The Art of Secrecy: Hybridizing Caesar and Columnar Ciphers for Enhanced Data Security

Syeda Wajiha Zahra[*], Mudassar Ali Zaman[†], Waqas Ahmed[‡], Muhammad Nadeem[§], Ali Arshad[**], Saman Riaz[††]

Abstract

Cryptography is currently the most secure way for transmitting data on the Cloud. It employs one or algorithms to securely transport data, preventing any unauthorized access or loss. An assortment of researchers has devised numerous protocols related to secure data transmission. Each method entails transforming data from an accessible format to an inaccessible one. However, more than these approaches are needed to ensure absolute information security. In the context of data security, each algorithm is susceptible to vulnerabilities. Ensuring the implementation of adequate data security protocols will effectively protect the encrypted data against any decryption attempts by malicious actors. An attempt to modify the data will render the assailant incapable of recovering the original and causing damage. This article introduces an innovative method that integrates the substitution cipher and transposition ciphers to guarantee data confidentiality and integrity during transmission and communication. By contrasting our work with prior research, we have demonstrated that the proposed algorithm outperforms the existing cypher schemes. At the end, a conclusion is subsequently attained through a comparative analysis.

Keywords: Cryptography; Vigenère Hybridizing Algorithms; Data Security; Caesar Cipher; Columnar Matrix; Hill Cipher.

Introduction

When private data is stored and delivered over the internet, physical barriers become ineffective in protecting it, stressing the need of security (Lokesh & BoreGowda, 2021). Cloud computing allows people and companies to access a variety of services via the Internet, reducing the need to directly maintain physical equipment (Saxena et al., 2019). Amazon Web Services (AWS), Microsoft Azure, and Google Cloud are some of the most widely utilized cloud computing systems (Chaabouni et

[*]Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan, syeda.wajia786@gmail.com

[†]Department of Computer Science, Alhamd Islamic University, Islamabad 44000, Pakistan, casspersquare97@yahoo.co.uk

[‡]Corresponding Author: Department of Computer Science, Alhamd Islamic University, Islamabad 44000, Pakistan, waqasahmad9107@gmail.com

[§]Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing 100083, China, nadeem72g@gmail.com

[**]Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan, alli.arshad@gmail.com

[††]Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan, samanriaz@hotmail.com

al., 2019). Data may be accessible with a single touch from any point in the globe. Cloud computing provides a variety of services that cater to the different needs of clients (Jangjou & Sohrabi, 2022) such as public, private, and hybrid clouds.

Widespread use of cryptography to ensure the privacy and integrity of user information. The procedure entails the encryption and cloud storage of user-associated data (Dubey et al., 2015). Cryptography is frequently employed to generate one-of-a-kind encryption methods that are utilized to safeguard data. The aforementioned measures consist of the utilization of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption with keys of either 128 bits or 256 bits (Upadhyay et al., 2021). The aforementioned encryption methods safeguard a variety of mathematical data and information, including emails, passwords, e-commerce, and banking transactions (Chaudhary et al., 2020). The utilization of cryptography techniques is critical in safeguarding network communications (Schlatt et al., 2023). The field of cryptography is dedicated to the protection of data through the implementation of encryption and decryption techniques. Involved are security mechanisms including authentication, confidentiality, and integrity (Murad & Rahouma, 2022). Cryptography and cryptanalysis are both intricately intertwined. The procedure encompasses various methodologies, including the utilization of images and microdots to obfuscate data during transmission or storage (Md, 2021). Historiographically associated with these techniques, cryptography has become increasingly significant in the realm of cloud computing (Akanksha et al., 2022). However, the migration of data to the cloud necessitates significant adjustments and poses concrete risks, potentially deterring clients from enrolling in cloud services. Unauthorized access to sensitive information and the potential for data loss may cause concern among users (Sun & Grishman, 2022).

Cipher text is the result of the transformation of plaintext during encryption. The term "plain text" denotes the unaltered message or data transmitted by the sender over a network. In contrast, "cipher text" is the encrypted iteration of the data that is deliberately disguised to impede human comprehension (Murad & Rahouma, 2021). Decryption, through the use of a variety of instruments or processes, is the process of converting encrypted text to ordinary text (Ahmad et al., 2022). An encrypted message may be decoded utilizing a secret key or a private key (Li et al., 2021). Encryption can be achieved with the aid of either a public or secret key. Digital encryption methods operate through the manipulation of the mathematical structure of a plaintext message. This is achieved by employing an encryption algorithm and a digital key to

produce a ciphertext rendition of the message (Hidayat et al., 2020). Maintaining a unique key between the sender and recipient enables the establishment of secure communication (Gao et al., 2023).

