ISSN: 0974-5823 Vol. 7 No. 11 November, 2022

International Journal of Mechanical Engineering

Multifactor Authentication using Double Encryption based Blowfish Algorithm for Data Security in Cloud Environment

L.Umarani
Research Scholar, Bharathiar University, umarcl@gmail.com

Dr.A. John Sanjeev Kumar
Assistant Professor, The American College, Madurai, johnsanjeevkumar@gmail.com

Abstract

The cloud is a paradigm for computing that gives customers on-demand, pay-as-you-go access to a shared pool of computing resources. Several firms gain from the cloud era in terms of capital investment and operational expenditure. One of the significant issues facing many firms is security as it relates to cloud computing. Cloud should have a robust authentication architecture in order to achieve highly secured resource access. The purpose of this research effort is to offer a reliable framework for cloud environments' authentication in order to realise a safe access control mechanism in the server. In order to provide cloud users with secure access to the network and data centres, this research proposes the Multifactor Authentication using Double Encryption based Blowfish (MFA- DEBF) Algorithm. MFA-DEBF enforces access control protocols to protect cloud resources from unauthorised access.

Keywords: Authentication, Cloud Security, Elliptic Curve Cryptography, RSA, Multifactor Authentication using Double Encryption based Blowfish Algorithm

1. Introduction

Authentication is the process of verifying the user's identity. The straightforward and well-liked traditional password-based authentication approach enables the system to identify the user using a distinctive identification and password [14]. Password-based authentication is still used by a number of conventional and cloud-based apps to verify users' identities. The application is made more secure by the availability of several better user authentication options, including x.509 certificates, One-Time Passwords (OTP) [7], biometric authentication, and captcha-based authentication [5].

To provide a stronger combination of authentication elements, these strategies can be combined [24]. Multi-Factor Authentication (MFA), Trusted Computing Group (TCG), Public Key Infrastructure (PKI), Single Sign-On (SSO), and Biometric Authentication are some of the several authentication techniques used in a cloud context. These techniques are frequently used to improve cloud security [15].

The public cloud service providers enable consumers to store a sizable amount of data at a reasonable cost and access the data whenever they need it. Due to the absence of control over the services provided at the public cloud, the issue with the public cloud is security concerns [9]. As many users practically share the same public cloud environment, there is a potential that attackers will launch attacks on the services and data stored [25]. With all of these many cloud security issues, protecting data from unauthorised users is the most difficult challenge [10]. The solution is authentication, in which the cloud provider checks the identity of the cloud user requesting services from the cloud server [16].

Password-based, hardware-based and biometric authentication are the current authentication methods. The most often used authentication method is password-based authentication [1]. However, because the passwords are easy to guess, it is vulnerable to issues. Similar to this, using the same password for many services can expose you to dictionary and guessing attacks [11]. The challenge with smart card-based authentication is that the user must always carry the smart card, and losing the smart card can be dangerous. The limitations of

biometric authentication are their inadequate ability to adapt to change, inaccurate feature extraction, and lack of privacy [12].

As an extension of Shamir's secret sharing feature, a multifactor authentication (MFA) method based on the reversed Lagrange polynomial handles the situations of confirming identification even if some of the components are out of place or missing [17]. An assigned appropriate is ready to assist with authentication by providing private information to the user when a problem affects or repeatedly misses their 2F keys [8]. Without giving the validator unauthorized access to personal data, it also helps qualify missing elements. The suggested approach is specifically designed to fulfil the MFA procedures, therefore its administration for 2FA and SFA is not praised [13]. A random timestamp cannot provide a useful level of biometric data protection since a spy might instantly extract the secret information [18]. The goal of multi-factor authentication is to integrate the most effective security measures.

2. Literature Review

According to Bruno et al. (2021) discussed [2] modern sophisticated technologies like cloud computing have made it possible to obtain data from any location. Using various procedures, authentication is crucial to preserving security. The safe computation methods for biometric authentication are homomorphic encryption, garbled circuit, and oblivious transfers (OT, GC) (HE). The oblivious transfer primitive allows a receiver to retrieve specified elements from a sender without the sender being aware of the component that has been selected. Second, the general computation is a binary circuit tool that guarantees security in two-party calculation. Yao protocol performs safe two-party computing after first scrubbing the binary circuit by replacing the bits in the table with their matching keys that are encrypted. Thirdly, Homomorphic Encryption encrypts the data using addition or multiplication operations without using the secret key. Typically, public-key cryptanalysis employs this characteristic [20]. These streamlined variations of biometric identification systems allow for cost savings but at the expense of accuracy.

Mohammad et al. (2015) [4] suggested an authentication approach for cross-enterprise biometric identification (CloudID) in the cloud. This technique protects against identity theft in the cloud and offers security to sensitive data. Unfortunately, this approach has a significant degree of complexity, and real-time identification in huge databases requires highly expensive processing power.

