Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 32s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Next-Gen Data Security Using Hybrid Cryptography and Email-Based Two-Factor Authentication

Nadakuditi Vijay Vamsi[*1], Radhika Rani Chintala [2]

[*1]department Of Cse, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, A.P, India

[2] Department Of Cse, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, A.P, India

Cite this paper as: Nadakuditi Vijay Vamsi, Radhika Rani Chintala , (2025) Next-Gen Data Security Using Hybrid Cryptography and Email-Based Two-Factor Authentication. *Journal of Neonatal Surgery*, 14 (32s), 7626-7638.

ABSTRACT

Now-a-days it must be mandatory for the organization to properly secure data using cryptographic techniques-the advancing digital communication and cloud storage. Despite the effectiveness of hybrid encryption mechanisms used in the traditional models, they are not easily implemented in the environment where there is high throughput because of the bottleneck in performance and vulnerability. An original algorithm in hybrid cryptography, ARB3, is brought forward in this paper. This next-generation algorithm combines the merits of Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and the BLAKE3 hashing algorithm. The three components brought together form a fast, secure, and efficient data protection mechanism: high speed symmetric encryption from AES, secure key establishing capabilities from RSA, and fast and secure hashing for data integrity verification from BLAKE3. This model also adds an electronic email 2FA to give an extra layer to access control and user verification: time-sensitive one-time passwords issued to their registered email account. Through rigorous test cases, ARB3 has been found to perform better as regards both encryption and decryption speed and throughput improvements over common cyber threats against traditional models. Hence, this hybrid model is scalable and robustly geared up to provide a state-of-the-art solution for contemporary applications where the demand for high-performance adaptable crypto systems is becoming more urgent.

Keywords: Hybrid Cryptography, AES, RSA, Blake3, Symmetric, Asymmetric, Hash function, two-factor authentication (2FA)

1. INTRODUCTION

Data security is a very burning question since the volume of digital data is increasing exponentially and more individuals become eager to rely on the services of cloud computing.The cryptography is essential in protection of sensitive information through maintaining confidentiality, integrity, and authenticity of information during transmission as well as storage. The conventional methods of cryptography could be categorized as symmetric key encryption which involves a single key to perform encryption and decryption and asymmetric key encryption, which involves public-private key pair to establish secure communication [1][2]. Also, hash functions enable developing data integrity verification since they entail creating a digest of any length of input [3].

Symmetric ciphers are fast and examples are AES, asymmetric ciphers are preferred where key exchange security is critical e.g. RSA [4][5]. New hashing developments have recently seen an improved performance, as well as stability on new hashing algorithms such as the BLAKE3 I However, it is also possible to improve it in some respects, as some legacy algos like MD5 and SHA-1 are also prone to failures [6]. All these techniques though bear limitations when used separately. To address these threats, hybrid cryptography where the strengths of several methods are combined together has emerged as a broad-based remedy to enhanced data security across a majority of the platforms including cloud-based data storage facilities, internet-based communications, and even financial-related systems [7][8]

1.1 Statement Problem

Even though, the present cryptographic solutions provide the basic data security, once deployed into the environment where high security levels and real-time performance are required, they might be retarded. Because Symmetric encryption is an effective algorithm, key distribution issues remain in distrustful networks because it requires the key on both sides. Asymmetric encryption is costly, so the encryption of large data sets simply could not be entrusted to it. With traditional systems admitting users into their systems with password credentials, they are thereby susceptible to phishing, credential stuffing, and brute force attacks [9]. Putting it simply, sensitive data is highly vulnerable in the cloud and web applications. Nevertheless, with numerous hybrid systems not establishing any reliable way to verify the users, attacks on security are made all the easier.

1.2 Purpose

The main purpose of conducting this research is to create and test a model of next-generation hybrid cryptography that contains AES, RSA, and BLAKE3 algorithms, which should ensure a greater level of data security and be called ARB3. The system further involves Two-Step Authentication (a.k.a. 2FA) through email with One-Time Passwords (or OTP) to enhance authentication of users. The goals in particular are:

The guarantee of high speed and safe data encryption/decryption with the use of hybrid cryptographic methods.[10]

Through the introduction of lightweight and available 2FA authentication of the user [11].

To assess the efficiency of ARB3 regarding speed, throughput and mass resistance to widespread security threats.

It provides an expandable and high performance which fits perfectly in the application at hand where security and high-speed are of paramount essence.

1.3 Study scope

This paper rests on the ground of creating feasible and secure file encryption and decryption agent that would operate within the cloud-based and high-throughput digital cyberspace. Limitation of the study:

To perform the encryption of data with AES, the security of the key with RSA, and check integrity of the data with the BLAKE3.

Coming up with an outline of an email-based 2FA system to authorize users before any support of encryption/decryption activity.

Testing of the performance to include encrypting/decrypting speed and throughput tests.

Trying out the system to the prevalent security threats such as unauthorized access and manipulating of data.

Neither biometric authentication nor post-quantum cryptographic methods are covered, but are proposed as subjects of possible future research.

1.4 Significance of Study

This research has made a wide contribution in the world of cybersecurity and cryptographic systems because it has proposed a mixture of systems that not only fix the performance impediments of conventional systems but offer better user authentication with easy strategies of 2FA[12]. This integration of the ARB3 hybrid cryptography and OTP via email forms the content of this confidentiality, integrity, and strong authentication of the system which are quite important entities in ensuring security in online transactions and in storage. The proposed solution can be implemented in the sphere of cloud computing, on secure messaging or in the financial services sector when the confidential data must be secured and the identity of the user is a critical part.Moreover, the model is scalable and efficient which qualifies it as fitting in real-time applications which is a step towards realisation of user-friendly high-performance security systems.