This paper presents a very effective cryptographic technique designed for protecting data, defending cloud data from attacks, and securely transporting data inside a reliable environment. Initially, a plain text is obtained and then encrypted using a fixed key. A data encryption process involves the use of an ASCII table. In the event that someone else tries to intercept the data, it will be quite easy for them to break the encryption that is generated by a single cipher by using the standard techniques. It is possible that we will be able to considerably increase the degree of data security by using a mix of numerous different ciphers and procedures. This will make it very difficult for any possible attacker to compromise the data. Initially, the plaintext will be turned into ASCII values, which will subsequently be converted into binary bits by a further transformation. Before these binary bits are turned into decimals, a key will be used to invert them. This will take place after the conversion. This study is distinguished by the fact that the inverted binary bits will be arranged in a matrix and managed by several matrix operations. This is the distinctive feature of the article. Following that, when these matrix operations have been completed, the elements of the matrix will be converted into ASCII values once again. If we stick to these procedures, we will be able to get the ciphertext.

Literature Review

In order to bolster data security, Suhael et al. (2024) implemented two hybrid cryptosystems. Hybrid cryptosystems employ a dual encryption and decryption layer. The plaintext is encrypted with the modified Playfair cipher at the initial layer, yielding the ciphertext. The ultimate ciphertext is produced by re-encrypting the initial ciphertext with RSA squared. While implementing this methodology ensures the strength of security protocols, the computations take an inordinate amount of time. The second hybrid cryptosystem decisively resolves this issue by employing the Chinese remainder theorem to expedite the encryption and decryption procedures.

Tan et al. (2021) describes a unique hybrid encryption and decryption approach. The ideas and operations of the Caesar Cipher and Vigenere Cipher algorithms are used in this approach. The efficiency of the suggested design is evaluated using MATLAB simulations and compared to existing ciphers such as Hill Cipher, Caesar Cipher, and

Vigenere Cipher. The examination included a review of a variety of variables, such as character frequency and graph behavior.

Pöpper (2024) presented a novel cipher that combines the Caesar Cipher and Vigenere Cipher in an improved manner, resulting in greater levels of perplexity and diffusion. The novel architecture of this cipher surpasses that of classical ciphers through the incorporation of alphabets, numerals, and symbols, resulting in an entirely bewildering state. By integrating contemporary cryptographic components, classical ciphers can be fortified to offer optimal levels of security protection.

The methodology employed in a study (Nadeem et al., 2023) protects data from unauthorized access and misuse. This approach is highly compatible with cloud networks. A key is generated by a Non-Deterministic Bit Generator (NRBG) and combines with the ordinary text bits via the XNOR operation; bit toggling is then implemented. Furthermore, I developed a matrix cipher encryption technique that generates a key from the raw text. This key is exclusively employed for data decoding in the initial phases. Both encryption stages employ unique methodologies to safeguard the data, culminating in the ciphertext generation. The plain text key must never be applied to any additional plain text.

Garg et al. (2019) presents the hybrid Cipher, a novel framework that is specifically engineered to ensure the security of data in transit throughout different tiers of software-defined networks. By utilizing encryption, the model that is incorporated into the software-defined controller ensures the security of open-flow requests and responses. Because of their capacity to function as autonomous security controllers and their capacity for customization, software-defined networks provide an ideal framework for the implementation of this concept. Through the utilization of the Hybrid Diagonal Transposition technique, software-defined wireless sensor nodes are able to enhance their situational awareness, protect user data, and aid in the detection and encryption of malevolent traffic flows. Hybrid Diagonal Transposition ultimately provides data intrusion protection for software-defined networks.

Priya (2022) introduces a hybrid cryptographic approach that is put into practice for the purpose of data encryption. Symmetric algorithms are utilized in the domain of data encryption, while asymmetric approaches are employed for the encryption of credentials. The proposal is based on the prevailing global condition, in which electronic storage and regulation are the sole means of managing medical data. Medical professionals, patients, government agencies, insurance providers, and other entities have access to this information.

