Research Article

ACCENTS Transactions on Image Processing and Computer Vision, Vol 9(25)
ISSN (Online): 2455-4707
http://dx.doi.org/10.19101/ TIPCV.2023.924002

Enhancing video encryption: AES and blowfish algorithms with random password generation

Shyam Babu Sah[1*] and Sandhya Gawade
School of Computer Science, Madhyanchal Professional University, Bhopal, India

Received: 16-May-2023; Revised: 08-August-2023; Accepted: 12-August-2023

Abstract
This paper explores the integration of AES and Blowfish algorithms for video encryption, utilizing a random password generation process to enhance efficiency in encryption and decryption. The study compares the results through various methodologies. One category assesses data using RGB buffer calculations, demonstrating that minimal RGB buffer variations ensure accurate encryption, making it suitable for video protection. Significant differences between original and encrypted image RGB attributes highlight robust encryption. The proposed approach combines AES's adaptability and Blowfish's efficiency, demonstrating their effectiveness for safeguarding sensitive digital content. The research advances video security within the contemporary digital landscape, addressing the imperative need for robust encryption techniques to protect valuable data during transmission and storage.

Keywords
AES, Blowfish, RGB buffer, Data security.

1.Introduction
In the contemporary era, a significant advancement in the field of information storage, particularly in the context of image data, has emerged within the research community. This development holds paramount importance due to its implications for data security, as well as the seamless transmission of information without infringing upon copyright protections.

To achieve these objectives, various techniques such as Cryptography, Steganography, and Watermarking have been explored, offering avenues for data security and authentication [1]. The concept of data concealment can serve multiple purposes, including safeguarding copyrighted content, revealing alterations in visual scenes [2], and facilitating covert message transmission. Additionally, data concealment techniques have the potential to assess the quality of compressed videos without relying on the original reference.

This is achieved by evaluating the discrepancies in the extracted hidden messages [3].

Steganography, as a legitimate approach within the realm of information concealment, plays a pivotal role [4]. Notably, security considerations are of paramount importance from the inception of designing distributed databases, especially in scenarios involving sensitive information [5]. The matter of security and intrusion detection mechanisms is also thoroughly explored in previous works [6–9].

Furthermore, the encryption and decryption processes applied to data during communication channels contribute significantly to data integrity. Techniques like DES, RSA, RC4, and RC5 are commonly employed for encryption and decryption purposes [10]. Block-based data segmentation can be executed through methods such as subset superset mining or distribution strategies [11–16]. This segmentation becomes particularly relevant in scenarios where the sender's data and the recipient's format differ, leading to heightened complexity and tighter security on the receiving end. Cryptography involves encoding the original content to produce ciphertext, while decryption reverses this process to retrieve the plaintext. Steganography, on the other hand, involves concealing the original content within another format, such as text, PDFs, or images. The recipient then independently extracts and decodes the concealed content. Cryptography, however, transforms the

*Author for correspondence

original plaintext into an encrypted, unintelligible form [13]. This encrypted content is surreptitiously transmitted by the sender to prevent unauthorized access, and upon reception, the reverse process is applied for decryption based on an algorithm. Decryption involves converting encoded data back to its original, readable format [17–21].

The primary objective of this paper is to explore the combined utilization of the AES and Blowfish algorithms for encrypting video data. By employing these robust encryption methods, the paper aims to enhance the security and confidentiality of video transmissions, aligning with the contemporary need for safeguarding sensitive digital information.

2.Literature review

In 2021, the importance of data security was emphasized by Goyal and Sharma [22] in the modern IT landscape, particularly in vulnerable cloud environments. Encryption methods like AES, DES, BLOWFISH, and Pailier were utilized to secure data in various formats, aiming to limit authorized access. Their performance was compared across different file types.

In 2021, cloud computing's dynamic nature was highlighted by Goyal and Sharma [23], enabling efficient data access and sharing. Data security concerns escalated with technological growth, necessitating secure data storage and transmission. Cryptographic techniques were introduced to ensure data integrity, analyzing DES, AES, Paillier, and Blowfish algorithms. Parameters like file size, encryption/decryption time, and memory usage were evaluated.