In order to improve cloud security, Abdu et al. (2018) suggested [3] a model of biometric identification system based on the multi-spectral model. Multi-spectral sensors first take a segmented image of the user's palm print. Spectral palm prints are combined utilising the Dual-Tree Complex Wavelet Transform-based picture fusion technique (DT-CWT). The inverse of DT-CWT is then utilised to recreate the fused Region of interest (ROI) image from the fused coefficients. Following normalisation, the image is put through a 2D Gabor filter using the Fourier function transform. To eliminate this redundant information, the Principal Component Analysis (PCA) algorithm is then used. The RSA algorithm generates the public and private keys based on the user's selection of random prime integers. The collected palm-print features are then encrypted with the aid of a public key. Regularized Extreme Learning Machine (RELM) classifier detects the user's encrypted features during the identification stage. This methodology improves the biometric identification process' accuracy and efficiency [21]. This model, however, was unable to carry out real-time online identification.

Liehuang Zhu et al. (2018) [25] presented effective and privacy-preserving biometric identification in cloud computing. The resulting feature vectors are expressed as Finger Code when the fingerprint is provided as input. The matrix is then produced at random by the database owner. The database owner then stores the matrix as a tuple on the cloud server after encrypting it. The database owner calculates the similarity score using Euclidean distance to produce the match result [23]. This model defends against potential threats while maintaining privacy. Yet, different skin conditions have an impact on the accuracy.

Harkeerat et al. (2019) presented [6] cancellable biometrics for remote multi-server biometric authentication. First, using Log-Gabor filters, the features of the face, palmprint, palm vein, and finger vein are retrieved. To alter a template, use Random Projection to combine the original feature vector with the random grid provided using the transformation key (RP). Due to their distance-preserving capabilities, the Random Distance Method (RDM) is used to create pseudo-identities that correspond to a variety of biometric features and reduces the dimensions and feature transformation [22]. This technique decreases the size while preserving privacy. However, it has the downside of necessitating the regeneration of all pseudo-identities in the database if the entire database becomes corrupt.

Multi-modal biometric security utilising the C3D Deep Learning (DL) Network was suggested by Ayesha et al. in 2020 [19]. The C3D DL network is initially fed the iris, fingerprint, and facial traits in order to detect the low-level features. The multi-modal bio-secret key that is utilised to decode the server-stored data was generated using the multi-user master key. Hence, to increase security, dynamic keys are produced for each user throughout the encryption process. Unfortunately, in terms of multi-modal biometric security, this paradigm is unable to deliver the desired results in real-time.

3. Proposed Methodology

3.1 Multifactor Authentication using Double Encryption based Blowfish Algorithm (MFA-DEBF)

The proposed system's flexible design enables us to independently examine each risk and its associated response. This facilitates cloud system management and enables administrators and users to incorporate specific solutions to mitigate hazards. Cloud users and cloud servers are two different types of entities in a cloud system. The proposed authentication process consists of the registration phase and the login phase.

Algorithm 3.1 MFA-DEBF Algorithm

//REGISTRATION PHASE

Step 1: Username, email address, and mobile number are sent by the client to the cloud server.
Step 2: The client is sent an email OTP and an SMS OTP by the server, which also saves the information that was received.
Step 3: Email OTP and SMS OTP are stored by the client and are sent by the server.
Step 4: Input from the client is sent to the cloud server via email and SMS.
Step 5: The generated Encryption keypair is verified by the server after the given OTP.
Step 6: When a client requests secure communication, the server delivers them the created EC-public key.
Step 7: Client gets EC-public key from the server.
Step 8: Utilizing PBDKF2, the client creates and stores a safe salted password.
Step 9: Secure password, subscription information, service information, and duration were sent to the server.
Step 10: The server maintains a database on the server that contains all the user ID and credential information.
Step 11: To use its private key, the server encrypts the subscription certificate.
Step 12: The encrypted subscription certificate is once more encrypted by the server using the client nonce that was received.
Step 13: The server then provides a successful message to the client as well as a double encrypted subscription certificate.
Step 14: With the server's public key and nonce, the client once more decrypts the certificate.

//LOGIN AND AUTHENTICATION

//First Factor Cloud Authentication

Step 1: When receiving an encrypted message, the cloud server initially decrypts it before verifying the user's provided digital signature.
Step 2: If the previous step is confirmed, the cloud server sends an OTP to the registered mobile and email addresses (OTP1 and OTP2, respectively), and waits for the two - step verification step.

//Second Factor Cloud Authentication

Step 3: To enter a cloud certificate, an email OTP, or a mobile OTP
Step 4: The user will be authorised and able to use cloud services if all three of the following requirements are found to be true.

Three steps are in the registration phase. In order to access the facilities offered by the cloud server, cloud users must first enroll with the cloud server by completing the three major steps: Cloud users must first enroll by providing their user ID, email address, and cell phone number. The server then validates and verifies all of the submitted information and delivers an OTP to the user's email and mobile number to confirm their identity.

The client enters valid OTPs in the second phase, at which point the server provides the client with a key for continued secure communication with the server as well as additional valuable information like a password. The third stage involves the user selecting a password, the type of service, and the length of the service. All information is then forwarded securely using a common server key and additional security precautions. The server then produces a cloud certificate which contains the user ID, subscription, and duration and sends it back to the client in an encrypted file after securely storing all of the user ID information for client identifying credentials in the server database.