Proposed Methodology

The present article posits the notion of constructing a hybrid cipher by integrating substitution and transposition ciphers. The fundamental principle that guides this methodology is to enhance the security of data transmission. In the event that an unauthorized individual or assailant endeavors to gain access to the data through a variety of means, their achievement will be exceedingly difficult to achieve.

Work Overflow

During data transmission, the attacker uses a variety of tactics and makes repeated attempts to obtain unauthorized access to the data. This hybrid cipher is designed to handle the problem of safeguarding data from attackers using many ways. The purpose of developing a model cipher algorithm is to prevent unauthorized access or abuse of data by potential attackers, due to the implementation of a strong hybrid cipher encryption method. Access to the data will be limited to authorized individuals only. Initially, the unformatted text will be used for encryption and then transformed into its corresponding ASCII format. Next, we will transform the ASCII representation into an 8-bit binary format, and then convert it into decimal digits. Prior to decimal transformation the binary numbers will be inverted using a key. They will first be translated into ASCII substitutes, then into binary form, and then inverted and XORed based on the binary values. Then, the decimals will be organized into a matrix and then applied to the Caesar Cipher, a kind of Substitution Cipher, using the 3-SHIFT algorithm to shift the decimals according to the method. Following this, an unauthorized individual attempting to decipher the message will encounter a challenge due to the reorganization of the shifted matrices by the Columnar Cipher, a type of Transposition Cipher. Subsequently, it will once again be transformed into ASCII substitutes, resulting in the Cipher text.

Data Encryption Process

In order to encrypt plain text, we first transform it into its ASCII representation and then into 8-bit Binary format. The binaries are then reversed using a key that is produced using the same procedure. The key is first translated into ASCII equivalents, then transformed into Binary format, and then inverted. Finally, it is XORed with the binary values. The decimals are organized into a matrix and then subjected to the Caesar Cipher, which is a kind of Substitution Cipher. The 3-SHIFT method is used to shift the decimals appropriately. The Columnar Cipher, which is a kind of Transposition Cipher, rearranges the shifted matrices in order to

increase the level of complexity for attackers. Ultimately, the Cipher text is acquired by translating the decimal values back into its corresponding ASCII characters as shown in Figure 1.

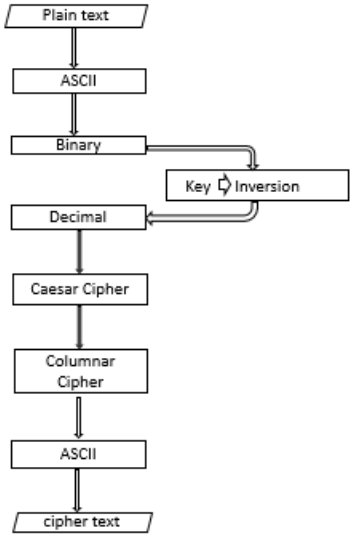

Figure 1: Data Encryption.

Algorithm 1: Encryption

Input: Plain text
Output: Cipher text

- Any plain text.
- Convert each text letter into ASCII symbols.
- Transform the ASCII equivalents into Binary Bits.
- Following the conversion to Binary, the Binary bits will be reversed using a key.
- Following the inversion, a key will undergo the identical process of inversion and XOR operation, resulting in binary bits that will then be transformed into decimal form.
- Next, the decimals will be expressed in matrix format and processed to the Caesar Cipher using a Shift of 3.
- Following the shifting process, the matrices will undergo a Columnar Cipher using the Transposition Algorithm.
- Subsequently, the resulting text will once again be transformed into ASCII equals.
- The ciphertext will be obtained.

Caesar Cipher

A technique that involves shifting a piece of text by a certain number of places or replacing certain numeric values with other numeric ones. The shifting process works like if you want to shift alphabet A and make it a ciphertext then the result will alphabet C as a ciphertext. Same process will take place if you apply this technique on numeric values. This technique is crucial in order to swap multiple letters or numbers. All the numerical values are swapped after transforming them into matrix form. Another significant flaw of the Caesar cipher is that it is liable to being quickly decoded, even when just the encrypted text is known. As a result of the restricted number of shifts that are able to occur. This article employs the Caesar Cipher with a Shift of 3, whereby numeric values in the matrices are shifted subsequent to conversion.

