A Next-Generation Biometric Identity-Based Encryption Model for Cloud Security

Rehna R S, S Maria Celestin Vigila
Department of Computer Science & Engineering, Noorul Islam Center for Higher Education, Kumaracoil, Tamilnadu, India
rsrehna@gmail.com, celestinvigila@gmail.com

ABSTRACT

There are still many issues with safeguarding the use of private information on cloud platforms due to our reliance on traditional encryption methods. Both RSA, AES, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are slow because they require costly computations and complex key systems. A biometric-assisted cryptographic system is to be developed to overcome current security challenges by integrating fingerprint verification with Identity-Based Encryption (IBE). The use of these approaches reduces the power required by the system, speeds up entry, and makes it safer to use. The system can resist security attacks and protect users' privacy by repelling replay and brute-force attacks. The performance evaluation shows that IBE is faster in terms of encrypting (40 ms), decrypting (45 ms), and generating keys (50 ms) than either RSA (150 ms), or ABE (60 and 65 ms). The proposed method causes 30% less work than RSA and ABE. RSA needs 80% while ABE has 50% as well. The biometric-assisted IBE system is safe and scalable as it can replace basic cryptography in securing cloud data and authenticating users as shown by these research findings.

Keywords: *Secure access control, identity-based encryption, biometric authentication, cloud data protection, and computing efficiency.*

1. Introduction

The rapid growth of cloud computing caused issues about how to ensure the security of sensitive data storage and access [1]. In traditional encryption methods, sensitive data are usually secured by using complicated key management schemes [2]. These key management schemes may cause many problems such as high computational overhead, leak of secret keys and unauthorized access [3]. Attribute-Based Encryption (ABE) [4], mainly Ciphertext-Policy ABE (CP-ABE) is a preferred system for the secure sharing of data in the cloud among many users [5]. Although CP-ABE was used successfully, it still had some problems such as inefficient key sharing, non-scalability [6] and increasing costs of decryption [7] that stopped it being used for real-time security sensitive systems.

Biometric authentication has got more focus as a safe way to add to safety because it is different for each person and passwords can be taken [8]. Biometrics can be used with cryptography to make it more restrictive and to strengthen the authenticity of it [9]. However, storing the real biometric data along with its transmission and the extraction by portable devices are a major concern related to privacy and spoofing attacks [10]. To address this, we propose a biometric-based cryptosystem which embeds the fingerprint verification scheme in IBE. IBE avoids the necessity for key distribution and maximizes overall efficiency by enabling encryption and decryption with specialized identities, in contrast to Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which relies on pre-established policies.

The main contributions of this work are the development of a biometric-aided cryptosystem incorporating fingerprint authentication and Identity-Based Encryption (IBE) to provide protected cloud data storage, enhanced efficiency in key management and encryption through the avoidance of CP-ABE complexities and utilization of identity-based encryption, and incorporation of robust security features that can withstand brute-force attacks, replay attacks, as well as biometric spoofing. Furthermore, the paper provides an in-depth performance comparison exhibiting reduced computational overhead and improved encryption performance over CP-ABE-based solutions. The rest of this paper is structured as follows: A summary of previous research on biometric cryptography and authentication is provided in Section 2, followed by a description of the suggested biometric-based encryption scheme in Section 3, a security and performance analysis in Section 4, and recommendations for further research in Section 5.

2. Literature Review

A literature review is an essential component of this study, as it identifies the existing challenges, approaches, and advancements in the field of biometric-driven encryption. It provides a clear representation of traditional cryptographic schemes such as RSA, AES, and CP-ABE, along with their limitations, particularly in key management and computational cost. By reviewing the constraints of CP-ABE over cloud systems, this research places Identity-Based Encryption (IBE) as a more effective alternative. Additionally, the criticism supports the selection of appropriate performance metrics to evaluate the effectiveness of encryption and its susceptibility to security breaches. Overall, it enhances the scientific rigor of the work and provides the basis for developing an efficient and secure biometric-enhanced encryption scheme specific to cloud security.