In 2022, encryption techniques for data security were explored by Shakeel et al. [24], focusing on algorithms like DES, IDEA, 3DES, AES, ECC, RSA, and blowfish. AES excelled in decryption. Suggestions were made to consolidate algorithms for enhanced security.

In 2022, the significance of data security across the IT sector was emphasized by Vishnoi et al. [25]. Encryption played a crucial role in rendering data unreadable to hackers. A low-bandwidth encryption method was introduced, compared to DES, 3DES, AES, blowfish, and RSA in execution time and file size. The proposed approach was faster for smaller data sizes, aiming to enhance encryption complexity. The key was generated from the message to enhance security.

In 2023, Parida and Bhanja [26] discussed the deployment of smart meters in Smart grid, introducing RSA, Blowfish, AES, DES, and 3DES algorithms. Hybrid RSA-Blowfish used intermediate Blowfish and RSA for encryption. Eigenvalue Encryption utilized eigenvalues for key generation, comparing both algorithms based on factors.

In 2023, the integration of cloud computing was examined by Yadav and Kumar [27], emphasizing data security's importance. Cryptography algorithms like DES, triple DES, Blowfish, AES, IDEA, RC4, RSA, and ECC were analyzed in a Node JavaScript environment, providing practical insights.

In 2023, the significance of secure communication was emphasized by Souror et al. [28] in the digital era. Cryptography played a vital role in safeguarding sensitive data during transmission and storage. They introduced the Hybrid-Blowfish algorithm, which combined Blowfish and SCA counter-measures, and compared DES, 3DES, AES, blowfish, RSA, and Hybrid-Blowfish, revealing a 25% increase in cyber-security strength.

In 2023, Susmitha et al. [29] indicated that data security involved protecting data from unauthorized access, ensuring privacy, availability, and integrity. Hybrid cryptography combined symmetric-key and public-key methods for secure communication and storage, safeguarding sensitive data. Cloud adoption addressed data storage challenges, but security concerns persisted. The study proposed a method to secure critical data and communication, addressing unauthorized access.

3.Methods

This paper delves into the utilization of AES and Blowfish algorithms for video encryption, integrating a random password generation approach to enhance the efficiency of the encryption and decryption processes. To facilitate this, a distinct phase was introduced where the video data was treated as a binary file, rather than being directly employed for encryption or decryption. This required a preliminary step of converting the entire video content into a binary file format, creating the foundation for subsequent encryption and decryption operations. Consequently, the input data used for the encryption and decryption procedures was in the binary format.

Figure 1 provides a comprehensive illustration of the operational process outlined in this study. It visually encapsulates the sequential steps involved in the

conversion of video content into binary data, followed by the encryption and decryption phases utilizing the AES and Blowfish algorithms. The process flow depicted in *Figure 1* serves as a visual aid in understanding the working mechanism adopted in this research.

