


Research Article

Harnessing Rubik's Cube Algorithm for Counteracting Man-in-the-Middle Attacks

Syeda Wajiha Zahra¹, Mudassar Ali Zaman¹, Muhammad Nadeem^{2,*} , Waqas Ahmed¹, Ali Arshad³ and Saman Riaz³

¹Department of Computer Science, Alhamd Islamic University, Islamabad, Pakistan

²Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing, China

³Department of Computer Science, National University of Technology, Islamabad, Pakistan

E-mail: nadeem72g@gmail.com

Received: 17 March 2024; **Revised:** 10 May 2024; **Accepted:** 23 May 2024

Abstract: In today's world, businesses and individuals alike rely on cloud computing for storing and accessing data. However, with the growing number of cyber threats, it is crucial to prioritize cloud security. Despite various algorithms designed to prevent cyber-attacks, attackers have developed advanced tactics to bypass security measures. That's why it is essential to understand the three primary platforms of cloud computing and how they work together to create a seamless environment. Cloud cryptography is a highly effective method for encrypting data and enabling authorized users to access it securely. With the aid of an algorithm and a key, cryptography transforms plaintext into ciphertext, providing a defence mechanism against malicious third parties. The use of cryptographic methods ensures that only authorized entities can access the data exchange. Data encryption is a recognized and efficient security tool for safeguarding an organization's information. By converting data into a code that can only be accessed or interpreted by someone with the correct encryption key, data encryption provides a reliable defense against cyber threats. Cloud computing services, such as email, calendars, Skype, and WhatsApp, are becoming increasingly essential to our daily activities. These services allow us to store and manage data on the cloud infrastructure, enabling remote access to our data from anywhere at any time. Before cloud computing, accessing data relied on client-server computing. However, with cloud computing, we have access to a decentralized network of servers worldwide that work together to create a seamless environment. In conclusion, protecting data is crucial, and with the growing number of cyber threats, it is essential to prioritize cloud security. By implementing effective data encryption and cloud cryptography, individuals and organizations can safeguard their information and data from malicious attackers.

Keywords: cryptography, malware, man-in-the-middle, cyber security, Rubik, social network, application, attacks

1. Introduction

In today's digital landscape, storing and retrieving data has become a critical component of our daily lives. Cloud computing has emerged as a popular method for achieving this, enabling users to access their data from any location and at any time. However, the safety and security of this data are of utmost importance to businesses, with external threats posed by attackers proving to be a major concern [1]. Though security measures have been put in place, attackers have developed advanced tactics that can bypass them, making it crucial for businesses to remain vigilant [2]. The cloud computing infrastructure is composed of three primary platforms, each with its unique role. The first layer is the central hub for installing and maintaining all services,

Copyright ©2024 Syeda Wajiha Zahra, et al.

DOI: <https://doi.org/10.37256/rrcs.3120244605>

This is an open-access article distributed under a CC BY license
(Creative Commons Attribution 4.0 International License)

<https://creativecommons.org/licenses/by/4.0/>

allowing for seamless communication between the various services [3]. The second layer comprises the platform layer, where operating systems are located and perform their functions. Lastly, the software layer is responsible for delivering the user interface, while the endpoint layer is solely designed for tasks related to administration and communication within the organization and is not accessible to users [4]. The cloud is essentially a global network of computers, with each server serving a unique function. While the term "cloud" may seem ambiguous, it is simply a conceptual entity made up of a decentralized network of servers located all over the world that work together to create a seamless environment [5]. Cloud computing services like email, calendars, Skype, and WhatsApp have become essential to our daily operations, with remote accessibility being a key feature [6]. This allows users to store and manage their data on the cloud infrastructure and access it through the internet from any place and at any time [7]. Before cloud computing became widely available, client-server computing was the primary method of computing [8]. Clients received data from a specific server to which they were connected, and the server used and modified resources as needed [9]. Clients could access the server's resources and obtain specific data by establishing a connection between their computer and the server's computer key [10]. The concept of cloud computing originated from the use of client-server architecture and distributed applications [11]. Cloud computing has become an integral part of our daily lives, and it is crucial to prioritize its safety and security [12]. The threats posed by external sources may seem overwhelming, but by taking a vigilant approach and implementing robust security measures, businesses can safeguard their data and continue enjoying the benefits of cloud computing [13]. Cloud cryptography is a highly effective method for data encryption, enabling authorized users to access and transmit information securely [14–16]. Cryptography is the science of encoding data to ensure the privacy and security of communication [17]. By using an algorithm and key to transform plaintext into ciphertext, cryptography provides a defense mechanism against potential security breaches [18]. When devices communicate with each other, it is good practice to use a cryptographic protocol to encrypt the data being transferred, ensuring only authorized entities have access to the data exchange [19–21]. With the widespread use of different devices in our daily lives, the need for secure connectivity is more crucial than ever, and cryptography is the key to ensuring secure communication [22]. In today's digital age, protecting an organization's sensitive information is paramount. Cybercrimes are on the rise, and to ensure network security, it is crucial to adopt a robust security tool [23]. Data encryption is a widely recognized and effective security approach that can help protect your information [24]. By converting data into a code that only authorized personnel can interpret, encryption ensures that unauthorized attempts to access the data will fail [25]. The information remains unclear and jumbled, thereby protecting it from hackers and other malicious actors [26]. Decryption, on the other hand, is the process of converting this code back into a meaningful format. So, if you want to prevent unauthorized access to your sensitive data, data encryption is a crucial procedure that you should consider implementing [27,28].

1.1 Motivation

Countless data breaches have occurred in recent years, emphasizing the importance of secure data transmission. Researchers have proposed a variety of data-securing techniques and algorithms, but none have fully eliminated limitations [29,30]. That's where our hybrid encryption algorithm comes in. By combining an existing image encryption and decryption algorithm with another cipher, we have developed a technique that enhances data security. What sets our approach apart is that we have repurposed an image encryption algorithm for text hybridization, which significantly strengthens overall security. Unlike previous approaches that have used Symmetric Key encryption or Asymmetric key encryption, our algorithm utilizes the ASCII table and other methods to manifold the encryption process. With our hybrid encryption algorithm, we have effectively eliminated existing limitations to create a more secure solution for data transmission.

1.2 Limitation

There have been numerous attempts by researchers to secure data using various single and hybrid algorithms. However, conventional techniques have become vulnerable over time, making them easy targets for cyber attacks.

Another hybrid algorithm that has been created combines Caesar Cipher and Vigenere Cipher, as discussed in [31]. While this algorithm has been successful, it did not manipulate the text before converting it into encrypted form, such as converting it into ASCII equivalents or binary and decimal inversion. In [32], a hybrid cipher encryption integrating Polybius cipher and Vigenere cipher was established. The plaintext underwent

Vigenere cipher before completing the process with Polybius cipher. Though this technique was effective, it had limitations, including initiating all ciphers directly on plaintext without devising them.

To combat this issue, researchers have explored new methods, including using chaos-based algorithms for image encryption, as described in [33]. This approach involves permutation techniques and a nonlinear map to replicate pixels, which has proved successful for image encryption but has not yet been applied to text encryption, making it a novel area of research.

Researchers are actively working to improve data security through innovative approaches. These studies provide valuable insights into the strengths and limitations of various encryption techniques and highlight the need for continued research and development in this critical area.