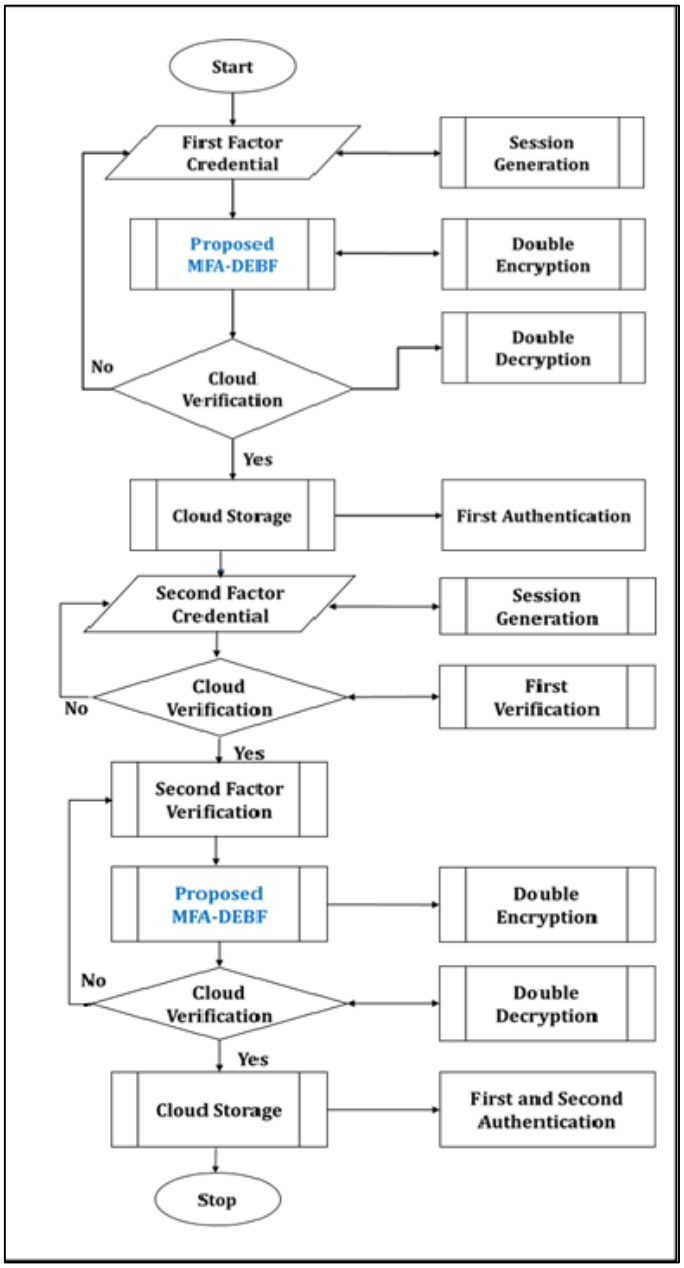

Figure 3.1 Flow Chart of Proposed Multifactor Authentication using Double Encryption based Blowfish Algorithm

The protocol also includes the ensuing two tiers of two-factor authentication to confirm the authenticity of the party making the request. The client accesses the first factor of authentication when the initial factor. The cloud technology has received and is handling the request. A web server and a database server make up the cloud services. The database server checks the credentials against entries that have previously been recorded, and after authentication process, a verification is given to the cloud provider to inform the user. In this case, the cloud user gives the cloud server their user ID and password.

After that to validate the second factor using an authorization application following the first factor has been successfully verified. The cloud server reviews the first factor after receiving the request and provides a confirmation or rejection back to the cloud for processing. After the first factor has been successfully revised, the cloud sends a request to check the second factor and sends the user an OTP request to validate the device. The user is given permission to access the cloud after authentication process.

The multifactor authentication process involves a cloud user securely submitting typical credentials, such as a user ID and a robust salted password, to the cloud server for verification. If those credentials are found to be correct, the server then requests the user to submit additional authentication factors, including a certificate that the cloud server has already offered as his authenticity certificate and an OTP via email and mobile.

3.1.1 Double Encryption based Blowfish Algorithm (DEBF)

The data is encrypted twice using the double encryption methodology before being uploaded to the cloud to increase data security. The blowfish algorithm is used in the algorithm to encrypt plain text, and a modified blowfish algorithm is then used to encrypt the key. Figure 3.2 illustrates the double encryption scheme's working mechanism.

The major goal is to investigate the underlying mechanisms by reducing the round count, expanding the block variable, and providing transformation methods on a few rounds in an effort to develop different innovations for message encryption. Four S-boxes, Key Expansion, Key Bits Shifting, are Modified F-Function, are used by the proposed DEBF. The message is more securely encrypted according to the improvements in cryptanalysis, which also heighten the tangible opportunities of the Blowfish algorithm.