Suresh et al[11].(2022) proposed an asymmetric model of cryptography to solve the age-old problem of private key storage. Their solution dynamically generates key pairs by combining fingerprint biometrics with user passwords. A grey-code technique was applied to transform a secure binary sequence based on the minutiae distances and Reed–Solomon error correction was used to improve stability. XORing the fingerprint-based string (after hashing) with the hashed password yielded a secure seed for RSA key generation. This method did not need the storage of the private key, making it both secure and repeatable in the key creation process.

Sridevi Sathya Priya et al[12]. (2023) in another study analysed the function of cryptography within biometric security with special emphasis on AES encryption. They produced a 128-bit cryptographic key from fingerprint and iris biometrics by extracting and fusing features together. Both fingerprint and iris data were needed for authentication, using a fuzzy commitment scheme to fuse the modalities. The generated key was subjected to randomness tests, which confirmed its stability and randomness, with a p-value less than 1. The AES protocol was utilized to encrypt and decrypt the biometric key to maintain strong and uniform protection. Similarly, Suyal et al. [13] proposed a framework that uses dual-layer encryption, combining ABE and symmetric encryption, to ensure the privacy of crowd workers in the cloud.

Jebrane et al[14]. (2024) spoke about the embedding of IoT technologies into healthcare, especially in Internet of Medical Things (IoMT) applications, where low computational power increases security vulnerabilities. Classical authentication protocols were found susceptible to impersonation and replay attacks. To bypass these, the researchers improved ILAPU-Q by incorporating CP-ABE for access control, thereby eliminating the need for dedicated storage. AVISPA and BAN Logic security validation played out resistance against primary attack vectors, and the performance test showed efficiency gains ranging from 95–98%. This development further enhances the security of IoMT systems, enhancing the reliability of telemedicine platforms and protecting patient data. The contribution highlights the continuing need for efficient cryptographic models tailored for sensitive healthcare applications [15,16].

3. Research Methodology

The proposed biometric-enabled cryptosystem combines fingerprint authentication with Identity-Based Encryption (IBE) to strengthen cloud security. The approach employs a structured, multi-phase encryption and decryption procedure that ensures secure data storage, effective access control, and resilience against potential attacks. The essential stages of the framework are outlined below with supporting mathematical formulations, and **Figure 1** illustrates the sequential workflow of the biometric-driven encryption model.

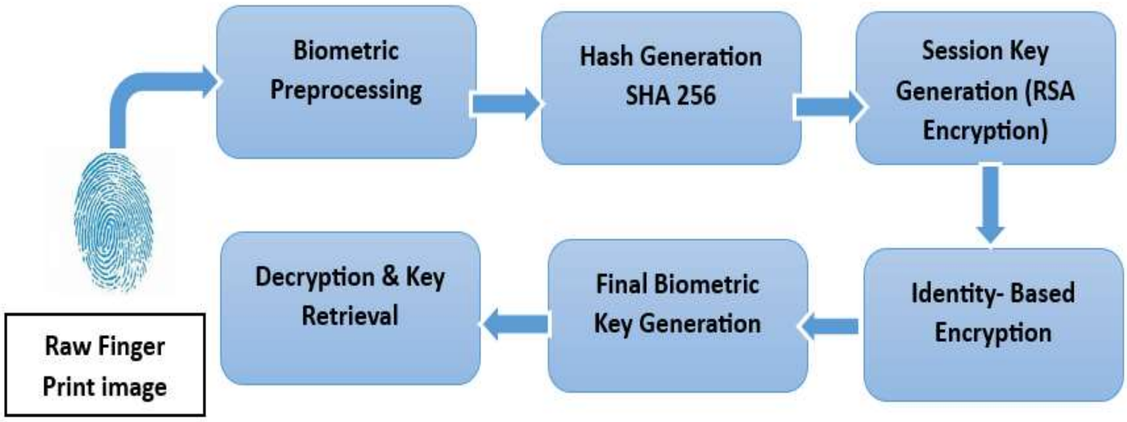

Figure 1: Biometric-driven Encryption model

3.1 Biometric Data Preprocessing

Before feature extraction, the fingerprint image is preprocessed to improve its quality and enhance ridge structures. To make ridge patterns clearer, filters such as the Gabor filter are applied. The Gabor filter is mathematically expressed as:

$$G(x,y) = exp\left(-\frac{x'^2+\gamma^2 y'^2}{2\sigma^2}\right) cos(2\pi f x' + \varphi) \quad (1)$$

Where $x' = x\, cos\theta + y\, sin\theta\ and\ y' = -x\, sin\theta + y\, cos\theta.$

Binarization: The enhanced image is converted into a binary form to clearly distinguish ridges from valleys.

$$B(x,y) = \begin{cases} 1, & if I(x,y) > T \\ 0, & otherwise \end{cases}$$

(2)

Where, I (x, y) is the grayscale pixel intensity and T denotes the threshold value.