1.3 Contribution

In today's world, safe communication is of utmost importance. That's why we've constructed a structured cryptography technique that ensures your messages are secure. Using the RC (Rubik's Cube) algorithm, which has been successfully used for image encryption, we've devised a way to encrypt text messages as well. Our process involves converting plaintext into ASCII values, which are then transformed into 8-bit binary. Next, we invert the binary bits using complementation and convert them into decimals, which are then transformed into matrices. The RC algorithm is performed on these matrices, shifting every element, and then a Columnar Cipher is applied, transposing all the matrices. Finally, we convert the elements back into ASCII equivalents to obtain the ciphertext. With our technique, you can rest assured that your messages will be completely encrypted and secure.

The execution of the Rubik's Cube method will unavoidably result in an extra computing burden owing to the complicated steps needed for manipulating the information. This will result in a substantial decrease in the speed and effectiveness of the encryption and decryption procedures, demanding a greater allocation of processing resources. Hence, it is crucial to handle the Rubik's Cube algorithm keys with extreme caution to guarantee the safe creation, distribution, and retention of the keys used for Rubik's Cube operations. To sustain the security of the encrypted data, it is essential to ensure that the keys are kept secure and well-protected.

1.4 Proposed Solution

This work presents a highly efficient cryptographic approach that offers robust protection for sensitive data, secures cloud data from potential threats, and ensures reliable data transmission in a dependable context. The process involves acquiring raw text and encoding it using a predetermined key. The data encryption process utilizes an ASCII table. If any unauthorized entity tries to intercept the data, it will be quite simple for them to decrypt the encryption produced by just one cipher using conventional methods. However, by utilizing multiple ciphers and protocols, it is possible to significantly enhance the level of data security. This approach can significantly prevent any potential attacker from compromising the data. The process commences by translating the original text into ASCII values, which are then transformed into binary bits by an additional process. Before converting these binary digits into decimals, they are inverted through the use of the 1's complement. This research is unique in that it uses the Rubik's Cube method for shifting the inverted binary bits, which are then converted into matrix form and manipulated using various matrix operations. This is the defining characteristic of the paper. After performing these matrix operations, the matrix elements will be reconverted into ASCII values. By following these techniques, we successfully obtain the ciphertext. Researchers have proposed numerous methods to protect data and its transfer. However, attackers continue to create novel tools and methodologies to violate data security and compromise privacy. Employing various cryptographic algorithms in conjunction with enhanced protocols can provide a feasible solution to protect data with an increased level of efficacy.

2. Literature Review

The study [24] presents a defensive architecture to lower the risk of threats that can adapt to their environment. Through the use of a technique that is very efficient, this architecture was purposely developed to minimize the impact of external threats. After that, the procedure is shown graphically on a map, and it is possible to evaluate it with the help of a tool. The results of the tests will give a helpful insight into the efficiency of the design that was inferred.

We will offer a comprehensive explanation of the use of a double encryption strategy to guarantee the secure transmission of data in the next article [25]. Before that, the XOR encryption of the plain text will be followed by the use of the salt technique.

Within the scope of the investigation [26], a network architecture that has undergone significant optimization is used. A clustering method that is only partially supervised is included in this design. This strategy pays careful attention to user answers both within and outside of the cloud server, and then applies certain policies and processes depending on those replies to maximize productivity.

What was recommended in the prior article [27] is A hybrid encryption and decryption method that was created by merging the concepts of the Caesar Cipher and the Vigenere Cipher approaches. To evaluate the proposed design's performance with well-known ciphers like the Caesar, Vigenere, and Hill ciphers, MATLAB simulations were carried out during the design process.

The Vigenere Cypher method is one of the cryptographic approaches that has been proposed as a potential candidate for inclusion in the research [28]. However, there is a problem with this technique, and that weakness is that the encryption key is duplicated. The vulnerability makes it possible to easily predict the ciphertext by the use of the Babbage-Kaiseki method. The encryption key may be obtained by using a combination of the Caesar Cipher and the Hill Cipher techniques. This will help to avoid the occurrence of the issue. Because of this, the vulnerability of the Vigenere Cipher method is expected to be concealed.

In this study [29], a novel hybrid security cipher is presented. This cipher is a combination of the Polybius Cypher and the Vigenère Cipher, which results in increased security in comparison to traditional ciphers. The study suggests that the standard Caesar cipher may be improved by using the Goldbach code method to compress the ciphertext, which would increase the level of security required.

By using a hybrid algorithm that combines the Caesar and Hill cryptosystems, the purpose of this study [30] was to improve the level of data security that is now available. The success of the strategy is shown by the results of the tests, which demonstrated a considerable decrease in the amount of time required for processing encryption and decryption techniques.

A method for encrypting images is presented in this paper [31], which makes use of optical chaos and DNA Rubik's cube scrambling to accomplish the encryption in question. The purpose of this endeavour is to enhance the effectiveness of encrypting bit planes while simultaneously increasing the complexity of the optical chaotic sequence that is produced as a result.

The multi-image encryption approach that is presented in the publication [32] makes use of a hyperchaotic map in addition to a three-dimensional cube. The construction of the system is based on the foundation that the cube graph may be created by combining planes.

The Chebyshev and Logistic maps are used to produce a new two-dimensional chaotic map, presented in the study [33]. To verify the wide range of chaos and long-term ergodicity that is shown by the recommended map, performance research is being conducted. Furthermore, a unique method for encrypting photos has been developed. This method includes the chaotic map, the Brownian motion model, and the transformation of the Rubik's Cube.

The purpose of this study [34] is to evaluate the impact that encryption delay has on the TCP and UDP transport protocols that are used in a software-defined networking (SDN) environment.

In the paper [35], a variety of data security methods are presented. These solutions provide substantial protection against unauthorized access. Initial steps include the creation of a specialized ASCII table that gives each index a value that is distinct from the others. The use of the given ASCII table might potentially be of assistance to an attacker in the process of decrypting the data during their decryption attempts. The use of a radix 64-bit encryption approach is employed to enhance security. This strategy leads to a twofold rise in the quantity of cipher data in comparison to the initial data.

2.1 Comparative Analysis

To ensure the safety and security of data, various algorithms and methods have been employed by specialists, which have yielded positive results thus far. However, with time, cybercriminals have become more sophisticated in their methods of illegally collecting and manipulating data. Therefore, we must implement advanced techniques to stay ahead of these threats. Upon conducting a thorough investigation, it was discovered that a significant number of researchers were utilizing outdated and traditional techniques for encryption and decryption of data. These approaches involved treating characters as plaintext and transforming them into

ciphertext as quickly as possible using different cryptographic systems. In contrast, this research proposes a revolutionary approach by leveraging a methodology from a previously published academic paper. This new strategy involves transforming the plaintext into an unrecognizable format using the picture encryption technique before converting it into ciphertext. Such a transformation takes place before the ciphertext conversion, thereby demonstrating a unique and innovative approach to the problem at hand. The purpose of this innovative strategy is to ensure the safety and security of data stored in cloud computing systems through the use of cutting-edge methods. To effectively prevent data access and disturbance by potential attackers at all stages, the use of multiple strategies is necessary. Relying solely on a single tactic could enable attackers to easily overcome it in Table 1.

Table 1. Comparative Analysis.