2. LITERATURE REVIEW

This research integrates the application of file deduplication and Advanced Encryption Standard encryption in order to enhance security properties of files. Deduplication was also implemented and was achieved by the Blake3 hashing method that enables duplicate data blocks to be discarded to maximize storage space. AES encryption provides good confidentiality with the unique files. In this particular case, it lied in the middle between a strong encryption and optimization of data. It is more viable in the issues that exist in the cloud computing, security and efficiency being the principal demands. [13]The paper focuses on the present trends in these branches, and it states that it is crucial to couple encryption and deduplication in order to provide an efficient scenario of cloud architecture which is safe.

The paper is devoted to advanced encryption processing mechanism which provides a complex of accounting data processing using modified DES algorithm [14].Through the streamlining of the system architecture in terms of hardware acceleration points and incorporating the more secure on AES algorithm as compared to DES algorithm, the authors demonstrate large time savings on encryptions tasks. This shows that in addition to making the training on information and data security more effective, proper management of encryption keys, backup, and recovery mechanisms should be put among the policies and procedures included in an organization's ISO 27001 documentation. The systems are thus improved to provide businesses with trustworthy and efficient covers to ensure the accounting data's integrity and confidentiality.

The safety of the data is necessary when we do not want the criminals to have the data at their disposal and offend them.Hybrid cryptography is the combination of both public-key and symmetric-key encryption and provides the best of both worlds: speed and security because most of the encryption is performed using a symmetric key but with the keys safety ensured by using the Beyond-the-key cryptography of the recipient. The data can be first wrapped with one layer followed by embedding this layer within layers and only the targeted audience will be able to reach the information. With growing swells in data sets, the necessity of safe storage has never been felt more acute than at present, with the orienting malware and the phishing risks on the rise. Small scale may not handle big datasets at a time, and cloud computing is gaining

popularity, however, it has its security issues as well. To alleviate these issues, the authors introduce a new method of the securement of sensitive files in the cloud based storage and compare the most often used types of encryption, such as AES, DES, and RSA algorithm in terms of their vulnerabilities. [15]

It is in the process of reading Hybrid Cryptography for Cloud Security: Methodologies and Designs [16] that I got the feeling of reading a lab manual briefly the first time I sat down to do it. Sherief H. Murad and Kamel H. Rahouma deconstruct the application of hybrid cryptography in a cloud setting, following the movements followed since 2013 to 2020 and striking application, limitation, design, and implementation of each of them. What they learned the most? It is when linked together that symmetric and asymmetric systems shine most and there is no need to note that the security and the performance may still keep on improving provided one keeps on refining that. Yea, the term hybrid cryptography usually comes with its fair share of hang-ups most memorable of which is key distribution issues and the pending cost, but Murad and Rahouma find themselves espousing a sturdy cloud hybrid that secures sensitive data. I would further investigate this research by looking into the unorganized land and figure how we could enhance the security of this land.

Everybody seems to concur with me concerning the fact that, in the current academic and research setting, it is required that data be kept confidential with increased security requirements. A combination encoding will solve that need quite successfully since it combines symmetrical and asymmetrical encryption. An example of the same thing is that it is possible to utilize symmetric key algorithms (AES) and asymmetric key algorithms (RSA) in combination; RSA is most efficient during secure key exchange process and AES is most efficient during quick and high-volume encryption and decryption phases. Run a data file through each of these two measures, and you have yourself a two-layer protection that the current studies continuously demonstrate to tighten cloud data. This has indeed been my experience in the past: once I used Protect key management in combination with RSA for strong key management, and combine with AES to get an efficient system that can be operated at high speeds, the result is a strongly-defended system.Jaspin et al. (2021) claim that using double encryption with AES and RSA significantly improves data confidentiality and integrity [17]. Swarnalatha et al. (2023) enhanced the security of sending and receiving files by performing the splitting and encryption of files even further by distributing and sending them across the cloud servers2.Key management and overhead computation issues are currently being worked on as open issues. Achieving a favourable performance-security trade-off in optimized hybrid systems will be the main focus of future research, particularly for cutting-edge technologies like blockchain and the Internet of Things.

"Secure File Storage on Cloud using Hybrid Cryptography" [18] is one of them; it examines hybrid cryptography methods to improve cloud storage input text security. 1. The suggested method encrypts and decrypts data using 3DES in conjunction with Blowfish encryption 3. A hybrid approach is used to assure improved security because the technique's recognized weakness is the weakness of a single cryptographic approach. For total protection against unwanted access, data encryption using this suggested paradigm is split into three sections that will be encrypted using various algorithms. 2. This study, in addition to discussing applicable work in the area, encompasses the various ways of encryption and their effectiveness.It also contains a descriptive discussion on the execution details of the proposed system with all its advantages as far as data integrity, very high security, authentication, and confidentiality are concerned.

