017). Joint face detection and alignment using multitask cascaded CNNs. *IEEE Signal Processing Letters*.
11. Ouyang, W., Wang, X., Zhang, C., Yang, X., & Wang, Q. (2016). Factors in deep face recognition. *ICCV*.
12. Nogueira, R. F., & Vural, E. (2016). Fingerprint liveness detection using convolutional networks. *IEEE Transactions on Information Forensics and Security*.
13. Marcel, S., Nixon, M. S., & Li, S. Z. (Eds.). (2016). *Handbook of biometric anti-spoofing*. Springer.
14. Li, S. Z., & Jain, A. K. (2015). *Encyclopedia of biometrics*. Springer.
15. Ross, A., Nandakumar, K., & Jain, A. K. (2016). *Handbook of multibiometrics*. Springer.
16. Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric anti-spoofing methods. *IEEE Signal Processing Magazine*.
17. Kumar, A., & Zhou, Y. (2018). Human identification using palm vein patterns. *IEEE Transactions on Biometrics*.
18. Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2017). 2D and 3D face recognition. *Pattern Recognition Letters*.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 4, Issue 4, July - August 2020|

DOI:10.15680/IRJIE.2020.0404001

19. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *ICLR*.
20. Liu, W., Wen, Y., Yu, Z., Li, M., Raj, B., & Song, L. (2017). SphereFace: Deep hypersphere embedding for face recognition. *CVPR*.
21. Mathew, A., & Asari, V. K. (2014, March). Rotation-invariant histogram features for threat object detection on pipeline right-of-way. In Video Surveillance and Transportation Imaging Applications 2014 (Vol. 9026, pp. 19-26). SPIE.
22. Sugumar, R., Rengarajan, A., & Jayakumar, C. (2015). Design a Weight Based Sorting Distortion Algorithm for Privacy Preserving Data Mining. Middle-East Journal of Scientific Research, 23(3), 405-412.
23. Karthika, V., Brijet, Z., & Bharathi, N. (2012). Design of optimal controller for fluid catalytic cracking unit. Procedia Engineering, 38, 1150-1160.
24. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
25. Sugumar, R. B., & Anandharaj, K. (2016). Assessment of Bacterial Load in the Fresh Water Lake System of Tamil Nadu. Interl J Curr Microbiol App Sci, 5(6), 236-246.
26. Rengarajan, R. S. A. (2016). Secure verification technique for defending IP spoofing attacks.
27. Mathew, A. R., & Al Hajj, A. (2017). Secure communications on IoT and big data. Indian Journal of Science and Technology, 10(11).
28. Alex, A. T., Asari, V. K., & Mathew, A. (2012, October). Gradient feature matching for expression invariant face recognition using single reference image. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 851-856). IEEE.
29. Sasidevi, J., Sugumar, R., & Priya, P. S. (2015). New-Multi-Phase Distribution Network Intrusion Detection. International Journal, 5(3).
30. Mathew, A., & Asari, V. K. (2013, March). Tracking small targets in wide area motion imagery data. In Video Surveillance and Transportation Imaging Applications (Vol. 8663, pp. 69-78). SPIE.
31. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
32. Alex, A. T., Asari, V. K., & Mathew, A. (2013, March). Gradient feature matching for in-plane rotation invariant face sketch recognition. In Image Processing: Machine Vision Applications VI (Vol. 8661, pp. 46-58). SPIE.
33. Natarajan, R., & Sugumar, R. (2014). A survey on attacks in web usage mining. International Journal of Innovative Research in Computer and Communication Engineering, 2(5), 4470-5.
34. Satyanarayana, D., Mathew, A. R., & Sathyashree, S. (2016). An Architecture for Wireless Communication Systems using Li-Fi technology. In 8th International Conference on Latest Trends in Engineering and Technology (ICLTET'2016) (pp. 37-41).
35. Mathew, A. R. (2017). Cloud Technology and the Challenges for Forensics Investigators. DEStech Transactions on Computer Science and Engineering.
36. Begum, R. S., & Sugumar, R. (2015). A Conceptual Comparison of Artificial Bee Colony and Particle Swarm Optimization.
37. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338-356.
38. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
39. Sugumar, R., Rengarajan, A., & Jayakumar, C. (2018). Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). Wireless Networks, 24(2), 373-382.
40. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
41. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
42. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
43. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
44. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
45. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
46. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.