Sr#	1	2	3	4	5	Proposed Work
References Year	[29] 2020	[28] 2020	[27] 2021	[26] 2021	[24] 2021	
Proposed Algorithm	Caesar cipher with Goldbach code compression	Hybridizing Polybius Cipher and Vigenère cipher	Combination of Caesar cipher, hill cipher, and Vigenère cipher	Hybridizing Caesar Cipher and Vigenère cipher	Advanced hill cipher algorithm with the involutory key matrix	Rubik's Cube algorithm with Columnar Cipher
Novelty	The encrypted text is reduced using the Goldbach G0 algorithm.	These ciphers are immune and hard to decode since their creation procedure is complicated, scattered, and cluttered.	Implemented a comprehensive range of data protection measures.	The MATLAB simulations assessed parameters such as letter frequency and graph behavior.	Both Ciphers are used for image encryption	Triple the value of every letter in the ciphertext, then generate a key from each text.
ASCII Table	Not Used	Not Used	Not Used	Not Used	Not Used	Standard
Research Gap	No text manipulation before converting the plaintext into ciphertext	This approach is vulnerable to straightforward decryption.	No recent advancements have been made in this algorithm.	Performing letter-by-letter swapping and modeling may be time-consuming and accurate for large communications.	Appropriate just for encrypting main keys.	Identified all gaps
Proposed paper Solution	Symmetric and Asymmetric cryptography	The ciphertext generated by the proposed technique is particularly resistant to decryption.	Creating an encryption key using the Vigenere cipher algorithm	Caesar and Vigenere Ciphers use line length to increase efficiency by shifting shift places.	maybe appropriate for written content.	All gaps are resolved

2.2 Novelty of Proposed Paper

To address the constraints that were discovered in earlier research articles, the study makes use of conventional ciphers in addition to novel approaches. It will be considerably harder for an attacker to breach any communication channel and compromise the data if these refined tactics are used. As a result, the chance of the data being used without authorization will be reduced. There is a possibility that traditional ciphers, such as Ceaser, Vernam, Columnar, and others like them, are at risk of weaknesses and display certain deficiencies. To overcome these weaknesses, we developed a method that has the potential to be further strengthened by including more security features in these ciphers.

Undoubtedly, hybrid encryption is the optimal method for enhancing security. By combining numerous encryption techniques, this approach provides a substantially elevated degree of security against many forms of crimes, beyond the protection offered by utilizing a single method. The hybrid algorithms are specifically designed to possess more flexibility and adaptability when confronted with various encryption or decryption conditions. They can integrate the advantages of many approaches to enhance performance and security according to unique needs. inevitably hybrid encryption is the optimal choice for guaranteeing exceptional security.

2.3 Problem Statement

A team of researchers has developed encryption methods to safeguard cloud-stored data from unauthorized access and potential attacks. The researchers employed matrix-based methodologies using ASCII tables to

achieve data encryption. While obtaining information in ciphertext format using a pre-existing ASCII table is feasible, it is not practical to maintain the data through its usage. To enhance data security, researchers have attempted to use a single randomized key for both data encryption and decryption. However, this approach does not guarantee absolute privacy for the data. To add an extra layer of information safety, one may use just a single key for encryption and two keys for decryption. A consortium of mathematical professionals has developed an algorithm by integrating multiple algorithms and using a distinct key in each of them. While these techniques can be used in any algorithm, data encryption may not always be entirely secure. The only reliable method to protect data from unauthorized access is to employ a range of modern methods and techniques that strengthen the data, making it challenging for potential attackers to obtain it.

3. Proposed Methodology

This article proposes the use of a combination of the Rubik's Cube method and the Columnar Cipher (Transposition Cipher) to ensure secure transmission and transfer of data and information. With this approach, any unauthorized individual attempting to breach the organization's security will face formidable challenges that significantly diminish their likelihood of success.

3.1 Work Overflow

During the process of data transfer, malevolent entities often employ various tactics to gain unauthorized access to sensitive information. To address this pressing issue, a hybrid cipher method has been devised to safeguard data from potential breaches. The central objective of this method is to thwart unauthorized exploitation or retrieval of data by unauthorized entities and ensure that only authorized individuals can access it. This encryption technique involves several steps, including the extraction of raw text, its transformation into ASCII equals, conversion into binary digits, and inversion using the 1's complement method. The next step involves converting these inverted bits back into decimal numbers and expressing them as matrices, which are then subjected to the Rubik's Cube technique to rearrange the matrix elements. To further enhance the complexity of the encryption, a Columnar Cipher, a type of Transposition Cipher that rearranges the matrices, is utilized. The transposed components of the matrices are then translated back into their respective ASCII equals, resulting in the production of the Cipher text.

3.2 Data Encryption

To ensure a secure encryption of plain text, maintaining the original meaning, avoiding the introduction of any additional information or segments, and preventing the loss of essential facts are of paramount importance. Additionally, it is vital to retain the same degree of formality as the original information when rephrasing it. The process of generating Cipher text involves transforming the ordinary text into its corresponding ASCII values, which are then negated using 1's Complement to obtain reversed binary digits. The reversed binary digits are then converted into decimal numbers and portrayed as matrices, which are subjected to the Rubik's Cube algorithm to rearrange their components. Furthermore, to further enhance the complexity, a Columnar Cipher, which is a Transposition Cipher, is applied to transpose the matrices. Finally, the transposed components are reconverted to their corresponding ASCII values, thereby producing the Cipher text as illustrated in Figure 1. The complete steps for data encryption has been discussed in Algorithm 1.

Algorithm 1. Encryption

Input: Plain text

Output: Cipher text

1. We have a plain text.
 2. Convert the plaintext into the corresponding ASCII characters.
 3. Following a binary operation, the binary digits will be reversed using the 1's complement.
 4. Next, the inverted components will be converted into decimal integers.
 5. Furthermore, the decimal numbers will be represented as matrices, and the Rubik's Cube technique will be used to manipulate the components of the matrix. Subsequently, the components will be reorganized using a pair of 128-bit keys.
 6. After the shuffling procedure, the matrices will use a Columnar Cipher that functions according to the Transposition Algorithm.
 7. Additionally, the development text will be transformed into ASCII equivalents.
 8. The message that was encrypted is now acquired.
-

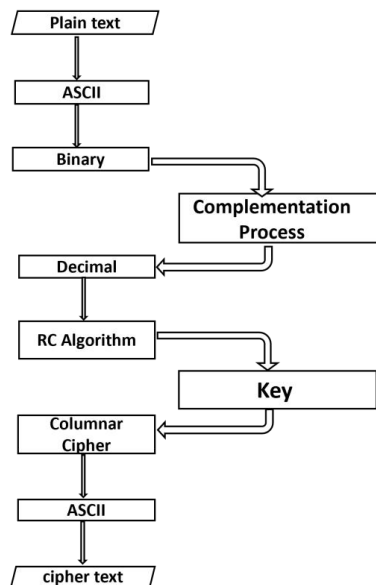


Figure 1. Data Encryption

3.2.1 RC (Rubik’s Cube) Algorithm

The Rubik's Cube has inspired the concept of the Rubik's Cube adaption, which is a puzzle that involves manipulating its components to reorganize their placement and achieve a configuration that is hard to comprehend. This same concept is applied to shuffle pictures by rearranging their pixels, producing a chaotic appearance. The Rubik's Cube transformation technique is used to achieve this, where the XOR operator is utilized with a distinct key to modify the odd rows and columns of the image, making it challenging to decrypt both the original and encrypted pictures. The even rows and columns are then encoded in reverse order using the same key.

The Rubik's Cube can be manipulated to produce a predefined or disrupted configuration. The concept of the Rubik's Cube transformation has been widely researched in a variety of publications, primarily focused on image encryption. To encrypt text, this technique is used by connecting each character in the text to a specific spot on the cube. Consequently, each segment of the cube represents a character in the text, which is then reorganized according to a spinning rule, producing a chaotic phrase. The receiver can access the original image by analyzing the encrypted picture using the key, thus ensuring the secrecy and integrity of the image data during transmission and storage.