After converting the numeric values into matrix form the Caesar cipher is being used with a Shift of 3 to swap all the elements of the matrices. For example, a 2x2 matrix contains 170, 145, 150 and 118 after applying this technique with a shift of 3 the resultant matrix elements will be 173, 148, 153 and 121. With this same technique all the matrices will be swapped, and we will have new transformed matrices.

Columnar Cipher

The technique entails arranging the plaintext in rows and then reading the resulting ciphertext in columns. For the purpose of operation, the cipher first arranges the letters of the plaintext in rows and then obtains the ciphertext by rewriting the letters in columns. To make this encryption technique more complex, secure and to keep safe from data breach we will use this cipher after transforming the numeric values into matrix form and execution of Caesar cipher. This cipher will transpose all the matrix elements which will enhance the security and the complexity for any kind of data intrusion. Furthermore all the matrices will be transpose and the resultant matrices will undergo the next processes to get the ciphertext. The purpose of using this cipher is to make the encryption stronger than the encryption techniques that have been proposed by different researchers and proposed in different articles. Many researchers have proposed multiple encryption methods, but the flaw is they used a single cipher for encryption and decryption which is easy to break in.

After the Caesar cipher takes place on the elements of the matrices, the Columnar Cipher which is a transposition cipher will transpose the whole matrices to change the location of the elements. For example, the elements of a matrix that we get after applying Caesar cipher are 173, 148, 153 and 121 and after applying Columnar Cipher the position

of the elements will be transposed 173, 153, 148 and 121. The same technique will be applied on the rest of the matrices will transpose and the position of all elements will be changed.

Data Decryption Process

The transformation of ciphertext into plaintext will be accomplished through the use of a series of phases. Converting the cipher into ASCII equivalents and matrices is the first step in the process since it is the initial stage. Rearranging the ASCII equals is the next step that the Columnar Cipher will take. Following that, the Caesar Cipher method will be applied, and a 3-SHIFT will be used in order to displace the components that correspond to it for displacement. In the next step, the ciphertext will be recalculated into decimal form, and the encryption key will be renewed. At the end of the process, the ciphertext will be converted into ASCII replacements, which will result in the plaintext being returned as shown in Figure 2.

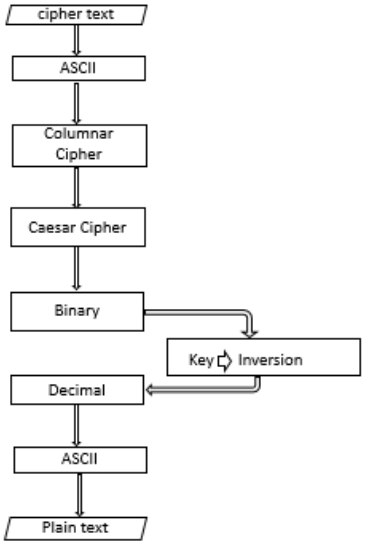

Figure 2: Data Decryption.

Algorithm 2: Decryption

Input: Cipher text
Output: Plain text

- The ciphertext is now obtained.
- The ciphertext will be transformed into ASCII characters.
- Following that, the ASCII equals will be subjected to a Columnar Transposition Cipher.

- Next, the transposed ASCII counterparts will undergo implementation of the Caesar Cipher with a Shift of 3.
- Next, the ASCII equals will be transformed into decimal values.
- A key that has been XORed will be used subsequent to the conversion.
- Next, the Decimals will be transformed into Binary bits.
- Following the process of Binary interchange the binary bits will be subsequently transformed into their corresponding ASCII equals.
- The Plaintext will now be derived using ASCII comparable values.

Testing of the Proposed Schemes

First, a plain text is taken to test the data, and then this plain text is encrypted with the help of a matrix cipher algorithm and an unreadable text is obtained, called ciphertext. After receiving the ciphertext, various decryption steps have been followed to convert the text from a nonreadable format to readable. In order to evaluate the data, the first step involves taking plain text and then encrypting it using a matrix cipher technique. The outcome is an unclear text referred to as ciphertext. After getting the ciphertext, a series of decryption processes are performed to restore the readability of the text.