Maturing data protection leads the current research to dive into hybrid crypto systems.Although difficult, creating hybrid crypto systems using combinations of symmetrical and asymmetrical techniques of encoding becomes a necessity to attain input text security. Even though with applications of asymmetric algorithms such as ElGamal and RSA, one would be able to alternate keys using secure methodologies, symmetric algorithms such as Twofish and AES are preferred due to their speed and the capacity to encrypt big sets of data. Study of combining these capabilities is already being attempted. Another example, hybrid of RSA and Twofish has shown promise of being able to shorten the ciphertext length equivalent to an improvement in output of a computing system. AES in combination with RSA is used to enhance more security in general. As a matter of fact, by delivering high encryption rates and good key management, the recent study by Kumar et al (2020) revealed that there exists a possibility of making data highly secure using hybrid cryptosystems even when applications are in cloud setting. Composites of ElGamal and symmetric ones have also been ventured into to provide resistance to error that have been caused by quantum usage.All these developments have been reached, as a matter of fact, but research areas where development still awaits are those where they address computing overhead together with key management complexity. Future developments, therefore, would be to act to improve a combination capacity or a scalability as well as achieve an optimum operation. [19]

Cloud computing revolutionized IT via services such as IAAS, PAAS and SAAS; however, they have introduced security issues, particularly authentication. Conventional methods i.e., password-based or biometrics are ineffective, as they would not stand brute force or computationally demanding attacks respectively. The paper intends to meet these challenges with a safe two-factor authentication (2FA) protocol based on one-way hashes, nonce-oriented methods and Elliptic Curve Cryptography (ECC). The given proposal has the advantage of being more secure against MITM, replay and session hijacking risks, more suitable usability by users, as well as cheaper to compute, than RSA because it utilizes ECC to employ a secure and efficient encryption usage, particularly under memory-constrained devices. Solving the problem with the idea of user IDs, salted passwords, OTPs and cloud certificates is effective since it approaches strict authentication requirements without sacrificing ease of use. The proposed model prefers sensitive data to be stored in clouds since with unauthorized access and

cyberattack safety taken into consideration, a sign indicative of a shift toward cloud security practice evolution.[20]

This paper researches on implementations of 2FA and integration of 2FA to CMU. Password vulnerability is currently a key security threat through phishing and weak password practices; therefore, 2FA would be a necessity in the safety department. The reason behind this particular user perception and behavior is the fact that CMU has been compelled to adopt the use of Duo 2FA on campus by the university. Earlier on, 2FA was a nuisance to users and they had to bear with its advantages and safeguard. Good experiences with Duo caused some of them to begin using Duo with other accounts. False beliefs, unsecure actions and design shortcomings that impede adoption are also diagnosed in literature. Prudent to ameliorate adoption rate are strategic messaging and a prudent plan that should be adopted as design agenda and mandates. Such a research study will be an asset to knowledge: It explains how a balance between accessibility and security could be sought after to facilitate the large 2FA implementation, and therefore sheds light into the field of resistance to the levels of user acceptance and efficacy system.[21]

Theoretical Analysis

This part gives a detailed description of the simplest processes behind the Advanced Encryption Standard (AES), BLAKE3 hash algorithm and reinforced RSA algorithm. It is important to have knowledge on the mechanism of these algorithms to be able to realize the usefulness of these algorithms in ensuring safety of data through hybrid cryptography.

Advanced Encryption Standard (AES)

AES is one of the most used cryptography with the symmetric form of encryption which is applied during encryption and decryption by using the same key. It belongs to the family of symmetric block ciphers, and it is famous as a fast, safe and platform-independent cipher. AES acts on block data that are of unvarying size data, to be exact 128 bits and has three key length viz, 128, 192 and 256 depending on the level of security needed.[22]

AES has an internal organization being a substitution permutation (SP) network, and the quantity of rounds that the data traversing in the encryption procedure is reliant to the key length. Namely, those numbers of rounds are 10, 12 and 14 in the case of keys of 128, 192, and 256 bits, correspondingly. [23] The four important operations that each round is comprised of are:

SubBytes (ByteSub): A value of pre-determined substitution box (S-box) is assigned to each block in it; the value of a specific block is then replaced using this value; this constructs a non-linearity over the cipher.

Row Switching (Shift Rows): In a block, the movement of the rows will be done to that of a cycle block of different offset V, so as to ensure one block has diffusion.

Column Mixing (MixColumns): In this step, it mixes the data column-wise and this further diffusion is done by performing a mathematical operation of data over finite field, GF(2^8).

Add Round Key :It is a bit task (Byte) XOR, on the output of the previous round and the round key, i.e. the extension of the encryption keys of two extended at a key expansion. This makes the transformation operation in and of itself unique and exorbitantly sensitive to the encryption key thus causing the cipher to be highly perplexing to target.

The specified amount of the successive round rotations is used and the final one does not apply the Mix Columns operation. This is the interplay shown in fig. 1. The benefit of AES is there is the blend of simplicity, speed and high level of resistance to cryptographic attacks thus AES has been adopted as a global standard in encrypting information in government, business and even personal security applications such as cryptography.