3.2.2 Columnar Cipher

The term "transposition cipher" originally referred to a type of encryption that rearranged plaintext letters. Ciphertext can be easily distinguished from plaintext by comparing their alphabetical frequencies, which are comparable. A considerable amount of research has been conducted on columnar transposition, which is thought to be the most widely studied transposition cipher.

The columnar cipher is a cryptographic technique that involves rearranging the order of letters present in the plaintext to generate the ciphertext. The columnar transposition cipher is one example of a cryptographic technique that involves rearranging plaintext into columns before the encryption process begins. In this cipher, the ciphertext is read by columns, while the plaintext is written in rows. The Columnar Cipher utilizes a method of encrypting communication by arranging plaintext in rows and then extracting the resulting ciphertext from the columns.

3.2.3 Complementation Process

The Binary Number System is a widely used method for expressing data in electronic formats. It comprises two distinct numeric values or representations. The first representation is 0, indicating the off state, while the second is 1, indicating the on state. This system is used to describe items that can exist only in two unique operating modes or events. The process of reversing or flipping binary digits is also known as bit inversion. During this process, the 0's and 1's undergo toggling.

3.3 Data Decryption

The process of decrypting encrypted material involves a series of sequential steps that are well-established. The first stage of the decoding process involves the transformation of the code into ASCII values and matrices. Subsequently, the Columnar Cipher is employed to reorder the ASCII equivalents. The Rubik's Cube algorithm is then used to reposition the elements to their original configurations. Finally, the message that has been encrypted is translated into decimal digits. The flow of data decryption has been shown in Figure 2 and complete data decryption process has been shown in Figure 3. Upon completion of the decoding process, the message is translated back to ASCII, resulting in the same information as the original message, as demonstrated in Figure 4. The complete steps for data encryption has been discussed in Algorithm 2.

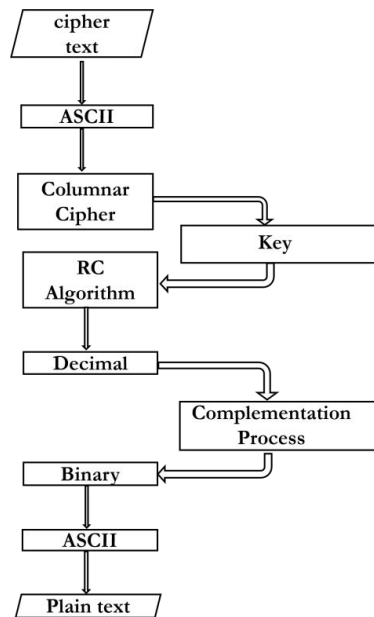


Figure 2. Flow of Data Decryption

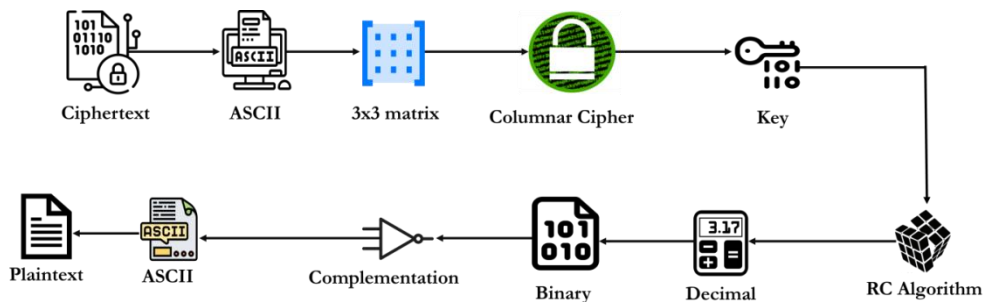


Figure 3. Data Decryption Mechanism

Algorithm 2: Decryption

Input: Cipher text

Output: Plain text

1. The encrypted text has been acquired.
 2. Subsequently, the text will be transformed into an order of ASCII characters.
 3. The ASCII characters are first subjected to a Columnar Transposition Cipher.
 4. Following that, the Rubik's Cube technique will be used to reorganize the transposed ASCII characters, using the same keys.
 5. Afterwards, the ASCII characters will be converted into decimal values.
 6. These decimal values will be further converted into binary digits.
 7. Next, the binary bits will be inverted using the 1's Complement technique.
 8. The inverted binary bits will be converted back into ASCII characters.
 9. Finally, the plaintext will be obtained by using the matching ASCII values.
-

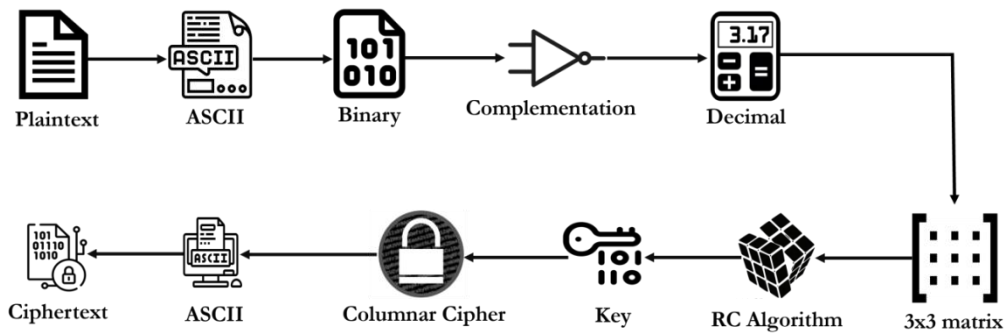


Figure 4. Encryption Mechanism

4. Testing

To assess the information, a composite cipher methodology is employed to encode the plain text, thus generating an indecipherable form of text known as ciphertext. Subsequently, a range of decryption procedures become necessary to restore the text to its original state of legibility.

4.1 Encryption Algorithm

Step 1: The original, unencrypted text is obtained as shown in Figure 5.

Data is BREACHED

Figure 5. Plaintext

Step 2: The plaintext will be encoded into ASCII characters as shown in Figure 6.

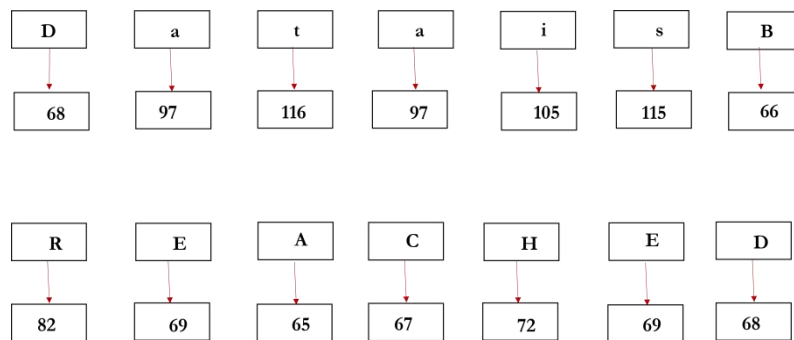


Figure 6. Converting text into ASCII equivalents

Step 3: The ASCII values will be transformed to 8-bit binary as shown in Figure 7.