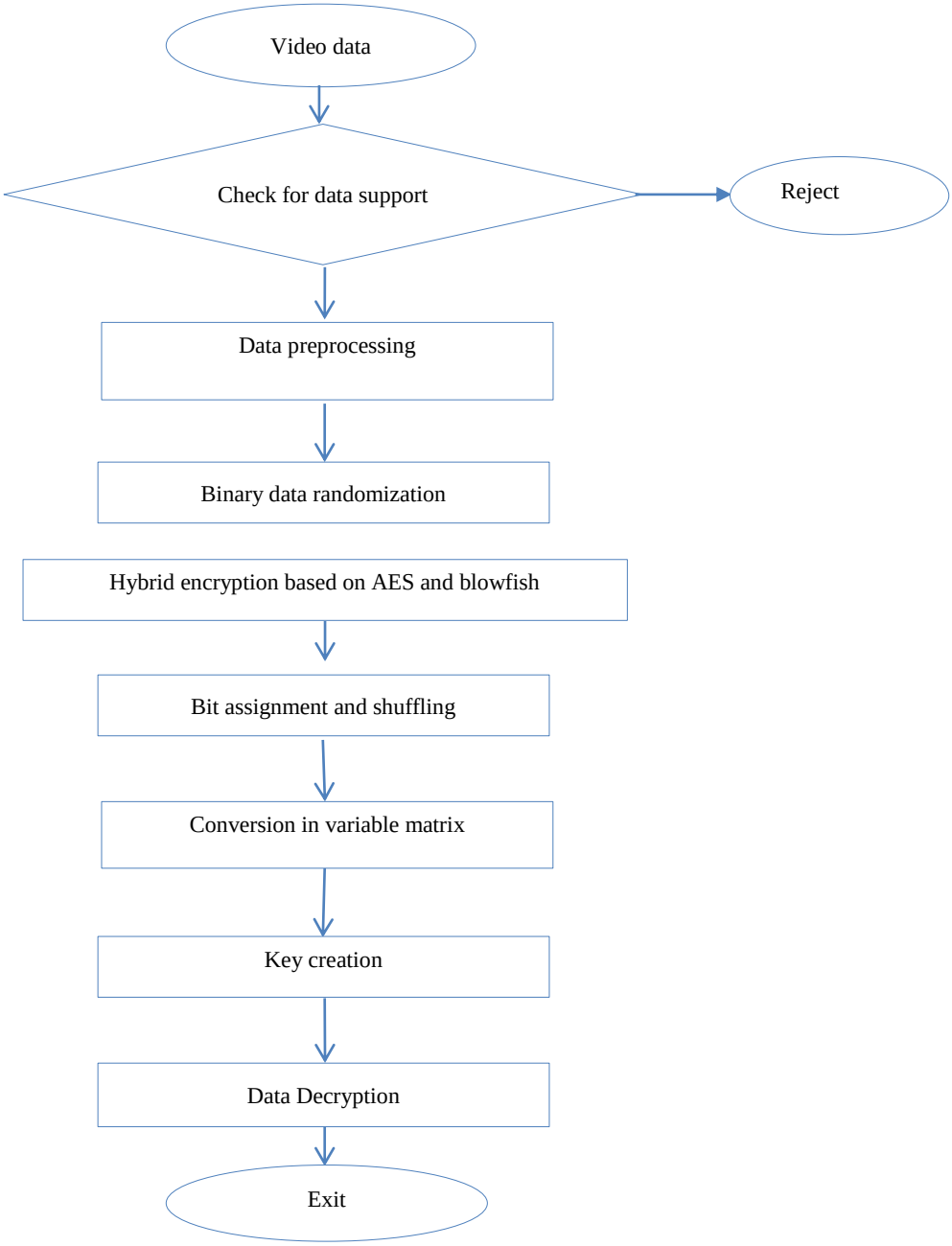

Figure 1 Flowchart of working procedure

The process of data encryption and decryption was facilitated by combining the AES and Blowfish algorithms. These algorithms operated by utilizing binary data as input for the encryption process. Initially, the AES algorithm was applied to the computational bytes of the data. AES effectively utilized the entire 256 bits of a plaintext block, which were distributed as 16 bytes and organized in various matrix formations such as 4×4, 8×8, 16×16, and 32×32. A notable advantage of AES arises from its

adaptability, wherein it employs 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 512-bit keys. Each round incorporates unique 256-bit round keys, derived from the original AES key. The selection of AES was influenced by its rapid processing speed and its ability to accommodate larger key sizes. Parallel to AES, the Blowfish algorithm played a pivotal role, executing security measures across 16 rounds while ensuring efficient image encryption. The decision to utilize Blowfish was influenced by its established efficacy in data protection and its optimized performance in image encryption processes.

4.Results and discussion

The first category of analysis involves a comparison of data utilizing RGB buffer calculations for two samples. This experimental process is visually presented in *Figures 2* and *3*. Diverse samples were examined during this experimentation, revealing that fluctuations within the RGB buffer remained minimal. This observation indicated that the encryption process functioned accurately, rendering it suitable for video encryption applications. Furthermore, the visual inspection unveiled substantial disparities in the RGB values between the original and encrypted images. Consequently, decoding the encrypted content proves to be a formidable task due to the extensive variations in RGB values. The discernible contrast in RGB attributes solidifies the encryption's effectiveness in introducing complexity, enhancing the overall security of the encrypted content. This underscores the encryption's resilience against unauthorized decryption attempts and reinforces its reliability as a safeguard for sensitive video data.