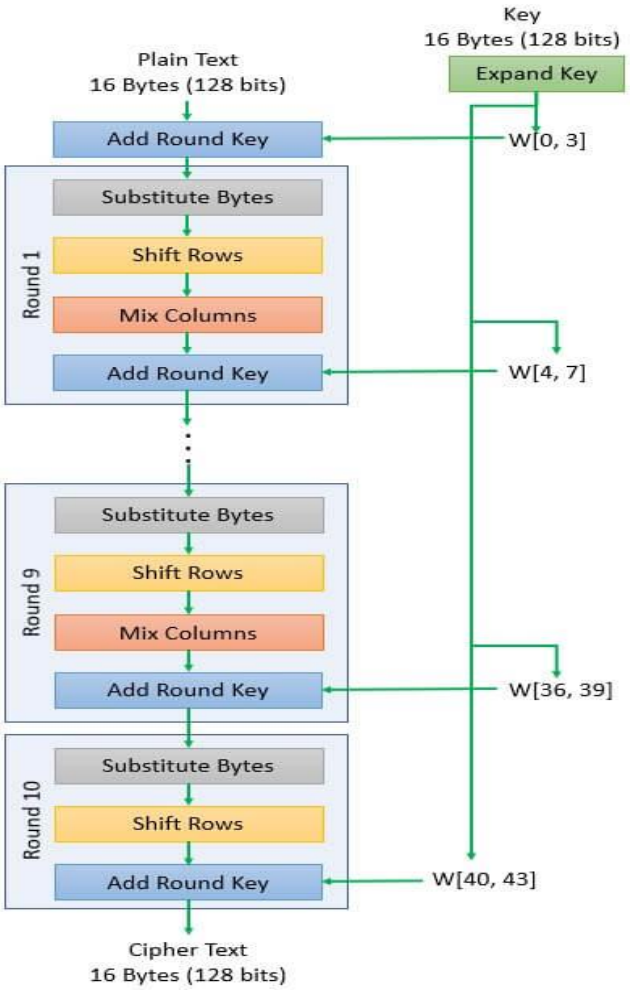

Fig 1: AES Encryption and decryption system

B. Rivest-Shamir-Adleman (RSA)

One of the simple encryptions of an asymmetric cryptographic algorithm is the RSA algorithm which has found wide recognition in both encryption of secured data and digital signatures. The RSA works with two different keys, unlike symmetric encryption algorithms, one key is publicly available (public key) the other is secret (private key) owned by recipient . The dual-key procedure makes it so that data encrypted by the public key could not be decrypted with any other key than the appropriate private key, and the reverse too, allows both creating secure communication as well as authentication of users.

Ron Rivest, Adi Shamir, and Leonard Adleman invented the RSA algorithm in the year 1977; the algorithm was named after them based on the first letters of their surnames [24]. The mathematical basis on which RSA operates is its central strength i.e. it is hard to decrypt the product of two large prime numbers and this process can be thought of being computationally infeasible using the available technology given large enough key sizes.

RSA uses the process of encrypting and decryption operations which are founded on modular exponentiation by the number theory on prime numbers. There are two powers that the algorithm uses and they get the e (the public exponent) as a component of the public key and d is the secret exponent and a component of the secret key. The formula written in the public key ciphers the Plain Text PT to ciphertext CT by using the formula CT = PT ^e mod n and the decryption follows with the help of the secret key as PT = CT^ d mod n.

Here n represents the power of product of two large prime numbers that is a very crucial component of the both the private and public key. The RSA computational scheme can be presented by Fig. 2 that describes the general way the algorithm is realized: the work of the key generation, encryption and decryption of the information. The RSA security relies on the difficulty of factoring large integer which becomes much harder when the key gets longer and modern secure systems typically use keys of around 2.048 bits or more.

Although very robust, classic RSA may be computationally costly, especially when the volumes of data processed are large

(or even limited in size) devices. Hence, refinements of the RSA tend to include employing optimization algorithm, e.g. Chinese Remainder Theorem (CRT), or utilize a hybrid encryption system in which RSA can be used to exchange a symmetric key (e.g. AES) with the advantages of both asymmetric and symmetric encryption [25].

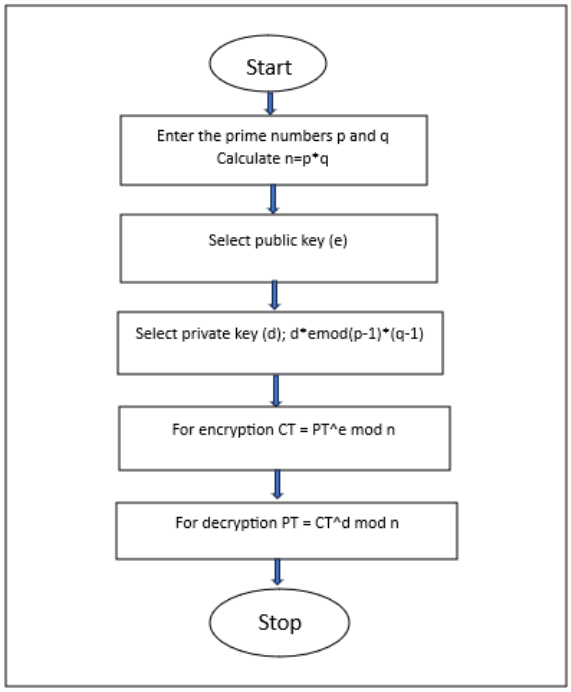

Fig 2: RSA Algorithm

C. Blake 3

BLAKE3 is a proposed cryptographic hash algorithm that shall boast of outstanding degree of performance along with the data integrity.It is set up to generate a fixed-sized hash output, allowing quick and sure data validity checks. In essence, BLAKE3 would give a unique hash or finger print of anything fed to it and this might be tested with great integrity and therefore, any alteration of the original content might be detected easily. This is why it is also an important element in safe data communication where precision and reliability is highly needed.

On speed, BLAKE3 has been found to be astonishingly quick compared to the older algorithms in hashing. To give an example, in comparison to the Keccak- one of the winners of the SHA-3 standard, it is roughly 3 times faster to compute a 512-bit hash in a modern CPU. BLAKE3 is approximately 1.26 times quicker as compared to Keccak as far as outputs of 256 bits output are concerned. These improvements are quantified in the number of cycles per byte that underlines the efficiency of BLAKE3 even when large amounts of data are involved .

BLAKE3 works through following important stages:

Data Chunking The data is broken up into small pieces or chunks, which are usually 1kilobyte. All the processing with these chunks can be done simultaneously, thus, one can accelerate the calculation. In the case of the data size below 1 KB, padding is carried on the data to achieve the chunk. The metadata in each of the chunks identifies it by its length, position in the sequence and the fact that it is the final one [26].