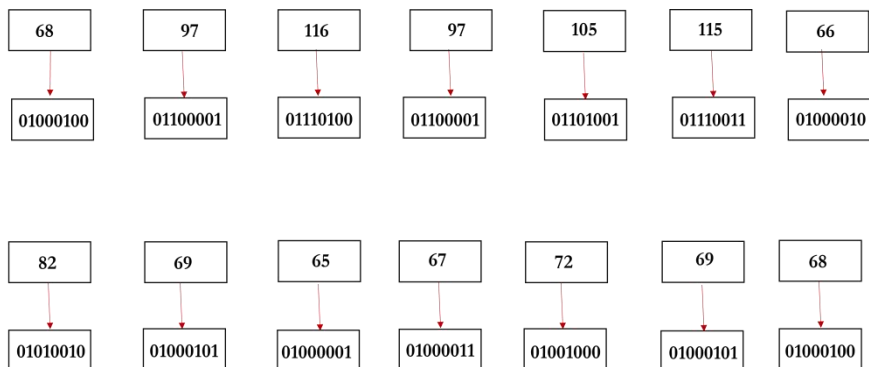


Figure 7. ASCII to Binary Conversion

Step 4: The 8-bit binary will undergo 1's Complement inversion as shown in Figure 8.

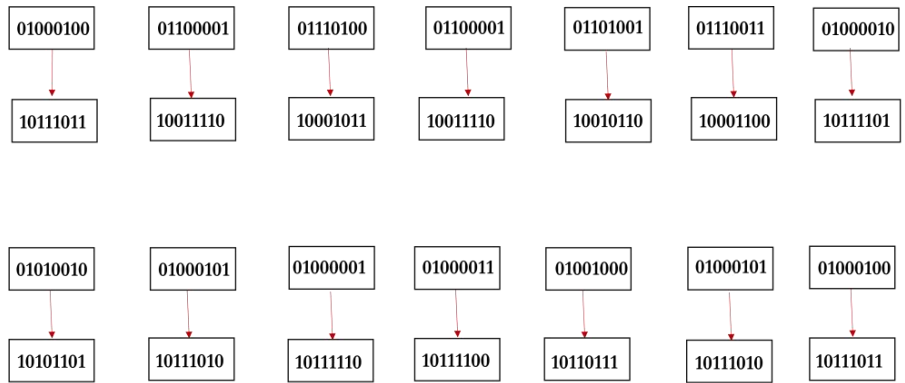


Figure 8. 1's Complement of 8-bit binary

Step 5: The inverted binary values will be transformed into decimal values as shown in Figure 9

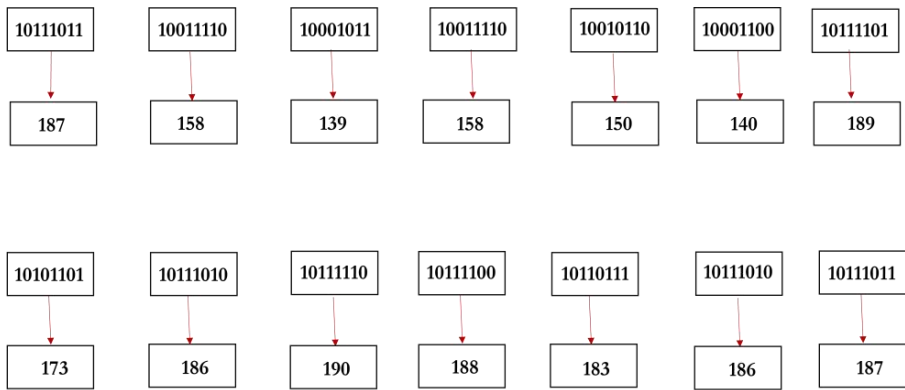


Figure 9. Converting Inverted Binaries into Decimal

Step 6: Afterwards, the decimals will be transformed into a matrix structure, and the Rubik's Cube algorithm will be executed on the decimals to rearrange them as in Figure 10.

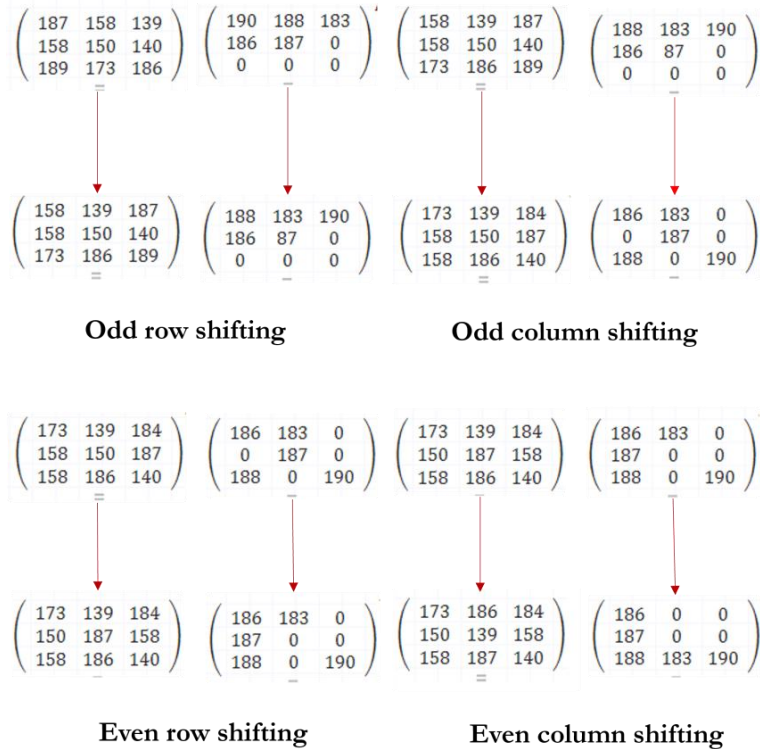


Figure 10. Results of the Rubik's Cube Algorithm

Step 7: The Columnar Cipher will be executed employing Rubik's Cube Algorithm and will rearrange the resulting matrices as shown in Figure 11.

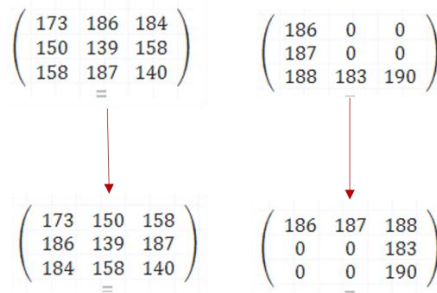


Figure 11. Results of the Columnar Cipher

Step 8: The transposed elements of the matrices will now be transformed back to their ASCII equals as shown in Figure 12.

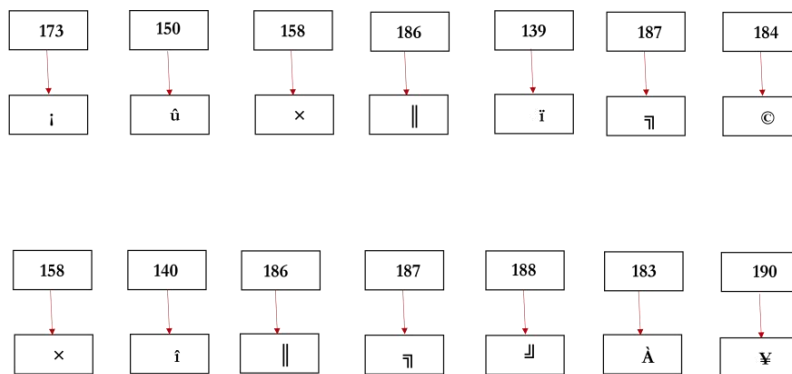


Figure 12. Again, converting the Decimals into ASCII equivalents

Step 9: The encrypted text has been obtained utilizing the conversion process as shown in Figure 13.