Minutiae Extraction: This step identifies distinctive fingerprint details such as ridge endings and bifurcation points. The detection mechanism is described as:

$$CN = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i+1}| \quad (3)$$

Where, P_i corresponds to pixel values in a 3 x 3 neighborhood.
From the extracted minutiae points, a feature vector is generated for subsequent processing. It is represented as:

$$F = \{(x_i, y_i, \theta_i)\}_{i=1}^{n}$$

(4)
Where, x_i, y_i are the spatial coordinates and θ_i represents ridge orientation.

3.2 Hash Generation

To ensure secure representation of the biometric data. Min-Max scaling is used for normalization ,which normalizes values between 0 and 1.

$$F' = \frac{F - min(F)}{max(F) - min(F)}$$

(5)
Hashing: The normalized feature vector is hashed using SHA-256 to generate a fixed-length secure hash.

$$H = SHA256(F') \qquad (6)$$

3.3 Session Key Generation

A temporary session key is produced to improve security, and it is established with the help of RSA encryption.

$$K_s = E_{RSA}(H, k_p)$$

(7)
Where, k_p is RSA public key, and encryption follows:

$$C = M^e \, mod \, N$$

(8)
Where, M is the message, e is the public exponent, and n=pq (product of two prime)

3.4 Identity Based Encryption Setup

The encryption is handled through Identity-Based Encryption (IBE), which makes key distribution easier. A trusted authority is responsible for creating the system parameters and the master secret key. In this approach, user identities such as email addresses or biometric identifiers serve directly as encryption keys, removing the necessity for complicated key management procedures.

$$SK_{ID} = H_1(ID)^{MSK} modp$$

(9)

Where, ID is the user identity, H_1 is a hashfunction, and p is a prime.
The biometric hash and session key are encrypted using IBE for secure cloud storage.

$$C = E_{IBE}(M, ID) \tag{10}$$

3.4 Final Biometric Key Generation

To improve the robustness of biometric security, extra transformation steps are introduced. One such method is the combination of an XOR operation with bitwise rotation, which further reinforces the protection of the biometric hash.

$$K_f = (K_s \oplus H) <<< r \tag{11}$$

where, $\oplus$ means XOR, <<< is a shift in a circular way to the left, and r is the number that you rotate by.

IBE Encryption: The modified biometric key is protected through Identity-Based Encryption (IBE) before being stored or transmitted.

$$C_f = E_{IBE}(K_f, ID)$$

(12)

3.5 Decryption and Key Retrieval

Authorized users are able to recover the original biometric key and gain access to the stored information. The decryption of the encrypted biometric key is carried out using the user's identity-based private key, ensuring that only the correct identity can successfully perform the decryption.

$$K_f = D_{IBE}(C_f, SK_{ID}) \tag{13}$$

By reconstructing the session key, the original biometric key can be accessed.

$$K_s = (K_f >>> r) \oplus H \tag{14}$$

Where, >>> denotes the right circular shift.

4. Key Strength of the Proposed Approach

Security is improved by avoiding the storage of raw biometric data, while computational load is minimized through the use of IBE-based encryption. The method reinforces access control since only legitimate users with verified identities can decrypt the information. It also provides protection against brute-force attempts, replay attacks, and biometric spoofing.