Compression Function: The cryptographic compression function is first applied to each of these blocks of data before being sent to the recipient and such functions include addition, bitwise XOR and bit rotations of 32-bit words. It is an entire diffusion of the input data and its creation is in BLAKE2 permutation plan. The outcome of the step assures the elimination of regularities that provide an evenly random-looking part of the hash.

Merkle Tree Construction: Every fragment of the data moves is hashed and finally the outcomes are put together to generate a binary Merkle tree. This is a hierarchy by its very nature, which enables BLAKE3 to implement a parallel processing of the information and consequent amalgamation of the obtained consequence effectively. The sink or the topmost node in tree is a hash of all the input that is added up.

Finalization: The root hash is handled under its final stage where it is handled once again into application domain and is further treated into another round of compression with application specific keys and settings. This reduces the hash to the standard 256 bits output size by cutting or padding the last hash hence uniformity in the application.

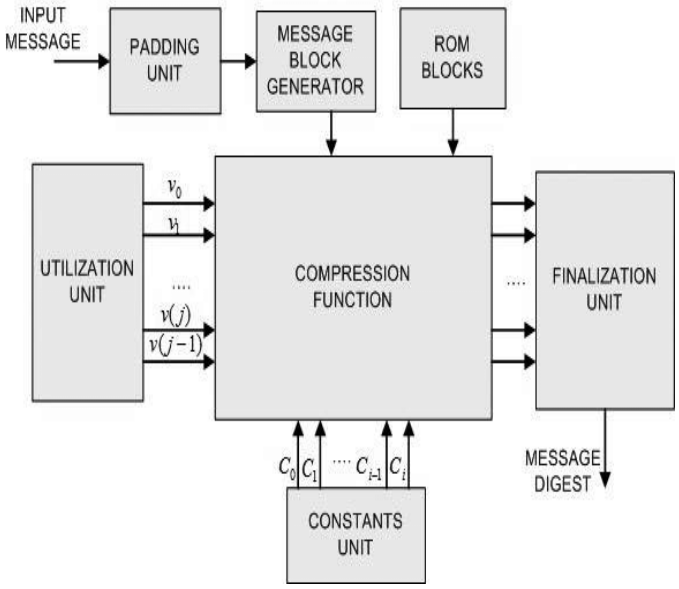

Fig 3: Architecture of the Blake3 hash function

The end product of the hashing process of BLAKE3 is the hash product of 256 bits usually presented in hexadecimal representation. This hash is a digital fingerprint of the fed data, which one can trust to verify the integrity of the data, maintain a consistency and identify any tamper activities [27].

A BLAKE3 data structure accepts input data and then hashes it to create a fixed sized hash that uniquely identifies that particular data set (as explained in Figure 3). Its robust cryptographic properties together with its speed imply that BLAKE3 is highly appropriate to operate within a hybrid cryptographic system, where fast secure integrity checks of data are required.

Practically, when using file transmission where confidentiality is required, BLAKE3 helps the system to identify modifications in files and corruption. This is implemented by computation of a hash of the original plaintext before sending and comparing it with the hash which was computed on its receipt. In case there is a match between the two hashes, it can be ensured that the data was not tampered with in transit; otherwise, there was a probably security breach or data cannot be encountered. Therefore, the proposed BLAKE3 provides high security and reliability of any data manipulation in contemporary systems of cryptography.

D. Two-Factor Authentication (2FA)

The Two-Factor Authentication procedure using the email commences when an end user logs in into the login page by a client side application e.g. web browser. The initial step entails input of the password which is usually accompanied by a username into the login box. Once this form get filled, the data has been taken to the server where it will be checked with the ones that will be existing in the user database. There is an instantaneous denial of access in case of a wrong password used [28].

Provided though, that the correct password is used, the second level of authentication comes into mobile play. The system also requires a second authentication passkey which is an OTP (One-Time Password) that is manually produced by the system, temporarily placed at the OTP keys database and then emailed to the registered account of the user. User enters this OTP itself in an application form on the client side.

Thereafter, the user proceeds to click the submit button and the OTP is sent once more to the server where it is authenticated.The OTP entered is checked by the server on the OTP in the OTP database together with the verification of its expiry or not. In case of bogus or expired OTP there is denial of access. In the places where the OTP is applicable, the server identifies the user and provides room in the system.

It is this two-step authentication that drastically amplifies security in the aspect that, even when the password is stolen, a hacker will not have the capacity of doing anything until one gets an additional access to the respective user email account. The procedure also represents an effective means of demonstrating identity for systems that handle sensitive or secure transactions as shown in Fig 4.