ï û × || ï ŕ © × î || ŕ Ɔ À ¥

Figure 13. Ciphertext

4.2 Decryption Algorithm

Step 1: The ciphertext is provided as shown in Figure 14.

ï û × || ï ŕ © × î || ŕ Ɔ À ¥

Figure 14. Ciphertext

Step 2: The ciphertext will be converted into ASCII equivalents as shown in Figure 15.

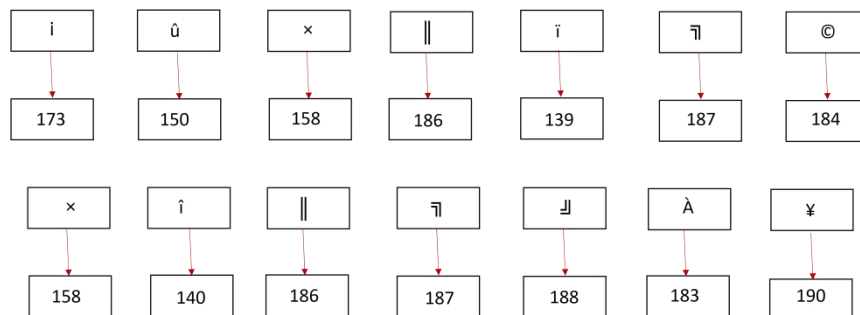


Figure 15. Converting Ciphertext into ASCII equivalents

Step 3: The ASCII values will be transformed into a matrix format and the Transposition Cipher will be applied as shown in Figure 16.

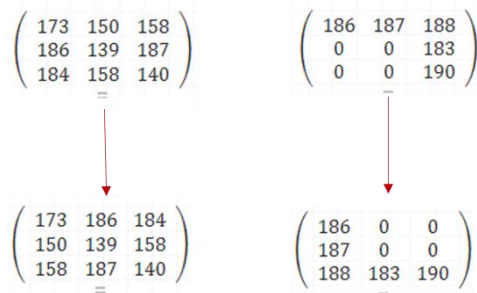


Figure 16. Result of the Columnar Cipher

Step 4: Next, the Rubik's Cube will be used on the transposed elements of the matrices as in Figure 17.

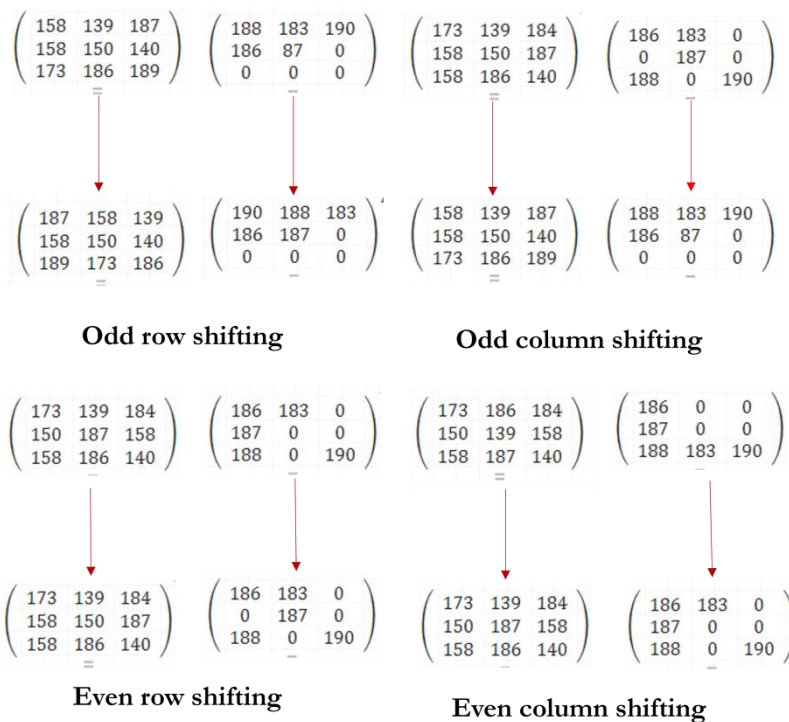


Figure 17. Result of the Rubik's Cube Algorithm

Step 5: The elements of the matrices will be transformed into binary form as shown in Figure 18.

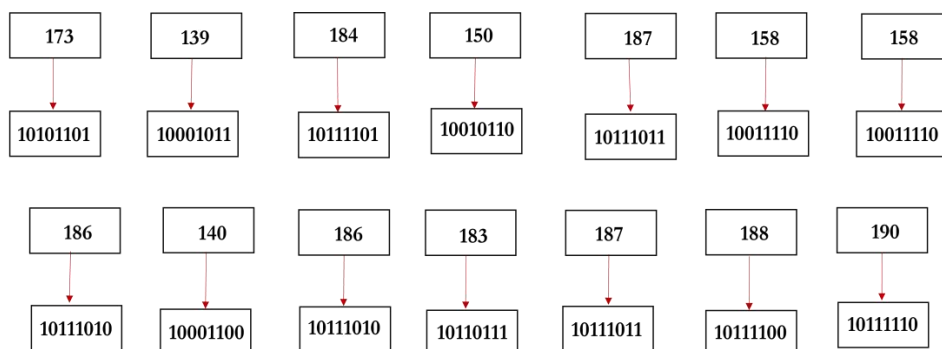


Figure 18. Converting the ASCII equivalents into Binary

Step 6: The binaries will be flipped using the 1's complement as shown in Figure 19.

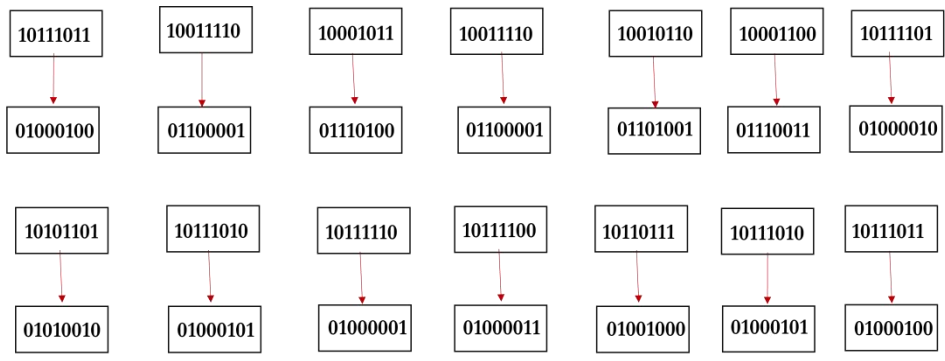


Figure 19. Binary Inversion

Step 7: The binary numbers will be transformed into decimal numbers as shown in Figure 20.

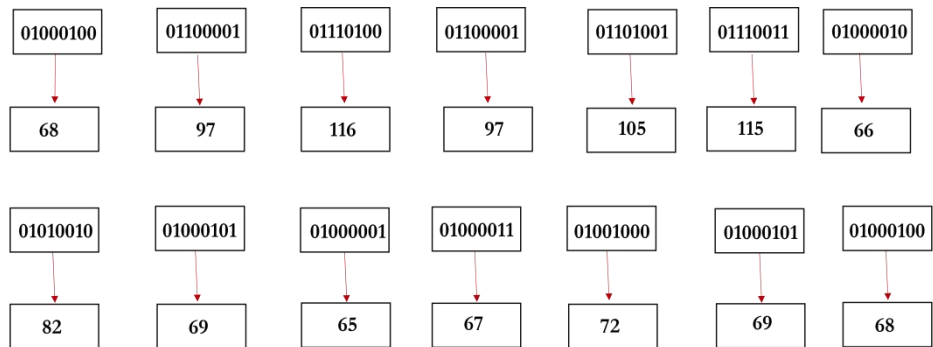


Figure 20. Converting Inverted Binary into Decimal

Step 8: The decimals will be then transformed into ASCII equals as shown in Figure 21.