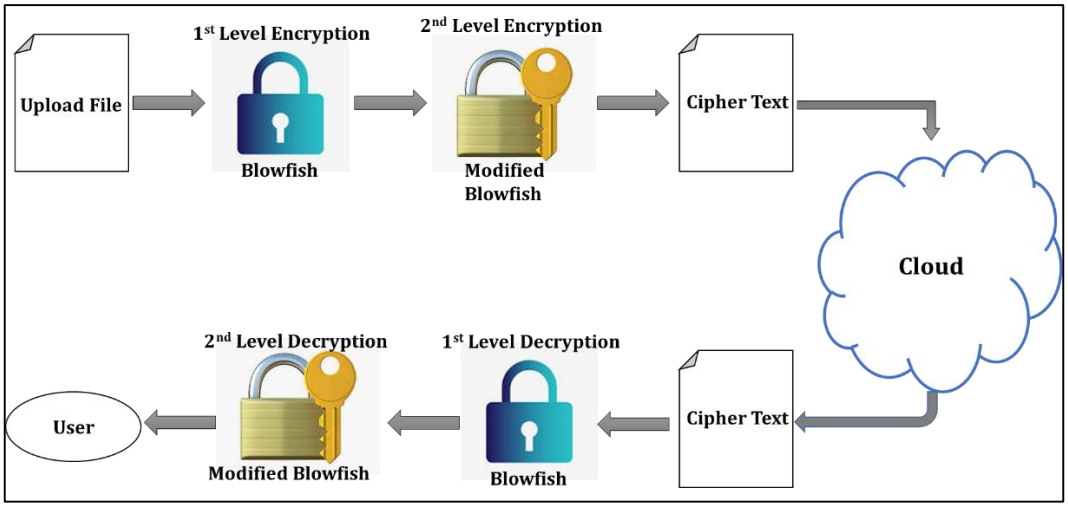

Figure 3.2 Architecture for Proposed Double Encryption based Blowfish Algorithm

The architecture of the proposed DEBF algorithm expressed that initially the uploaded files are encrypted using traditional blowfish algorithm. Then the second level encryption is performed using modified blowfish algorithm. After that, the cipher text is stored in cloud. Furthermore, the encrypted files are decrypted using first level decryption using traditional blowfish and then second level decryption is performed by modified blowfish algorithm.

4. Results and Discussion

An innovative strategy using a multifactor secure authentication technique in addition to standard user IDs, passwords, and OTP verification process The effectiveness of two existing algorithms was evaluated and contrasted with the proposed MFA-DEBF algorithm. Elliptic Curve Cryptography (ECC) and Rivest-Sha-mir-Adleman (RSA) were two existing approaches, and the respective charts were produced for varying file sizes to obviously indicate the superiority of the earlier compared to the latter.

Table 4.1 and figure 4.1 depicts that the proposed MFA-DEBF algorithm takes 845.592601ms lesser than RSA and 98.87ms lesser than ECC. Whereas, The proposed MFA-DEBF algorithm performs with minimum key generation time, encryption, and decryption time for 5kb file size.

Table 4.1 Time Taken for 5kb File Size

Algorithms	Key Gen. time (ms)	Encryption Time (ms)	Decryption Time (ms)	Total Time (ms)
RSA	313.6852	152.1758	471.7316	937.5926
ECC	130.8893	29.5168	30.463899	190.869999
Proposed MFA-DEBF	75.6093	16.2368	0.153899	91.999999

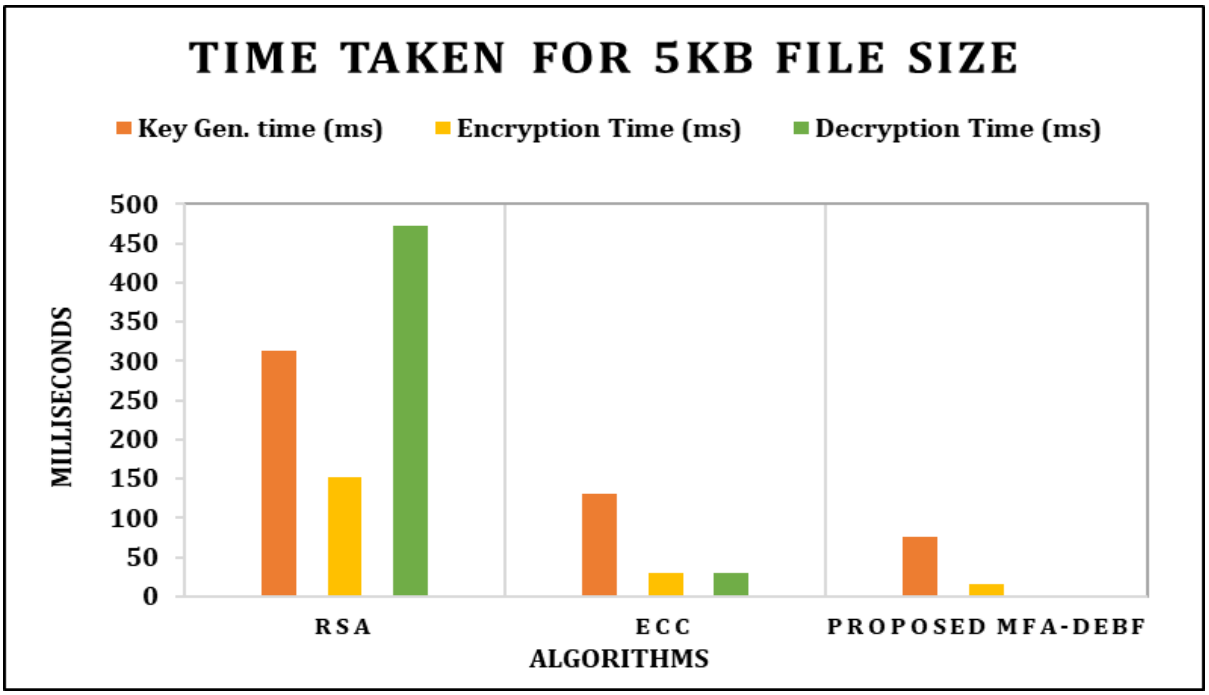

Figure 4.1 Time Taken for 5kb File Size

Table 4.2 and figure 4.2 depicts that the proposed MFA-DEBF algorithm takes 1012.288ms lesser than RSA and 112.87ms lesser than ECC. The proposed MFA-DEBF algorithm performs with minimum key generation time, encryption, and decryption time for 10kb file size.