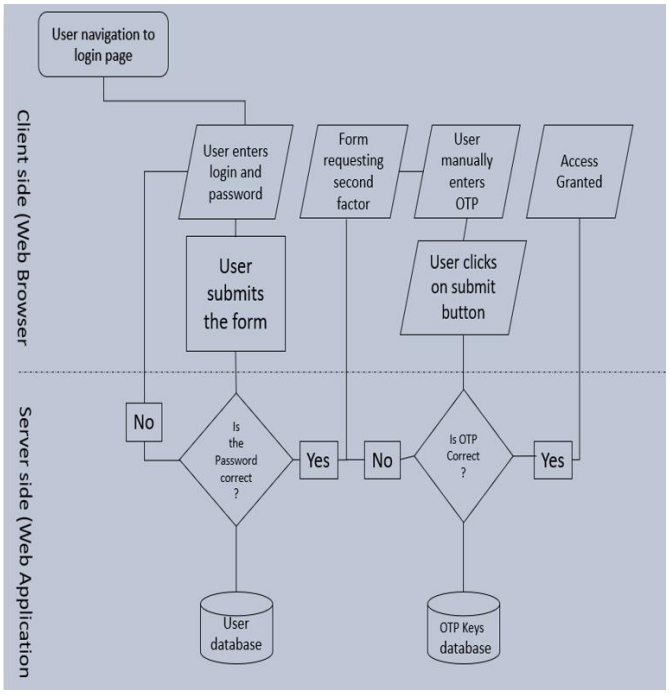

Fig 4: Architecture of Email-Based Two-Factor Authentication

3. PROPOSED METHOD

The graphical user interface of ARB3EncryptorApp program keeps secret the hybrid cryptography functionality of the application, consisting of a lot of cryptographic algorithms that have been combined to perform safe encryption and decryption of files. There is encryption of file data with the Advanced Encryption Standard (AES); AES key is strongly encrypted using the RSA algorithm; file data is hashed based on the Blake3 hash algorithm to verify data integrity; two-factor authentication by email containing a one-time password (OTP) sequel provides that only authorized users make encryption and decryption. This system represents confidentiality, strong authentication, and integrity verification as indicated in the Table 1.

Table1: - Security Parameters in ARB3 Hybrid Cryptography Model

Component	**Parameter**	**Purpose**
AES (Symmetric Encryption)	Key Size: 128 / 192 / 256 bits SP Network Rounds Byte Substitution, Row Shifting, Column Mixing, Round Key Addition.	Used for high-speed encryption and decryption of data. Number of rounds varies based on key size (10, 12, or 14). Core AES operations ensuring confusion and diffusion.

RSA (Asymmetric Encryption)	Public and Private Key Pair (e.g., 2048 bits)	Secures the AES key during transmission (key exchange).
BLAKE3 (Hash Function)	Hash Output Length (256 bits default)	Ensures data integrity and provides a digital fingerprint.
Two-Factor Authentication (2FA)	Email-based One-Time Password (OTP) Time-sensitive Code	Adds an extra verification step for access control. OTPs expire after a short period for added security.

3.1 Main Components and Functionalities

The usage is started with the file selection that enables the user to search and select any file on his system. When a file is picked, it goes through RSA key generation that creates a set of 2048 bit RSA key; the public key is used to encrypt the AES key which is used in the encryption process and the private key that is used to decrypt the AES key which is used in the decryption process. Besides the RSA key generation itself, a secure digest of the original file is generated in the course of database encryption targeting the Blake3 hashing algorithm. This digest will be retained and compared later when decrypting for file integrity. For key security, the application uses PBKDF2 (Password-Based Key Derivation Function to derive a secure AES key from a password provided by the user, and random salt is used to resist brute-force attacks.

3.2 Encryption Process (Hybrid Cryptography)

The password, email address, and file path are provided to the user when it is being encrypted. The user will be required to accept a secure one-time password (OTP) which would be sent to the corresponding email address he/ she has provided.When successful entry of the password is confirmed, the process goes ahead and generates AES key through PBKDF2 and then goes ahead to encrypt the file via AES algorithm using CBC cipher method.It then encrypts the AES key with RSA public key cryptography. The output of the process is three files; one containing the email address in the future in the form of ".mail file, an encrypted file with a ".enc" added after the file name, and another file called file.hash containing the file Blake3 hash.User notification is also sent when the encryption process is complete as shown in Fig 5.

3.3 Decryption Process with OTP Verification

The user selects the .enc file to be decrypted. The related files with extension. mail and .hash files are automatically sought by the program. It forwards a fresh one-time pass word (OTP) to the electronic mail id after by checking the e-mail address coming from the .mail file. OTP confirmation has to be made again so that decryption takes place. After successful authentication, the AES key is decrypted with the help of the RSA private key, and the abovementioned AES key can be used to decrypt the encrypted file. After the padding is removed, the result is saved in a.dec document where it reports that this is the decrypted copy of the original file which is presented in Fig 5.

3.4 OTP-Based Two-Factor Authentication (2FA)

OTP is some arbitrary one-time password that is created, during both encryption and in the decryption. The OTP is transmitted using the smtplib to the email of the user with SMTP. Thus, the authentication details of the email sender have to be set up in the software. The layer of authentication here makes this a second factor authentication and that is even supposing the file somehow with the encryption in it got decrypted with no authorised access in Fig 5, nobody would be able to go on to decrypt it unless he/she had access to the email account of the user.

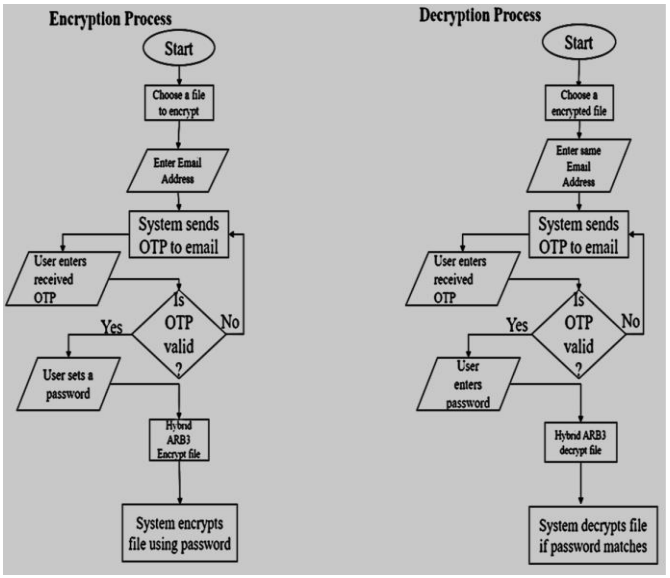

Fig 5: Proposed ARB3 and Email-Based Two-Factor Authentication Flowchart

3.5 Security Highlights

The hybrid encryption model is operated through this application by synergizing the superior speed and efficiency of symmetric AES encryption with the secure key exchange process of the RSA encryption scheme. User authentication is enforced with two-factor authentication (one-time password plus password). It uses Blake3 hashing to verify tampering with the file against the integrity of the file. PBKDF2 also resists the brute-force attack, which provides another mechanism to the whole encryption procedure.