Various methods have been used to transform the original text into encrypted code. Initially a plaintext is shown in Figure 3. After getting the plaintext each character is translated into its corresponding ASCII value as shown in Figure 4. Following the conversion, the ASCII equals undergo further conversion into binary bits as shown in Figure 5. The binary bits are then reversed using a key as shown in Figure 6. Next, the inverted binary are transformed into decimal as shown in Figure 7. The decimals are represented in matrix form shown in Figure 8. The matrices undergo a Caesar Cipher with a shift of 3, as seen in Figure 9. Each element in the matrix are moved by a value of n+3, where n is the position of the element. Then columnar transposition is performed. The cipher operates via matrices as shown in Figure 10. The elements of these matrices are once again transformed into ASCII equals as shown in Figure 11. Finally, the ciphertext has been acquired, as shown in Figure 12.

University

Figure 3: Plaintext.

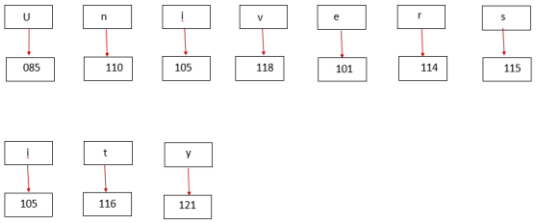

Figure 4: Converting the plaintext into ASCII values.

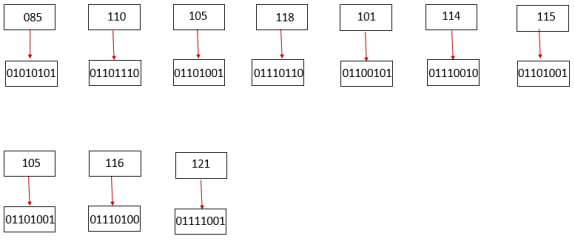

Figure 5: Converting ASCII values to Binary Bits.

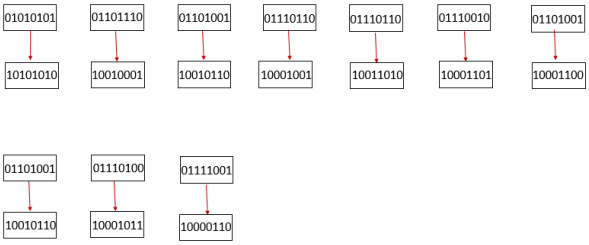

Figure 6: Binary Inversion.

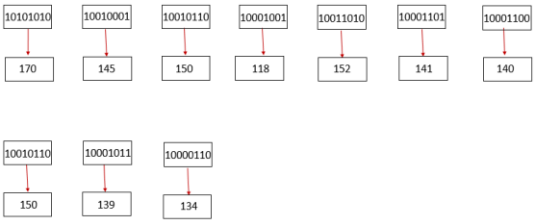

Figure 7: Converting inverted Binary bits into Decimal values.

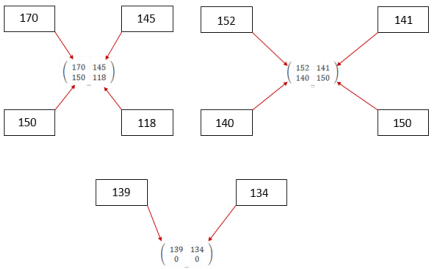

Figure 8: Conversion of decimal to 2x2 matrix.

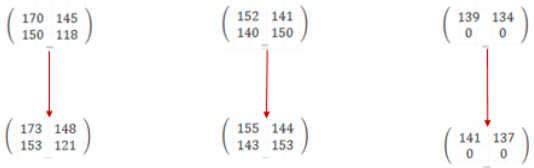

Figure 9: Results of Caesar Cipher.

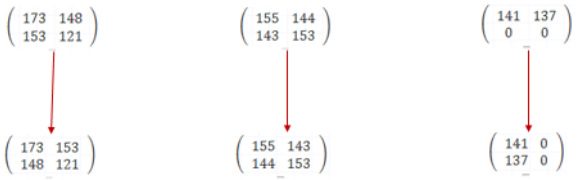

Figure 10: Results of Columnar Cipher.

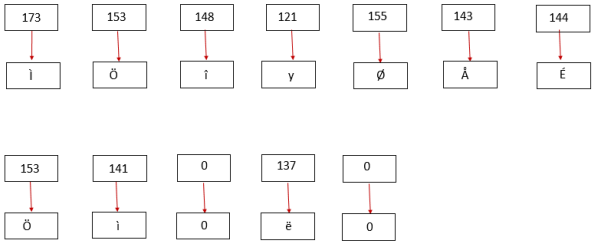

Figure 11: Converting each decimal value into ASCII values.