Table 4.2 Time Taken for 10kb File Size

Algorithms	Key Gen. time (ms)	Encryption Time (ms)	Decryption Time (ms)	Total Time (ms)
RSA	365.641	178.7443	569.4614	1113.8467
ECC	142.231501	31.4292	40.7682	214.428901
Proposed MFA-DEBF	76.951501	18.1492	6.4582	101.558901

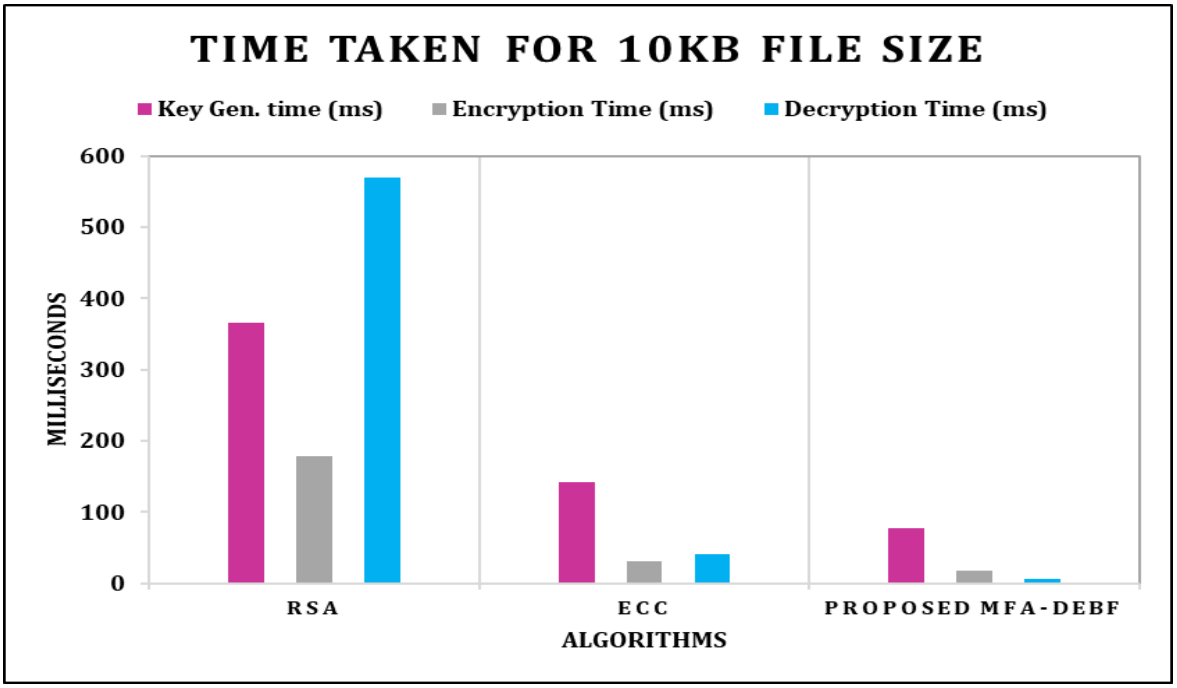

Figure 4.2 Time Taken for 10kb File Size

Table 4.3 and figure 4.3 depicts that the proposed MFA-DEBF algorithm takes 935.1979ms lesser than RSA and 73.87ms lesser than ECC. The proposed MFA-DEBF algorithm performs with minimum key generation time, encryption, and decryption time for 15kb file size.

Table 4.3 Time Taken for 15kb File Size

Algorithms	Key Gen. time (ms)	Encryption Time (ms)	Decryption Time (ms)	Total Time (ms)
RSA	403.9648	200.5511	426.157	1030.6729
ECC	143.6282	30.1304	5.5864	169.345
Proposed MFA-DEBF	78.3482	16.8504	2.2764	95.475