4. RESULTS AND DISCUSSION

4.1 Final Output with Results: -

The encryption processing via the ARB3 Encryptor App results in three output files .enc hash and .mail invariably. The .enc file is the secure encryption of the original data with the help of AES encryption which ensures confidentiality. The .hash file contains the Blake3 hash of what the content was: a kind of digital fingerprint to verify the file integrity. The .mail file would store the email of the intended individual to receive the information, for utilization in the OTP-based two-factor authentication as shown in Fig 8. It subsequently employs the AES key one is able to extract from the users and decrypts the contents, before writing out to a .dec file that contains the recovered fully restored original file. A hash comparison is done between the .hash file and the freshly decrypted contents to verify data integrity as shown in Fig 9.

A)EncryptionProcess

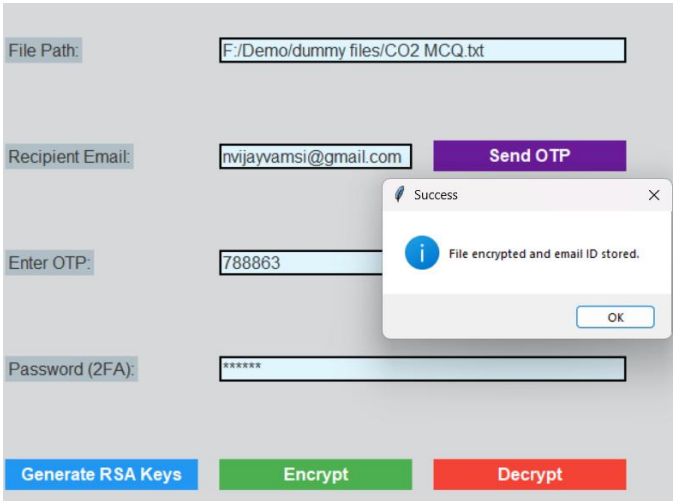

Fig 6: Encryption Time

B)DecryptionProcess

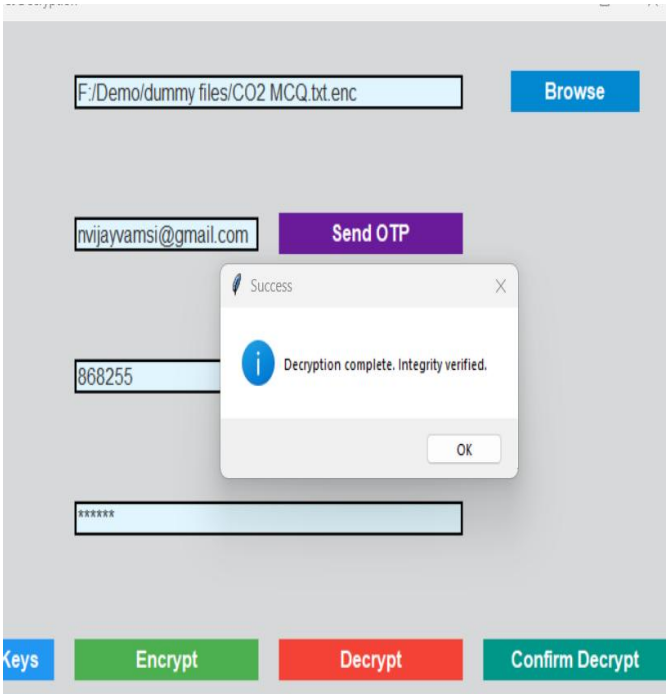

Fig 7: Decryption Time

5. CONCLUSION AND FUTURE SCOPE :

The proposed hybrid ARB3 cryptographic model-an amalgamation of the AES for high-speed encryption, the RSA for secure key exchange, and BLAKE3-for fast, reliable hashing, combined with email-based two-factor authentication-forms an effective and secure solution for the modern needs of data protection. Regarding cloud-based and high volumes of application performance, the idea will enable the confidentiality, integrity, as well as the authentication of the information. The performance outcomes show that ARB3 is faster than all the encryption and decryption of its predecessor, not to mention that it is resistant to the prevalent cyber threats which, therein, is a more than adequate testament to its scalability and real-life utility.

In the case of verifying identity, the future way of enhancing the ARB3 will be to add some sort of biometric based authentication or authorization in order to maintain a constant layer of defense to the security as far as verification is concerned. The different potential line of future extension of ARB3 may be viable to support real time application in Internet of Things (IoT), edge computing devices and bring light to life and powerful cryptographic algorithms. One can also verify the model against the threat of quantum computers and maybe in the future it will be against the threats with post-quantum cryptographic algorithms.. This is another area of application in secure messaging, cloud APIs and secure file shares etc that would assist we get some publicity as well as further strengthen its impact in different business sectors.

REFERENCES

[1] H. Sharma, R. Kumar and M. Gupta, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/INOCON57975.2023.10101044.

[2] V. Verma, P. Kumar, R. K. Verma and S. Priya, "A Novel Approach for Security in Cloud Data Storage Using AES-DES-RSA Hybrid Cryptography," 2021 Emerging Trends in Industry 4.0 (ETI 4.0), Raigarh, India, 2021, pp. 1-6, doi: 10.1109/ETI4.051663.2021.9619274.