ìÖÎyØÅÉöÌ0ë0

Figure 12: Cipher Text.

During the decryption process, let's first consider a ciphertext as shown in Figure 13. The Ciphertext is translated into ASCII equals as shown in Figure 14. Subsequently, the ASCII equals are transcribed in a matrix format as shown in Figure 15. The Columnar Transposition Cipher is now applied to the matrices as shown in Figure 16. Next, the matrices

undergo the Caesar Cipher with a shift of 3, as seen in Figure 15. Each element are displaced by a distance of n-3 as shown in Figure 17. The ASCII equals are transformed into binary digits as shown in Figure 18. Following that, the binary bits undergo further inversion as shown in Figure 19. The next step involves converting these binary bits, which are inverted, back into decimal numbers as shown in Figure 20. In this procedure, we get the text as shown in Figure 21. Finally, the decrypted text is acquired as shown in Figure 22.

ÌÖÎyØÅÉöÌ0ë0

Figure 13: Cipher Text.

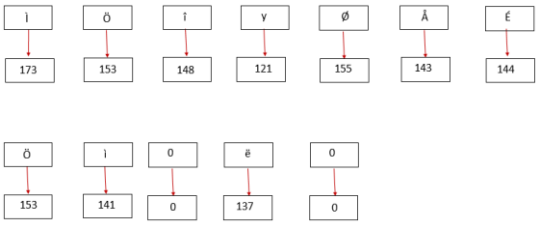

Figure 14: Converting the ciphertext into ASCII values.

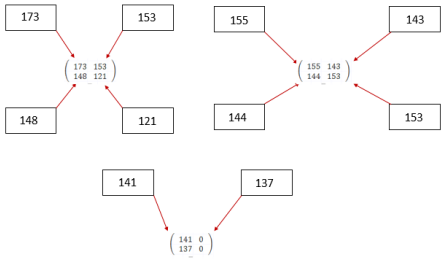

Figure 15: Converting the ASCII values into 2x2 Matrix Form.

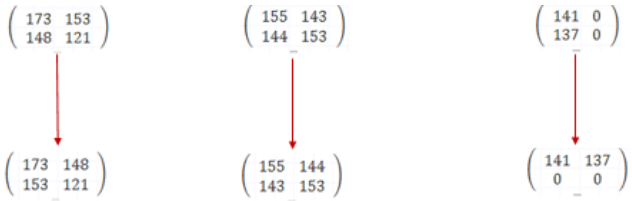

Figure 16: Results of Columnar Transposition.

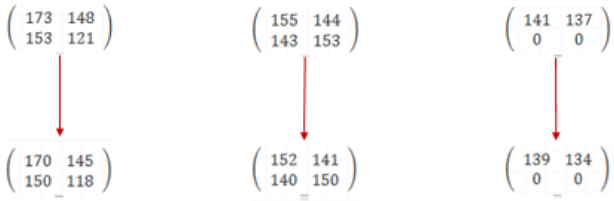

Figure 17: Results of Caesar Cipher.

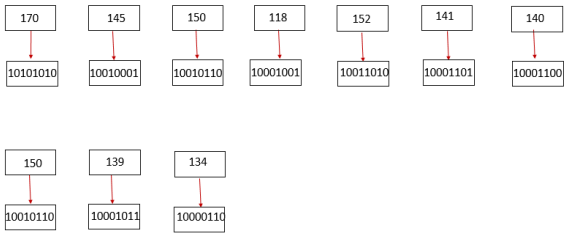

Figure 18: Converting ASCII values into Binary Bits.

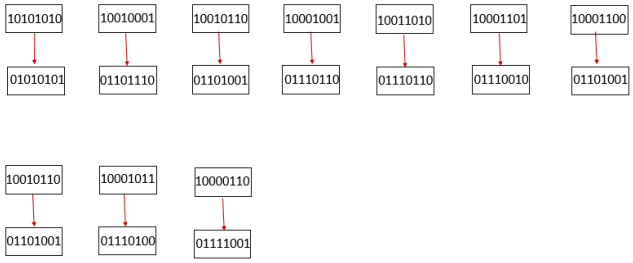

Figure 19: Inversion of Binary Bits.