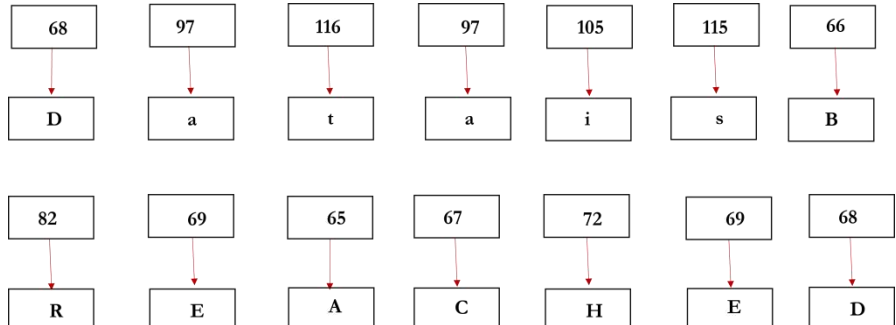


Figure 21. Again converting into ASCII

Step 9: The plaintext is acquired as shown in Figure 22.

Data is BREACHED

Figure 22. Plaintext

5. Results

In the beginning, we decided to go with a plaintext @dmin that was five characters long. An first step involves converting the plaintext into ASCII values. After that, these ASCII values are converted into binaries that are 8 bits in size. Utilising the Complementation process, the binaries are inverted before moving on to the decimal stage. This is done in order to prepare for the decimal stage. Afterwards, the binary digits that have been inverted are turned into decimal numerals. The decimal values are then converted into a three-by-three matrix once we have them in our possession. The matrix is subjected to the application of the Rubik's cube procedure, which includes first shifting the values upward and then moving the components to the right.

Following that, the components of the matrix are transposed by using the Columnar cypher, also known as the Transposition cypher. It is necessary to use a symmetric key in order to guarantee safety. Following the completion of all of these operations, the values that are produced are then transformed back into their counterparts in ASCII, which ultimately results in the ciphertext and the identical process will be carried out with each and every one of the other plaintexts that were discussed before. Different testing results of proposed algorithm has been shown in Table 2.

Table 2. Different results have been carried out

Testing	Plain Text	Plain Text Length	Key	Cipher Text	Cipher Text Length
1	@dmin	5	D@m!n	øæÆγú	5
2	C@ssPer	6	@\$_172	γ»ñ\î	6
3	Tr@cKer	7	cRA!k	îγ Üi½£	7
4	SP@m	4	Rx_8r8	»γ¼æ	4

The mixed approach is specifically intended to effectively process massive amounts of information by not experiencing major speed reductions. By incorporating distributed computing and improved data modeling, it is possible to split the mathematical effort across numerous processors or points, resulting in enhanced flexibility and performance. The integrated technique in cloud settings via significant traffic is capable of scaling to handle simultaneous encryption and decryption requests from different people or apps despite generating any delays or bottlenecks.

6. Conclusion

The following statement outlines the development of a hybrid encryption algorithm, which has been identified as an efficient and trustworthy method for systematically encrypting data. The approach incorporates a variety of designs and was determined to be the most reliable and effective after an exhaustive examination of numerous methodologies and strategies outlined in previous academic publications.

The methodology involves the utilization of different ways at varying time intervals to protect data against any unauthorized attempts to disable this mechanism. Each step of the procedure has been thoroughly planned to ensure varying degrees of safety. An attacker must have a detailed understanding of the specific decryption method and encryption key used to successfully breach each level.

This article introduces an innovative form of encryption known as a hybrid cipher approach. The method involves using both the Rubik's Cube algorithm and the Columnar Cipher (Transposition Cipher), along with additional phases. Both the encryption and decryption phases utilize the same key to ensure that the algorithm remains secure. Further, it is not possible for a particular key to function properly in a separate environment.

By utilizing this hybrid encryption technology, data stored on cloud servers can be guaranteed to be completely protected from potential hackers. If all of the approaches outlined in this strategy are carried out well, the original data will remain inaccessible to a potential intruder. As a result, the chance of a successful breach will be significantly reduced.

Moving forward, the Rubik's Cube algorithm will undergo revisions and various methods will be employed to ensure the safety of all types of data stored on cloud servers, regardless of data structure. The research will be extensively studied alongside other papers, and an analysis will be conducted to determine whether the present strategy is the most suitable of all proposed approaches. An algorithm will then be developed to measure the efficiency of this strategy. This method may encounter implementation challenges and inherent weaknesses. We are currently addressing these concerns and will shortly release a paper providing comprehensive information on using traditional ciphers to develop a hybrid model.

Conflict of Interest

There is no conflict of interest for this study.

References

- [1] Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics* **2021**, *11*, 16, <https://doi.org/10.3390/electronics11010016>.
- [2] Ustebay, S.; Turgut, Z.; Aydin, M.A. Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier. In Proceedings of 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT). Ankara, Turkey, 3–4 December 2018, pp. 71–76, <https://doi.org/10.1109/IBIGDELFT.2018.8625318>.
- [3] Verma, V.; Kumar, V. DoS/DDoS attack detection using machine learning: A review. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC), New Delhi, India, 20–21 February 2021, <http://dx.doi.org/10.2139/ssrn.3833289>.
- [4] Mohiyuddin, A.; Javed, A.R.; Chakraborty, C.; Rizwan, M.; Shabbir, M.; Nebhen, J. Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System. *Int. J. Fuzzy Syst.* **2022**, *24*, 1203–1215, <https://doi.org/10.1007/s40815-021-01104-y>.
- [5] Islam, M.M.; Hasan, M.Z.; Shaon, R.A. A novel approach for client side encryption in cloud computing. In Proceedings of 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 7–9 February 2019, pp. 1–6, <https://doi.org/10.1109/ECACE.2019.8679151>.
- [6] Zahra, S.W.; Nadeem, M.; Arshad, A.; Riaz, S.; Ahmed, W.; Abu Bakr, M.; Alabrah, A. Emergence of Novel WEDEX-Kerberotic Cryptographic Framework to Strengthen the Cloud Data Security against Malicious Attacks. *Symmetry* **2024**, *16*, 605, <https://doi.org/10.3390/sym16050605>.
- [7] Mushtaq, M.F.; Jamel, S.; Disina, A.H.; Pindar, Z.A.; Shakir, N.S.A.; Deris, M.M. A Survey on the Cryptographic Encryption Algorithms. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, <https://doi.org/10.14569/ijacsa.2017.081141>.
- [8] Abed, S.; Waleed, L.; Aldamkhi, G.; Hadi, K. Enhancement in data security and integrity using minhash technique. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *21*, 1739–1750, <https://doi.org/10.1591/ijeecs.v21.i3.pp1739-1750>.
- [9] Pise, A.A.; Singh, S.; Gadilkar, S.; Esther, Z.B.; Pise, G.S.; Imuede, J. Utilizing Asymmetric Cryptography and Advanced Hashing Algorithms for Securing Communication Channels in IoT Networks Against Cyber Espionage. *J. Cybersecur. Inf. Manag.* **2024**, *13*, 46–59, <https://doi.org/10.54216/jcim.130105>.
- [10] Ahmad, S.A.; Garko, A.B. Hybrid Cryptography Algorithms in Cloud Computing: A Review. In Proceedings of 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 10–12 December 2019, pp. 1–6, <https://doi.org/10.1109/ICECCO48375.2019.9043254>.
- [11] Jangjou, M.; Sohrabi, M.K. A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. *Arch. Comput. Methods Eng.* **2022**, *29*, 3587–3608, <https://doi.org/10.1007/s11831-022-09708-9>.
- [12] Lee, B.-H.; Dewi, E.K.; Wajdi, M.F. Data security in cloud computing using AES under HEROKU cloud. In Proceedings of 2018 27th wireless and optical communication conference (WOCC), Hualien, Taiwan, 30 April–1 May 2018, pp. 1–5, <https://doi.org/10.1109/WOCC.2018.8372705>.
- [13] Biswas, C.; Gupta, U.D.; Haque, M.M. An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. In Proceedings of 2019 international conference on electrical, computer and communication engineering (ECCE), Cox'sBazar, Bangladesh, 7–9 February 2019, pp. 1–5, <https://doi.org/10.1109/ECACE.2019.8679136>.
- [14] Sharma, Y.; Gupta, H.; Khatri, S.K. A Security Model for the Enhancement of Data Privacy in Cloud Computing. In Proceedings of 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019, pp. 898–902, <https://doi.org/10.1109/AICAI.2019.8701398>.
- [15] Abdullah, M.Z.; Khaleefah, Z.J. Design and implement of a hybrid cryptography textual system. In Proceedings of 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 21–23 August 2017, pp. 1–6, <https://doi.org/10.1109/ICEngTechnol.2017.8308141>.
- [16] Harini, M.; Gowri, K.P.; Pavithra, C.; Selvarani, M.P. A novel security mechanism using hybrid cryptography algorithms. In Proceedings of 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), Karur, India, 27–28 April 2017, pp. 1–4, <https://doi.org/10.1109/ICEICE.2017.8191910>.