5. Results and Discussions

The efficiency of the proposed IBE method is assessed against ABE, RSA, and AES across four major security parameters: key generation time, encryption rate, decryption rate, and overall computational cost. The comparative findings are presented in the figures given below. Figure 2 shows the key generation time (in milliseconds) for IBE, ABE, RSA, and AES. Since key generation directly influences the efficiency of encryption systems, it plays a critical role in overall performance. The results show that IBE records a key generation time of 50 ms, which is much lower than RSA (120 ms) and ABE (70 ms), though slightly higher than AES (30 ms). These findings highlight that IBE strikes a balanced trade-off between performance and security, offering stronger efficiency than RSA and ABE while still ensuring robust cryptographic protection.

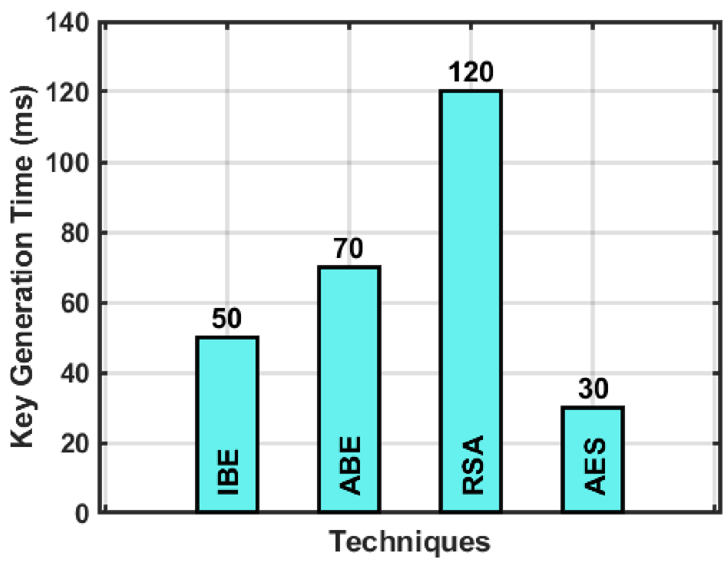

Figure 2: Evaluation of Key Generation Time among IBE, ABE, RSA, and AES

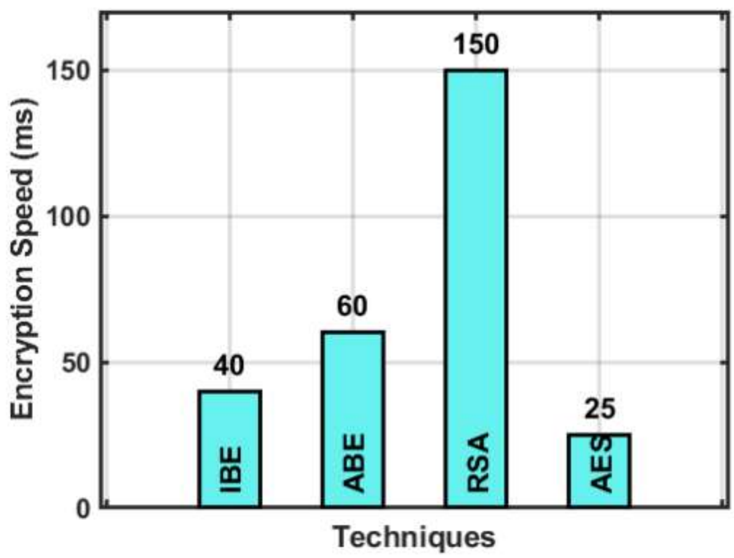

Figure 3: Comparative Analysis of Encryption Speed in IBE, ABE, RSA, and AES

Figure 3 shows the encryption speed (in milliseconds) for IBE, ABE, RSA, and AES. IBE achieves an encryption time of 40ms, which is faster than ABE (60ms) and RSA (150ms), making it a more efficient choice for cloud-based security applications. AES, as a symmetric algorithm, records the fastest time (25ms) due to its lightweight design. **Figure 4** illustrates the decryption speed (in milliseconds) across the same techniques. IBE completes decryption in 45ms, outperforming ABE (65ms) and RSA (140ms). Although AES remains the fastest with 20ms, it does not provide the identity-based access control advantages that IBE offers. These results demonstrates that IBE reduces the computational cost compared with conventional public-key