5.Conclusion

This study employed the AES and Blowfish algorithms to facilitate video encryption, incorporating a process of random password generation to amplify the effectiveness of encryption and decryption operations. The results underwent diverse comparisons. The initial category involved a comparison of data using RGB calculations. The analysis revealed minimal variations in RGB buffers, affirming the accurate operation of the encryption process, rendering it highly suitable for video encryption. Conversely, stark disparities were evident in the RGB attributes between the original and encrypted images, signifying the formidable challenge in deciphering the content due to pronounced RGB variations. This intricacy bolstered the encryption's efficacy in augmenting data security. The research contributes to understanding the potency of AES and Blowfish algorithms in ensuring robust video encryption, reinforcing their role in safeguarding sensitive data.

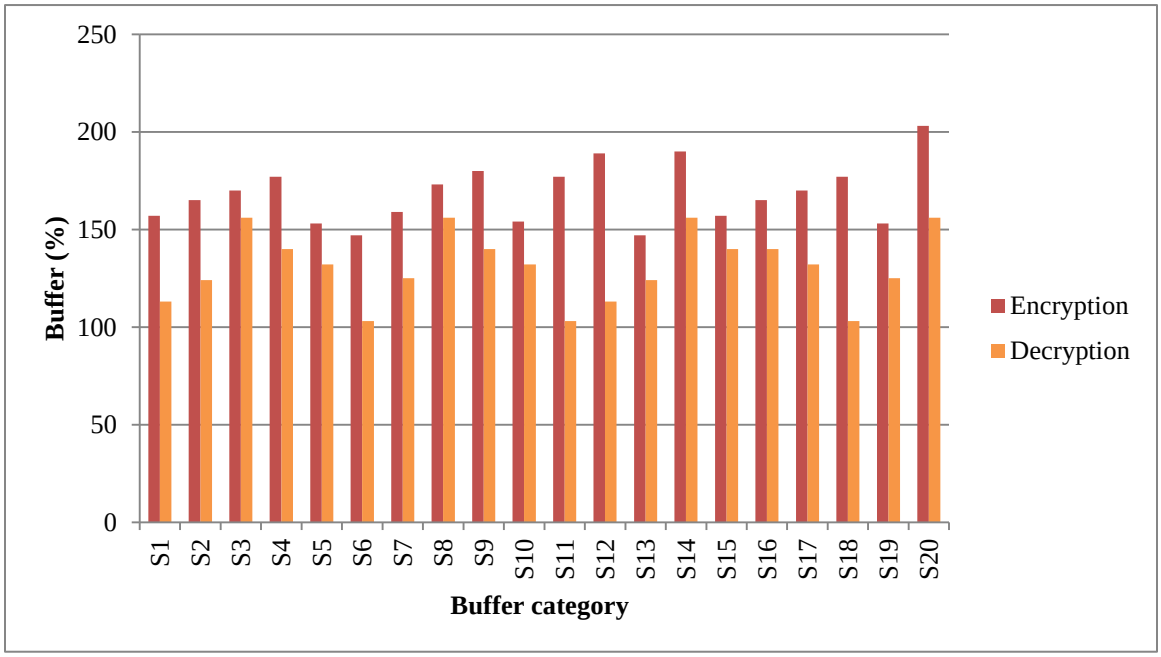

Figure 2 Buffer segment comparison based on for sample 1 considering encryption and decryption process