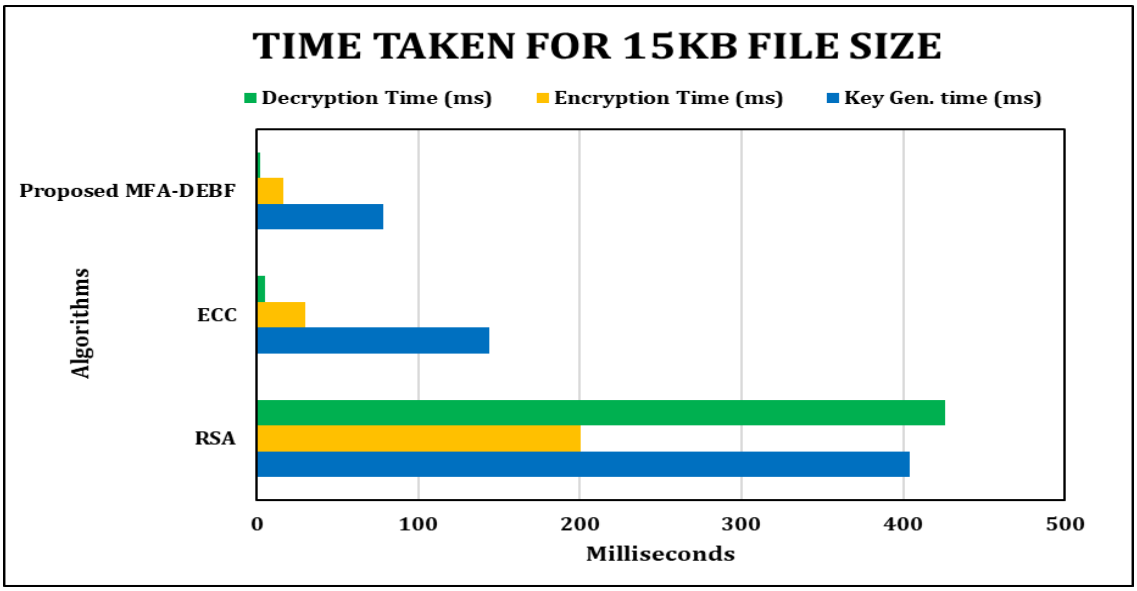

Figure 4.3 Time Taken for 15kb File Size

Table 4.4 and figure 4.4 depicts that the proposed MFA-DEBF algorithm takes 1164.9758ms lesser than RSA and 117.74ms lesser than ECC. The proposed MFA-DEBF algorithm performs with minimum key generation time, encryption, and decryption time for 20kb file size.

Table 4.4 Time Taken for 20kb File Size

Algorithms	Key Gen. time (ms)	Encryption Time (ms)	Decryption Time (ms)	Total Time (ms)
RSA	500.6242	332.2658	472.371	1305.261
ECC	163.9626	51.9811	42.0815	258.0252
Proposed MFA-DEBF	90.6826	28.7011	20.9015	140.2852

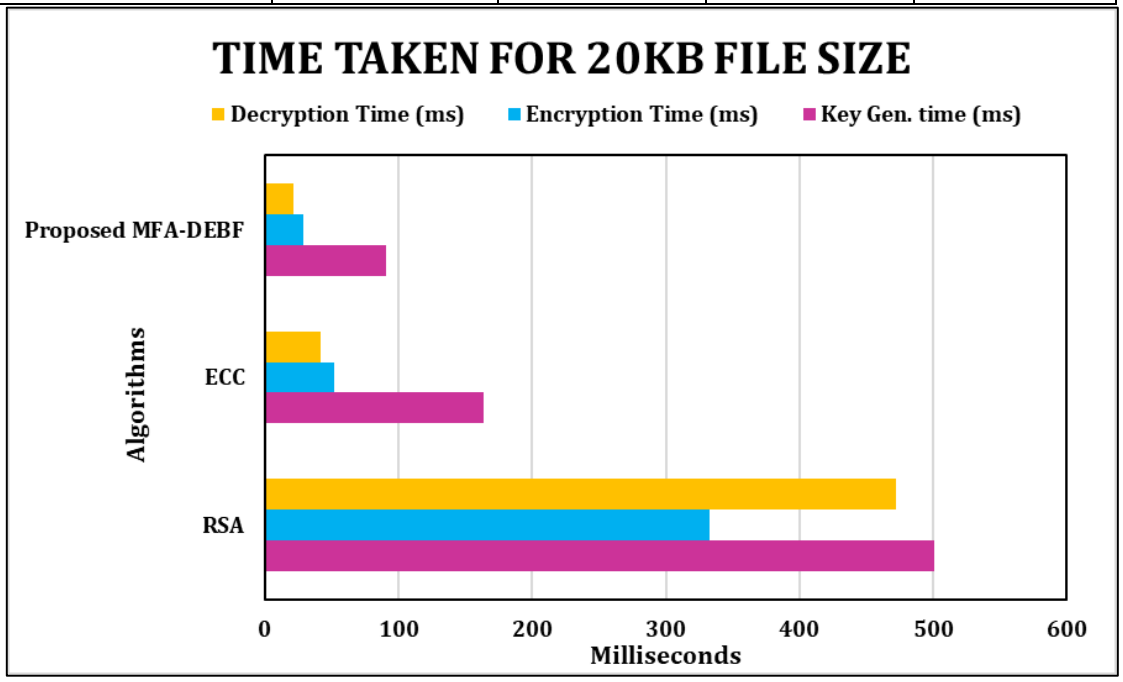

Figure 4.4 Time Taken for 20kb File Size

Table 4.5 and figure 4.5 depicts that the proposed MFA-DEBF algorithm takes 1263.924ms lesser than RSA and 79.87ms lesser than ECC. The proposed MFA-DEBF algorithm performs with minimum key generation time, encryption, and decryption time for 25kb file size.