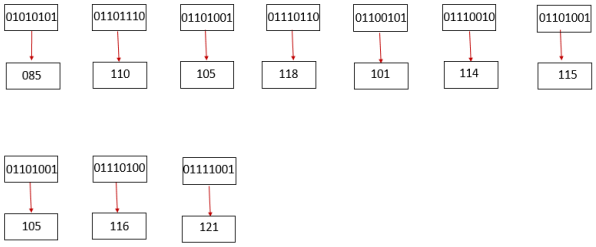

Figure 20: conversion of each binary into ASCII form.

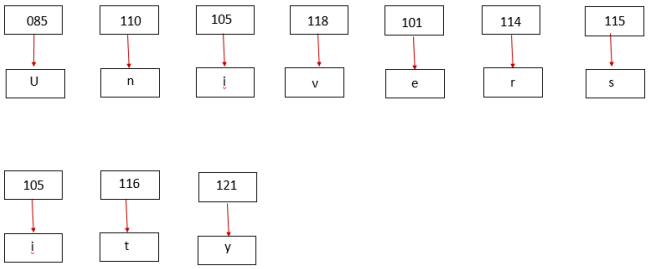

Figure 21: Conversion of ASCII values into Text form.

University

Figure 22: Plaintext

Discussion

Researchers have produced unique procedures by performing surveys on numerous cryptography processes and using existing ones. Researchers have successfully implemented many methods of encryption and decoding. Upon analysis, it is discovered that the majority of individuals utilized traditional methods for data encryption and decryption. These methods involved employing various techniques and ciphers, but still relied on the outdated approach of directly converting plaintext characters into ciphertext.

In this study, a novel technique is adopted from a recently published paper. This technique involves transforming the plaintext into an unintelligible form ahead of converting it into ciphertext. Implementing efficient encryption mechanisms is crucial for ensuring the security of data in cloud computing. Utilizing a singular approach renders it vulnerable to exploitation by attackers. Nevertheless, using distinct methodologies at each stage renders data leakage or disruption unachievable for intruders. A complete comparative analysis is shown in Table 1.

Table 1. Comparative analysis.

	Tan et al. (2021)	Pöpper (2024)	Nadeem et al. (2023)	Garg et al. (2019)	Priya (2022)	Chinnasamy & Deepalakshmi (2018)
Algorithm	Hybrid Caesar Cipher, Vigenere Cipher	Improved the performance of Caesar Cipher and Vigenere Cipher	Hill Cipher algorithm	Hill Cipher algorithm	Hill Cipher Chain algorithm	Hybridizing Caesar and Columnar cipher
Novelty	MATLAB simulations and compared with different algorithms	Classical ciphers improved the optimal security	Implemented a comprehensive array of data protection measures	Client communication by the use of a cryptographic key	Primary Key Encryption	Text and Key inversion
ASCII	Not Used	Not Used	Standard	Standard	Standard	Standard
Gaps	Transformation of text into ASCII values for encryption and decryption is not enough	classical cipher algorithm may be readily deciphered	No recent advancement has been made in this algorithm	Generating a distinct key from every line might provide superior precision compared to using a single key	Suitable for primary key encryption	Identified all gaps
Solutions	Combining the Caesar Cipher and Vigenere cipher algorithm via hybridization	Classical ciphers achieve a condition of complete disorientation	The use of 64-bit radix encryption resulted in a cipher text exceeded the size of plain text	Derive a distinct key using the Hill matrix technique	Suitable for every text	All gaps are resolved

Conclusion

When an attacker attempts to compromise this approach, the data remains secure since it employs many techniques at different stages. The safety of each step in this document varies significantly from all other points included. In order to decrypt the data, it is crucial to use the same key that was used during the encryption process, and the same procedure that was employed must also be employed. This study presents a Hybrid Cipher Encryption method for encoding data. This algorithm employs a mixture of the Caesar Cipher (Substitute Cipher) and Columnar Cipher (Transposition Cipher) with novel stages. In each stage, the same key is utilized to ensure the security of the algorithm during both encryption and decryption processes. By using the Hybrid Encryption Algorithm throughout the encryption process, cloud-hosted data may be fully protected from potential attackers. When all the techniques used in this algorithm are executed with efficiency, the number of assaults launched by an attacker against the cloud host becomes inconsequential, since they will never be able to access the original data. This further decreases the probability of a successful attack. This algorithm will be improved in the years to come by using cutting-edge methods to improve data security. A static key, a generated plain text key, and the public key of the receiver may all be used to decode the contents of the data when someone else tries to decrypt it. Moreover, the number of cipher texts that are used will be greater than the initial quantity, which will make it difficult for the attacker to figure out the character count of the initial data.