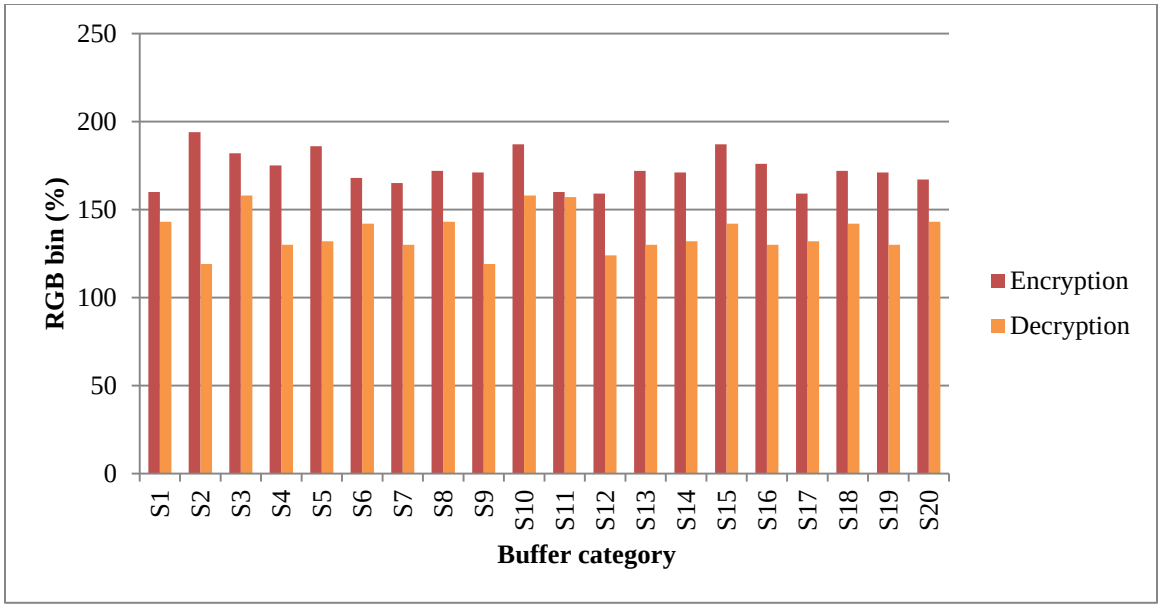

Figure 3 Buffer segment comparison based on for sample 2 considering encryption and decryption process

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Dibas H, Sabri KE. A comprehensive performance empirical study of the symmetric algorithms: AES, 3DES, Blowfish and Twofish. In international conference on information technology (ICIT) 2021 (pp. 344-9). IEEE.

[2] Patel K. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. International Journal of Information Technology. 2019; 11:813-9.

[3] Wajgade VM, Kumar DS. Enhancing data security using video steganography. International Journal of Emerging Technology and Advanced Engineering. 2013; 3(4):549-52.

[4] Alexan W, Hemeida F. Security through blowfish and lsb bit–cycling with mathematical sequences. In signal processing: algorithms, architectures, arrangements, and applications (SPA) 2019 (pp. 229-34). IEEE.

[5] Assa-Agyei K, Olajide F. A comparative study of twofish, blowfish, and advanced encryption standard for secured data transmission. International Journal of Advanced Computer Science and Applications. 2023; 14(3):393-98.

[6] Elkandoz MT, Alexan W, Hussein HH. Double-layer image security scheme with aggregated mathematical sequences. In international conference on advanced communication technologies and networking (CommNet) 2019 (pp. 1-7). IEEE.

[7] Singh AK, Alshehri M, Bhushan S, Kumar M, Alfarraj O, Pardarshani KR. Secure and energy efficient data transmission model for WSN. Intelligent Automation & Soft Computing. 2021; 27(3):761-9.

[8] Commey D, Griffith S, Dzisi J. Performance comparison of 3DES, AES, Blowfish and RSA for dataset classification and encryption in cloud data storage. International Journal of Computer Applications. 2020; 177(40):17-22.

[9] Husein AM, Harahap M, Dharma A, Simarmata AM. Hybrid-AES-Blowfish algorithm: key exchange using neural network. In international conference of computer science and information technology (ICoSNIKOM) 2019 (pp. 1-4). IEEE.

[10] Ahmad R, Mohamed Omar MF, Rajendran J, Ismail W. Performance analysis of enhanced AES-128 and blowfish algorithms through parallel-pipelined-memory techniques. Wireless Personal Communications. 2022; 127(4):3615-35.

[11] Joseph T, Kalaiselvan SA, Aswathy SU, Radhakrishnan R, Shamna AR. Retracted article: a multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. Journal of Ambient Intelligence and Humanized Computing. 2021; 12(6):6141-9.

[12] Wahid SD, Buja AG, Jono MN, Aziz AA. Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: a structural equation modeling. International Journal of Advanced Technology and Engineering Exploration. 2021; 8(74):73-81.

[13] Kumar A, Kumar SA, Dutt V, Kumar Dubey A, Narang S. A hybrid secure cloud platform maintenance based on improved attribute-based encryption strategies. International Journal of Interactive Multimedia and Artificial Intelligence.2022; 8(2):150-7.