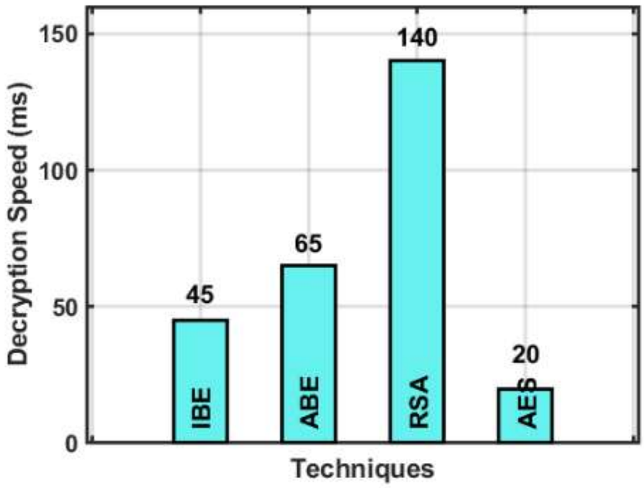

Figure 4: Comparative Analysis of Decryption Speed in IBE, ABE, RSA, and AES

systems such as RSA making it a better fit for real-time authentication scenarios. Figure 5 depicts the computational overhead (in percentage) for IBE, ABE, RSA, and AES. Overhead represents the extra processing demand introduced by an encryption algorithm. The findings indicate that IBE incurs a 30% overhead, which is lower than ABE (50%) and RSA (80%), but slightly higher than AES (20%).

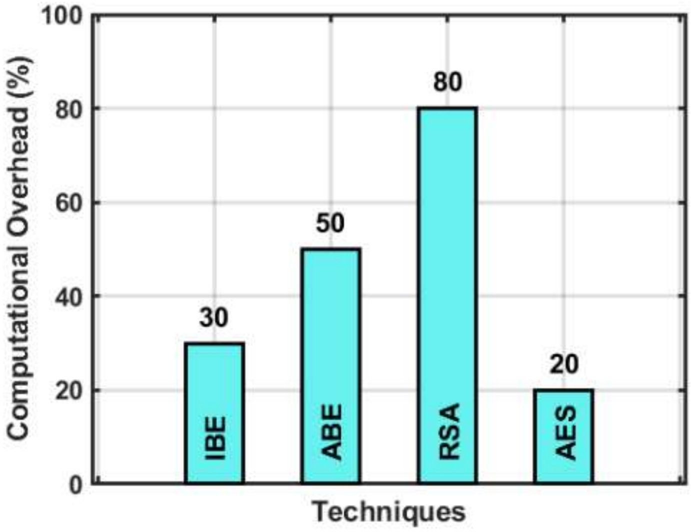

Figure 5: Comparative Analysis of Computational Overhead in IBE, ABE

These findings highlight that IBE achieves a practical balance between security and performance. Compared with ABE and RSA, IBE demonstrates greater efficiency while still upholding a strong security framework It can also improve the security with the use of biometric authentication, but at the cost of a little more time. However, IBE is a better trade-off than ABE and RSA by allowing us to avoid the overhead of key management and still being safe enough. Although AES is the fastest, it is a symmetric scheme and does not provide identity-based access control. We find that IBE can be a more effective solution than ABE by reducing key generation time, increasing encryption and decryption time, and decreasing the computational overhead, making it a good candidate for secure and scalable cloud-based biometric authentication.

6. Conclusion

This paper presents a system that uses a body-based method to keep a key safe, built on the Identity-Based Encryption (IBE) approach. The new system uses a fix of needing a finger to get data safe, to make the data safer, to get stricter rules of use, and to make the work of the machine go faster. The study shows that IBE is much better than both CP-ABE and RSA in finding a key to get in the data, keeping data safe with the key, and taking the data out of the safe. For example, IBE takes 50ms to find the key, 40ms to keep the data safe with the key and 45ms to get the data out of the safe with the key, so it takes less time to get the data out with the new system when set against either CP-ABE or RSA. Besides being fast, it is as safe, and so has a very good way of keeping and using the key in the cloud. The future work may resemble more on making the machine fast to use and making the scheme more safe with multi-biometric systems.

Conflict of Interest

The authors declare no conflict of interest.