[3] K. Tajane, R. Pitale, S. Zambre, H. Huda, A. Utage and V. Dhar, "Efficient Cloud Data Deduplication with Blake3 and Secure Transfer using AES," 2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2024, pp. 572-579, doi:10.1109/ICPCSN62568.2024.00096.

[4] Z. Li, "Exploration on Accounting Data Encryption Processing System Based on DES Algorithm," 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), Ballari, India, 2023, pp. 1-6, doi: 10.1109/AIKIIE60097.2023.10389923.

[5] C. Susmitha, S. Srineeharika, K. S. Laasya, S. K. Kannaiah and S. Bulla, "Hybrid Cryptography for Secure

File Storage," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1151-1156, doi: 10.1109/ICCMC56507.2023.10084073.

[6] Murad, Sherief & Rahouma, Kamel. (2022). Hybrid Cryptography for Cloud Security: Methodologies and Designs. 10.1007/978-981-16-2275-5_7.

[7] K. Jaspin, S. Selvan, S. Sahana and G. Thanmai, "Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm," 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2021, pp. 791-796, doi: 10.1109/ESCI50559.2021.9397005.

[8] V. Sharma, A. Chauhan, H. Saxena, S. Mishra and S. Bansal, "Secure File Storage on Cloud using Hybrid Cryptography," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702323.

[9] E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems," 2020 IEEE East-West Design & Test Symposium (EWDTS), Varna, Bulgaria, 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.

[10] S. A. Ahmad and A. B. Garko, "Hybrid Cryptography Algorithms in Cloud Computing: A Review," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.

[11] Od, Zina & Derdour, Makhlouf & Bouhamed, Mohammed Mounir. (2024). Improving Resource Security by Integrating Authentication and Cryptography. 1-8. 10.1109/ECTE-Tech62477.2024.10851191.

[12] omwoyo, R., Kamau, J., & Mgala, M. (2022). A review of Two Factor Authentication Security Challenges in the Cyberspace. International Journal of Advanced Computer Technology, 11(5), 1-6. Retrieved from https://ijact.org/index.php/ijact/article/view/112

[13] Y. Sharma, H. Gupta and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 898-902, doi: 10.1109/AICAI.2019.8701398.

[14] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 1635-1638, doi: 10.1109/WiSPNET.2016.7566416.

[15] B. P. Gajendra, V. K. Singh and M. Sujeet, "Achieving cloud security using third party auditor, MD5 and identity-based encryption," 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 1304-1309, doi: 10.1109/CCAA.2016.7813920.

[16] B. Swathi, S.D Bhaludra, S. Raveendranadh, “Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm”, International Journal of Advance Research in Science and Engineering 6(11), 2017.

[17] Kumar, Sanjeev & Karnani, Garima & Gaur, Madhu & Mishra, Anju. (2021). Cloud Security using Hybrid Cryptography Algorithms. 599-604. 10.1109/ICIEM51511.2021.9445377.

[18] Baqtian, H & Ali Al-Aidroos, Naziha. (2023). Three Hash Functions Comparison on Digital Holy Quran Integrity Verification. 11. 1-7.

[19] F. Kahri, B. Bouallegue, M. Machhout and R. Tourki, "An FPGA implementation of the SHA-3: The BLAKE hash function," 10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13), Hammamet, Tunisia, 2013, pp. 1-5, doi: 10.1109/SSD.2013.6564030.

[20] kaur, Sandeep & Kaur, Gaganpreet & Shabaz, Dr. Mohammad. (2022). A Secure Two-Factor Authentication Framework in Cloud Computing. Security and Communication Networks. 2022. 1-9. 10.1155/2022/7540891.

[21] Colnago, Jessica & Devlin, Summer & Oates, Maggie & Swoopes, Chelse & Bauer, Lujo & Cranor, Lorrie & Christin, Nicolas. (2018). It's not actually that horrible: Exploring Adoption of Two-Factor Authentication at a University. 1-11. 10.1145/3173574.3174030.

[22] Lu, C. C., & Tseng, S. Y. “Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application Specific Systems, Architectures and Processors”, 2002. Proceedings. The IEEE International Conference on (pp. 277285).

[23] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 1635-1638, doi: 10.1109/WiSPNET.2016.7566416.

[24] Kumar, Sanjeev & Karnani, Garima & Gaur, Madhu & Mishra, Anju. (2021). Cloud Security using Hybrid Cryptography Algorithms. 599-604. 10.1109/ICIEM51511.2021.9445377.

[25] F. J. Aufa, Endroyono, and A. Affandi, “Security System Analysis in Combination Method: RSA Encryption

and Digital Signature Algorithm," Proc. - 2018 4th Int. Conf. Sci. Technol. ICST 2018, vol. 1, pp. 1–5, 2018, doi: 10.1109/ICSTC.2018.8528584.

[26] F. Kahri, B. Bouallegue, M. Machhout and R. Tourki, "An FPGA implementation of the SHA-3: The BLAKE hash function," 10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13), Hammamet, Tunisia, 2013, pp. 1-5, doi: 10.1109/SSD.2013.6564030.

[27] Baqtian, H & Ali Al-Aidroos, Naziha. (2023). Three Hash Functions Comparison on Digital Holy Quran Integrity Verification. 11. 1-7.

[28] Melo, Laerte & Amaral, Dino & Albuquerque, Robson & de Sousa Junior, Rafael & Sandoval Orozco, Ana & García Villalba, Luis. (2024). A Secure Approach Out-of-Band for e-Bank with Visual Two-Factor Authorization Protocol. Cryptography. 8. 51. 10.3390/cryptography8040051.