- [17] Chinnasamy, P.; Deepalakshmi, P. Design of Secure Storage for Health-care Cloud using Hybrid Cryptography. In Proceedings of 2018 second international conference on inventive communication and computational technologies (ICICCT), Coimbatore, India, 20–21 April 2018, pp. 1717–1720, <https://doi.org/10.1109/ICICCT.2018.8473107>.
- [18] Soman, V.K.; Natarajan, V. An enhanced hybrid data security algorithm for cloud. In Proceedings of 2017 International conference on networks & advances in computational technologies (NetACT), Thiruvananthapuram, India, 20–22 July 2017, pp. 416–419, <https://doi.org/10.1109/NETACT.2017.8076807>.
- [19] Maitri, P.V.; Verma, A. Secure file storage in cloud computing using hybrid cryptography algorithm. In Proceedings of 2016 international conference on wireless communications, signal processing and networking (WiSPNET), Chennai, India, 23–25 March 2016, pp. 1635–1638, <https://doi.org/10.1109/WiSPNET.2016.7566416>.
- [20] Arunkumar, M.; Ashokkumar, K. A review on cloud computing security challenges, attacks and its countermeasures. *AIP Conf. Proc.* **2024**, *3037*, 020047, <https://doi.org/10.1063/5.0196063>.
- [21] Jimmy, F.N.U. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *J. Artif. Intell. Gen. Sci.* **2024**, *2*, 129–171, <https://doi.org/10.60087/jaigs.v2i1.102>.
- [22] Gu, Y.; Li, K.; Guo, Z.; Wang, Y. Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm. *IEEE Access* **2019**, *7*, 64351–64365, <https://doi.org/10.1109/access.2019.2917532>.
- [23] AlRoubiei, M.; AlYarubi, T.; Kumar, B. Critical Analysis of Cryptographic Algorithms. In Proceedings of 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 1–2 June 2020, pp. 1–7, <https://doi.org/10.1109/ISDFS49300.2020.9116213>.
- [24] Mandowen, S.A. Advanced hill cipher algorithm for security image data with the involutory key matrix. *J. Physics: Conf. Ser.* **2021**, *1899*, 012116, <https://doi.org/10.1088/1742-6596/1899/1/012116>.
- [25] Meraouche, I.; Dutta, S.; Tan, H.; Sakurai, K. Neural Networks-Based Cryptography: A Survey. *IEEE Access* **2021**, *9*, 124727–124740, <https://doi.org/10.1109/ACCESS.2021.3109635>.
- [26] Tan, C.M.S.; Arada, G.P.; Abad, A.C.; Magsino, E.R. A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *J. Physics: Conf. Ser.* **2021**, *1997*, 012021, <https://doi.org/10.1088/1742-6596/1997/1/012021>.
- [27] Qowi, Z.; Hudallah, N. Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *J. Physics: Conf. Ser.* **2021**, *1918*, 042009, <https://doi.org/10.1088/1742-6596/1918/4/042009>.
- [28] Vatshayan, S.; Haidri, R.A.; Verma, J.K. Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher. In Proceedings of 2020 international conference on computational performance evaluation (ComPE), Shillong, India, 2–4 July 2020, pp. 848–852, <https://doi.org/10.1109/ComPE49325.2020.9199997>.
- [29] Arroyo, J.C.T.; Delima, A.J.P. Caesar Cipher with Goldbach Code Compression for Efficient Cryptography. *Int. J. Emerg. Trends Eng. Res.* **2020**, *8*, 2999–3002, <https://doi.org/10.30534/ijeter/2020/19872020>.
- [30] Serdano, A.; Zarlis, M.; Nababan, E.B. Performance of Combining Hill Cipher Algorithm and Caesar Cipher Algorithm in Text Security. In Proceedings of 2021 International conference on artificial intelligence and mechatronics systems (AIMS), Bandung, Indonesia, 28–30 April 2021, pp. 1–5, <https://doi.org/10.1109/AIMS52415.2021.9466039>.
- [31] Chen, W.H.; Zhou, X.F.; Zheng, N.; Li, M.J.; Hu, M. Image encryption scheme based on optical chaos and DNA Rubik's Cube algorithm. *Phys. Ser.* **2023**, *98*, 115507, <https://doi.org/10.1088/1402-4896/acfe48>.
- [32] Gao, X.; Mou, J.; Banerjee, S.; Cao, Y.; Xiong, L.; Chen, X. An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *J. King Saud Univ. - Comput. Inf. Sci.* **2022**, *34*, 1535–1551, <https://doi.org/10.1016/j.jksuci.2022.01.017>.
- [33] Zhao, Y.; Meng, R.; Zhang, Y.; Yang, Q. Image encryption algorithm based on a new chaotic system with Rubik's cube transform and Brownian motion model. *Optik* **2023**, *273*, 170342, <https://doi.org/10.1016/j.jleo.2022.170342>.
- [34] Upadhyay, D.; Zaman, M.; Joshi, R.; Sampalli, S. An Efficient Key Management and Multi-Layered Security Framework for SCADA Systems. *IEEE Trans. Netw. Serv. Manag.* **2021**, *19*, 642–660, <https://doi.org/10.1109/tnsn.2021.3104531>.

- [35] Arshad, A.; Nadeem, M.; Riaz, S.; Zahra, S.W.; Dutta, A.K.; Alzaid, Z.; Alabdan, R.; Almutairi, B.; Almotairi, S. Hill Matrix and Radix-64 Bit Algorithm to Preserve Data Confidentiality. *Comput. Mater. Contin.* **2023**, *75*, 3065–3089, <https://doi.org/10.32604/cmc.2023.035695>.