[14] Kurniawan DE, Iqbal M, Friadi J, Hidayat F, Permatasari RD. Login security using one time password (OTP) application with encryption algorithm performance. In journal of physics: conference series 2021 (p. 012041). IOP Publishing.
[15] Rehman S, Talat Bajwa N, Shah MA, Aseeri AO, Anjum A. Hybrid AES-ECC model for the security of data over cloud storage. Electronics. 2021; 10(21):2673.
[16] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. 2019; 7:82721-43.
[17] Kumar S, Kumar D, Singh N. Performance and security analysis using B-128 modified blowfish algorithm. Multimedia Tools and Applications. 2023:1-8.
[18] Sridhar S, Smys S. Hybrid RSAECC based secure communication in mobile cloud environment. Wireless Personal Communications. 2020; 111(1):429-42.
[19] Samvatsar M, Kanungo P. An analytical review and analysis for the data control and security in cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2020; 7(73):241-6.
[20] Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo KK, Zomaya AY. Blockchain for smart communities: applications, challenges and opportunities. Journal of Network and Computer Applications. 2019; 144:13-48.
[21] Dubey AK, Giri M, Sahare M, Dubey AK. Step-up analysis and generalization approach for trusted NFC application development for enhancing real time use Location. In international conference on communication systems and network technologies 2011 (pp. 318-22). IEEE.
[22] Goyal M, Sharma A. Implementation and analysis of various encryption techniques with blowfish on various data files. In international conference on technological advancements and innovations (ICTAI) 2021 (pp. 541-6). IEEE.
[23] Goyal M, Sharma A. Enhancing hybrid encryption techniques for secured data processing for small medium enterprises in cloud. In international conference on technology, research, and innovation for betterment of society (TRIBES) 2021 (pp. 1-5). IEEE.
[24] Shakeel M, Sirisha A, Joshi A, Ushasree R, Vaishnavi M, Verma D. An analysis of different cryptocraphy techniques and the role of coding and information theories in overcoming security threats. In 5th international conference on contemporary computing and informatics (IC3I) 2022 (pp. 223-8). IEEE.
[25] Vishnoi A, Aggarwal A, Prasad A, Prateek M, Aggarwal S. Text encryption for lower bandwidth channels: design and implementation. In third international conference on intelligent computing instrumentation and control technologies (ICICICT) 2022 (pp. 1460-4). IEEE.
[26] Parida D, Bhanja U. Smart meters: cyber security issues and their solutions. In 2nd international conference on vision towards emerging trends in communication and networking technologies (ViTECoN) 2023 (pp. 1-6). IEEE.
[27] Yadav V, Kumar M. Key cryptographic methods in the cloud: a comparative study. In 3rd international conference on intelligent communication and computational techniques (ICCT) 2023 (pp. 1-5). IEEE.
[28] Souror WW, Fouad M, Takieldeen AE. Hybrid-blowfish security strengths using side channel countermeasures. In international telecommunications conference (ITC-Egypt) 2023 (pp. 314-21). IEEE.
[29] Susmitha C, Srineeharika S, Laasya KS, Kannaiah SK, Bulla S. Hybrid cryptography for secure file storage. In 7th international conference on computing methodologies and communication (ICCMC) 2023 (pp. 1151-6). IEEE.

Shyam Babu Sah is pursuing M.Tech in Computer Science & Engineering at Madhyanchal Professional University, Bhopal (MP), India, and holds a B.Tech degree in Computer Science & Engineering from Shaheed Bhagat Singh State Technical Campus, Ferozepur (PB), India. His primary area of interest is Network Security.
Email: sahshyambabu11@gmail.com

Sandhya Gawade is currently employed as an Assistant Professor in the Department of Computer Science and Engineering at Madhyanchal Professional University, located in Bhopal, India. She holds both a Bachelor of Engineering (B.E.) and a Master of Engineering degree in Computer Science and Engineering from Rajiv Gandhi Technical University in Bhopal, Madhya Pradesh. Her research interests encompass the fields of Data Mining, Optimization, and Machine Learning.
Email: sandhya.gawhade@gmail.com