References

Ahmad, A., AbuHour, Y., Younisse, R., Alslman, Y., Alnagi, E., & Abu Al-Haija, Q. (2022). MID-Crypt: a cryptographic algorithm for advanced medical images protection. *Journal of Sensor and Actuator Networks*, *11*(2), 24.

Akanksha, D., Samreen, R., Niharika, G. S., Shruthi, A., Kiran, M. J., & Venkatramulu, S. (2022). A hybrid cryptosystem based on modified vigenere cipher and polybius cipher. *EPRA Int. J. Res. Dev*, *7*, 2455-7838.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, *21*(3), 2671-2701.

Chaudhary, S., Suthar, F., & Joshi, N. (2020). Comparative study between cryptographic and hybrid techniques for implementation of

security in cloud computing. *Performance Management of Integrated Systems and its Applications in Software Engineering*, 127-135.

Dubey, R., Saxena, A., & Gond, S. (2015). An innovative data security techniques using cryptography and steganographic techniques. *International Journal of Computer Science and Information Technologies (IJCSIT)*, *6*(3), 2175-2182.

Gao, S., Wu, R., Wang, X., Wang, J., Li, Q., Wang, C., & Tang, X. (2023). A 3D model encryption scheme based on a cascaded chaotic system. *Signal Processing*, *202*, 108745.

Garg, P., Sharma, M., Agrawal, S., & Kumar, Y. (2019). Security on cloud computing using split algorithm along with cryptography and steganography. International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1,

Harinahalli Lokesh, G., & BoreGowda, G. (2021). Phishing website detection based on effective machine learning approach. *Journal of Cyber Security Technology*, *5*(1), 1-14.

Hidayat, T., Franky, D. S. T., & Mahardiko, R. (2020). Forecast analysis of research chance on AES algorithm to encrypt during data transmission on cloud computing. 2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP),

Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. *Archives of Computational Methods in Engineering*, *29*(6), 3587-3608.

Li, Q., Wang, X., Ma, B., Wang, X., Wang, C., Gao, S., & Shi, Y. (2021). Concealed attack for robust watermarking based on generative model and perceptual loss. *IEEE Transactions on Circuits and Systems for Video Technology*, *32*(8), 5695-5706.

Md, H. (2021). Enhancing the security of caesar cipher algorithm by designing a hybrid cryptography system. *Int. J. Comput. Appl*, *183*, 55-57.

Murad, S. H., & Rahouma, K. H. (2021). Hybrid cryptographic approach to safeguard cloud computing services: a survey. Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2021,

Murad, S. H., & Rahouma, K. H. (2022). Hybrid cryptography for cloud security: Methodologies and designs. Digital Transformation Technology: Proceedings of ITAF 2020,

Nadeem, M., Arshad, A., Riaz, S., Zahra, S. W., Dutta, A. K., Al Moteri, M., & Almotairi, S. (2023). An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms. *Computers, Materials & Continua*, *74*(2).

Pöpper, C. (2024). *Applied Cryptography and Network Security: 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024, Proceedings. Part I* (Vol. 14583). Springer Nature.

Priya, P. M. (2022). Hybrid Diagonal Transposition Cipher Model for Securing Data in Software Defined Networks. *Journal of Science & Technology (JST)*, *7*(4), 60-87.

Saxena, S., Shrivastava, A., & Birchha, V. (2019). A proposal on phishing url classification for web security. *International Journal of Computer Applications*, *178*(39), 47-49.

Schlatt, V., Guggenberger, T., Schmid, J., & Urbach, N. (2023). Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *International journal of information management*, *68*, 102470.

Suhael, S. M., Ahmed, Z. A., & Hussain, A. J. (2024). Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem. *Baghdad Science Journal*, *21*(1), 0151-0151.

Sun, H., & Grishman, R. (2022). Lexicalized Dependency Paths Based Supervised Learning for Relation Extraction. *Computer Systems Science & Engineering*, *43*(3).

Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A hybrid encryption and decryption algorithm using caesar and vigenere cipher. Journal of Physics: Conference Series,

Upadhyay, D., Zaman, M., Joshi, R., & Sampalli, S. (2021). An efficient key management and multi-layered security framework for SCADA systems. *IEEE Transactions on Network and Service Management*, *19*(1), 642-660.