References

[1]. S. El Kafhali, I. El Mir, M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Arch. Comput. Methods Eng.,* vol. 29, no. 1, pp. 223-246, Jan. 2022, https://doi.org/10.1007/s11831-021-09573-y

[2]. S. Ahmad, S. Mehfuz, J. Beg, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment," *J. Supercomput.,* vol. 79, no. 7, pp. 7377-7413, May. 2023, https://doi.org/10.1007/s11227-022-04964-9.

[3]. D. Shivaramakrishna, M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control," *Alex. Eng. J.,* vol. 84, pp. 275-284, Dec. 2023, https://doi.org/10.1016/j.aej.2023.10.054

[4]. M. Rasori, M. L. Manna, P. Perazzo, G. Dini, "A survey on attribute-based encryption schemes suitable for the internet of things," *IEEE Int. Things J.,* vol. 9, no. 11, pp. 8269-8290, Feb. 2022, doi: 10.1109/JIOT.2022.3154039

[5]. A. Saidi, O. Nouali, A. Amira, "SHARE-ABE: An efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and fog computing," *Cluster Comput.,* vol. 25, no. 1, pp. 167-185, Feb. 2022, https://doi.org/10.1007/s10586-021-03382-5

[6]. R. Hu, Z. Ma, L. Li, P. Zuo, X. Li, J. Wei, S. Liu, "An access control scheme based on blockchain and ciphertext policy-attribute based encryption," *Sensors,* vol. 23, no. 19, pp. 8038, Sep. 2023, https://doi.org/10.3390/s23198038

[7]. S. Deng, G. Yang, W. Dong, M. Xia, "Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation," *Multimed. Tools Appl.,* vol. 82, no. 14, pp. 22251-22274, Jun. 2023,https://doi.org/10.1007/s11042-022-13537-0

[8]. R. Alrawili, A. Abdullah S. AlQahtani, M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Comput. Elect. Eng.,* vol. 119, pp. 109485, Oct. 2024

[9]. M. A. Hossain, M. A. AlHasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *Int. J. Comput. Appl.,* vol. 44, no. 5, pp. 455-464, May. 2022, https://doi.org/10.1080/1206212X.2020.1809177

[10]. K. K. Prakasha, U. Sumalatha, "Privacy-preserving techniques in biometric systems: Approaches and challenges," *IEEE Access,* Feb. 2025,DOI: 10.1109/ACCESS.2025.3541649

[11]. K. Suresh, R. Pal, S. R. Balasundaram, "Two-factor-based RSA key generation from fingerprint biometrics and password for secure communication," *Complex Intell. Syst.,* vol. 8, no. 4, pp. 3247-3261, Aug. 2022, https://doi.org/10.1007/s40747-022-00663-3

[12]. S. Sridevi Sathya Priya, N. M. Sivamangai, R. Naveenkumar, A. Napolean, G. Saranya, "Biometric-based key generation using AES algorithm for real-time security applications," *In Homomorphic Encryption for Financial Cryptography: Recent Inventions and Challenges,* pp. 157-180, Aug. 2023. Cham: Springer International Publishing, https://doi.org/10.1007/978-3-031-35535-6-8

[13]. Suyal, H., Singh, A., & Shrivastava, G. (2025). Privacy Preserving Efficient Worker Selection in the Cloud-Based Crowdsourcing Platform. *Internet Technology Letters*, *8*(5), e70092.

[14]. J. Jebrane, S. Lazaar, "An enhanced and verifiable lightweight authentication protocol for securing the internet of medical things (IoMT) based on CP-ABE encryption," *Int. J. Inf. Secur.,* pp. 1-20, Sep. 2024, https://doi.org/10.1007/s10207-024-00906

[15]. Panwar, A., Bhatnagar, V., Khari, M., Salehi, A. W., & Gupta, G. (2022). A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake. *Computational Intelligence and Neuroscience*, *2022*(1), 3045107.

[16]. Rehna R S and S Maria Celestin Vigila, "A Detailed Review of Cryptographic and Biometric Security Mechanisms for Safeguarding Sensitive Healthcare Data in Cloud Computing Environments", In: Puneet Kumar Gupta (eds), Computational Models for Intelligence and Automation, SCRS, India, 2025, pp. 113-126, https://doi.org/10.56155/978-81-975670-1-8-11.