Table 4.5 Time Taken for 25kb File Size

Algorithms	Key Gen. time (ms)	Encryption Time (ms)	Decryption Time (ms)	Total Time (ms)
RSA	606.1371	370.2108	492.4375	1468.7854
ECC	174.2679	56.0273	54.4362	284.7314
Proposed MFA-DEBF	119.9879	42.7473	42.1262	204.8614

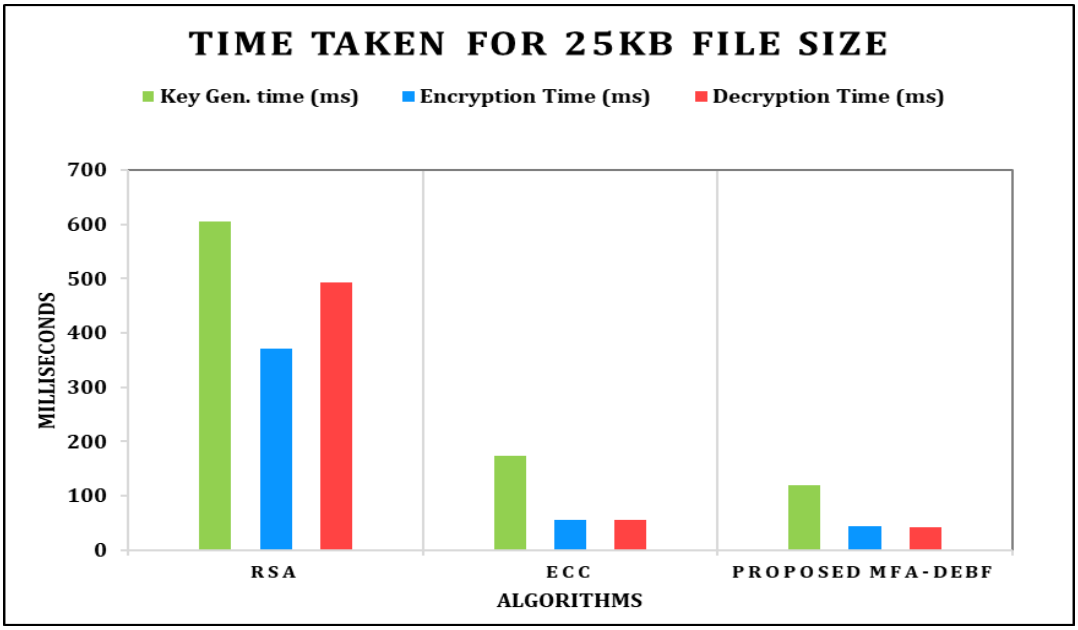

Figure 4.5 Time Taken for 20kb File Size

Table 4.6 and Figure 4.6 makes it clear that the proposed MFA-DEBF achieves 3.15% greater than RSA and 2.89% greater throughput than ECC. The proposed MFA-DEBF achieves better throughput than existing algorithms.

Table 4.6 Throughput in kilobytes/milliseconds

Algorithms	Throughput (kb/seconds)
RSA	74.9
ECC	100.06
Proposed MFA-DEBF	390.08

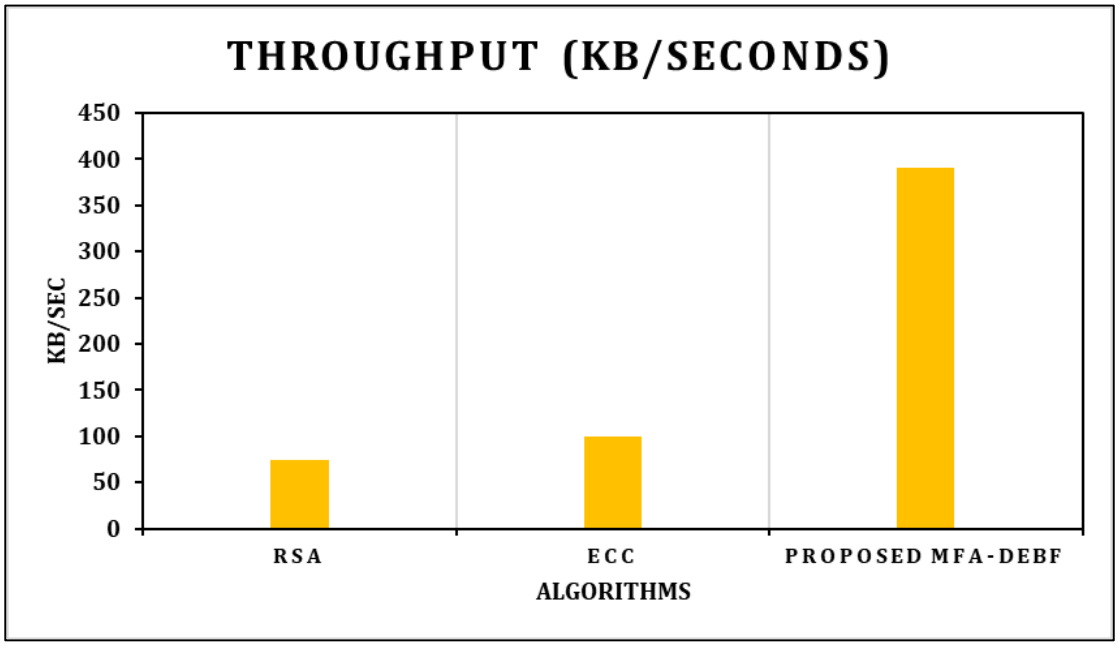

Figure 4.6 Throughput

The analysis was completed in table format, and the execution time was recorded. The suggested MFA-DEBF offers more execution speed and security than RSA and ECC, which leads to a better user experience. An experiment demonstrates that the proposed MFA-DEBF is faster than RSA and ECC, primarily on memory-constrained platforms and in terms of time, as well as that it offers greater security. The proposed MFA-DEBF achieves high throughput and takes less time than RSA and ECC.

5. Conclusion

This study provides an essential solution to the user and administrator in order to handle the authentication system with greater efficiency. As a result, it offers secure multifactor authentication and guards against key hazards to sensitive data by outlining the strategy for maintaining the security. In the end, encrypted data on the cloud is becoming more significant and important. The experimental results obvious that the proposed MFA-DEBF produced better performance than existing RAS and ECC algorithms. The proposed methodology improves when more individuals enter it, making it more appropriate for the current paradigm, like the cloud. All industries will eventually change some or all of their processes and data to the cloud due to the enormous benefits it offers. It will take a lot of work to establish the right security so that business may be conducted in cloud environments.

References

[1] Ahmet, O. Mustacoglul Ferhat, and C. F. Catak Geoffrey, "Password-based encryption approach for securing sensitive data," Security and Privacy, pp. 1–12, 2020.

[2] Costa, Bruno, Pedro Branco, Manuel Goulão, Mariano Lemus & Paulo Mateus 2021, "Randomized Oblivious Transfer for Secure Multiparty Computation in the Quantum Setting," Entropy, vol. 23, no. 8, p. 1001. -1

[3] Gumaei, Abdu, Rachid Sammouda, Abdul Malik S Al-Salman & Ahmed Alsanad 2019, "Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation." Journal of Parallel and Distributed Computing, vol. 124, pp. 27-40. 3

[4] Haghighat, Mohammad, Saman Zonouz & Mohamed Abdel-Mottaleb, 2015, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification." Expert Systems with Applications, vol. 42, no. 21, pp. 7905-7916. 2

[5] K. Latha and T. Sheela, "Block based data security and data distribution on multi cloud environment,"Journal of Ambient Intelligence and Humanized Computing, 2019.

[6] Kaur, Harkeerat & Pritee Khanna 2020, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," Future Generation Computer Systems, vol. 102, pp. 30-41. 5

[7] M. L. T. Uymatiao and W. E. S. Yu, "Time-based OTP authentication via secure tunnel (TOAST): a mobile TOTP scheme using TLS seed exchange and encrypted offline keystore," in Proceedings of the 2014 4th IEEE International Conference on Information Science and Technology, Shenzhen, China, 26 April 2014.

[8] M. Olalere, M. Taufik Abdullah, R. Mahmod, and A. Abdullah, "Bring your own device: security challenges and A theoretical framework for two-factor Authentication," International Journal of Computer Networks and Communications Security, vol. 4, no. 1, pp. 21–32, 2016,

[9] O. Le´on, J. Hern´andez-Serrano, and M. Soriano, "Securing cognitive radio networks," International Journal of Communication Systems, vol. 23, no. 5, pp. 633–652, 2010.

[10] Ometov, S. Bezzateev, N. M¨ akitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: a survey," Cryptography, vol. 2, no. 1, pp. 1–31, 2018.

[11] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," International Journal of Communication Systems, vol. 32, no. 6, p. e3900, Article ID e3900, 2019.

[12] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment," ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1–19, 2021.

[13] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks," in Advances in Cryptology – EUROCRYPT 2018, pp. 456–486, Springer International Publishing, Cham, 2018.
[14] S. Kaur and G. Kaur, "Threat and vulnerability analysis of cloud platform: a user perspective," in Proceedings of the 15th INDIACom; INDIACom-2021; IEEE Conference ID: 51348 2021 8th International Conference on Computing for Sustainable Global Development, pp. 508–514, New Delhi (IN-DIA), 17 March 2021.
[15] S. Nagaraju and L. Parthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," Journal of Cloud Computing, vol. 4, no. 1, pp. 1–23, 2015.
[16] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," IEEE Transactions on Dependable and Secure Computing, vol.1, p.1,2020.
[17] Singh and T. D. Singh, "A 3-level multifactor Authentication scheme for cloud computing," International Journal of Computer Engineering &Technology, vol. 10, no. 1, pp. 184–195, 2019.
[18] T. Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 6141–6149, 2021.
[19] Tarannum, Ayesha, Zia Ur Rahman, L. Koteswara Rao, T, Srinivasulu, & Aimé Lay-Ekuakille 2020, _An efficient multi-modal biometric sensing and authentication framework for distributed applications.' IEEE Sensors Journal, vol.20, no. 24, pp. 15014-15025. 6
[20] V. Singh and S. K. Pandey, "Revisiting cloud security threats: replay attack," 2018 4th International Conference on Computing Communication and Automation (ICCCA), in Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA) Greater, pp. 1–6, Noida, India, 14 December 2018.
[21] Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," IEEE Transactions on Dependable and Secure Computing, vol. 1, p. 1, 2016.
[22] Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," Science China Information Sciences, vol. 65, no. 1, 2022.
[23] Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," Computers & Security, vol. 88, Article ID 101619, 2020.
[24] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3599–3609, 2018.
[25] Zhu, L, Zhang, C, Xu, C, Liu, X, Huang, C, 2018, "An efficient and privacy-preserving biometric identification scheme in cloud computing," IEEE Access, vol.6, pp. 19025-19033. 4