iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52986

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Cryptographic Technique for Communication System

Mr. Aditya Sam Koshy[1], Mr. Aditya Bhardwaj[2], Mr. Anmol Saroha[3], Mr. Abhinav Dwivedi[4], Mr. Amish Jha[5], Mr. Aradhy Mishra[6]
IMS Engineering College

Abstract: ***The Cryptography is gotten from a Greek word which implies the craft of ensuring data by changing it into a muddled organization and unreadable format. It is a mix of arithmetic and software engineering. The dynamite growth of the Internet has made an expanded familiarity with intrigue uncertainty issues. Even though security is the measure worries over the internet, numerous applications have been created and structured without considering fundamental destinations of data security that is confidentiality, authentication, and protection. As our day by day exercises become increasingly more dependent upon data networks, the significance of an understanding of such security issues and trouble will also increase. To forestall some undesirable clients or individuals to gain admittance to the data, cryptography is required. .This paper introduces a new hybrid security cipher by combining the three most important Ciphers such as Gronsfeld Cipher , Polybius Cipher and Vigenere Cipher. This` hybrid encryption cipher provides greater security as compared to classic ciphers.***

I. INTRODUCTION

In today's rapidly advancing world, technological innovations have reached a point where the majority of people prefer using the internet as the primary means to transmit information across the globe. There are numerous ways to communicate information using the internet, such as through emails and chats. The internet has made data exchange incredibly convenient, fast, and accurate. However, one of the main challenges of transmitting data over the internet is the inherent "security risk" it poses. Personal or sensitive information can be compromised or hacked in various ways. Therefore, it becomes crucial to prioritize data security during the process of data transfer [1]. Security plays a significant role in open networks, and cryptography serves as a vital tool in this field. Cryptography is an ancient and secure method of protecting information in public networks. However, the purpose of cryptography extends beyond providing confidentiality; it also addresses other issues such as data integrity, authentication, and non-repudiation [2]. Cryptography can be defined as a set of techniques and methods used to transmit valuable data and information securely, ensuring that only the intended recipient can access and retrieve this information [2]. Cryptography involves a systematic approach and procedure to conceal data and information during communication. It is an art of hiding information from unauthorized individuals. As technology advances, the need for data security over communication channels has become increasingly critical. Encryption is the systematic process of converting plain text messages into ciphertext. The encryption process requires an automated encryption algorithm and a key to transform the plain text into encrypted form, known as ciphertext [3]. In the cryptography system, encryption is performed at the sender's end before transmitting the message to the receiver. Decryption is the reverse systematic process of encryption, which converts encrypted ciphertext back into plain text messages. In the cryptography system, the decryption process is executed at the receiver's end. It involves several steps, including a decryption algorithm and a key. Cryptography can be broadly categorized into two classes based on the key used, which serves as the instruction to convert original text into encrypted content: Asymmetric Key Encryption and Symmetric Key Encryption. Symmetric key encryption employs the same key for both encryption and decryption processes. While this system is simple yet powerful, the key distribution becomes a critical issue that needs to be addressed. On the other hand, asymmetric key encryption utilizes two mathematically related keys: a Public Key and a Private Key for encryption. The public key is accessible to everyone, but any data encrypted with a user's public key can only be decrypted using the corresponding private key of that specific user, whether acting as a sender or receiver. The use of symmetric key encryption ensures efficient and fast encryption and decryption processes since the same key is employed. However, the challenge lies in securely distributing and managing the shared key. Any compromise of the key would jeopardize the security of the encrypted data. Asymmetric key encryption overcomes this challenge by utilizing a pair of mathematically related keys. In asymmetric key encryption, the public key is widely available and can be freely shared with others. It is used for encrypting data before transmission. On the other hand, the private key is kept secret and known only to the intended recipient. The private key is used for decrypting the received data. The mathematical relationship between the public and private keys ensures that data encrypted with the public key can only be decrypted with the corresponding private key, establishing a secure communication channel [2].

©IJRASET: All Rights are Reserved

This method offers several advantages. First, it eliminates the need for secure key distribution, as the public key can be openly shared. Second, it enables digital signatures, where the sender can encrypt a message with their private key, providing authentication and non-repudiation. The recipient can verify the signature using the sender's public key, ensuring the integrity of the message and confirming the identity of the sender.

However, asymmetric key encryption tends to be computationally more expensive compared to symmetric key encryption. Therefore, a common approach is to combine both encryption methods, known as hybrid encryption. In hybrid encryption, a symmetric key is generated for each session, and the actual data is encrypted using the symmetric key. Then, the symmetric key is encrypted with the recipient's public key and transmitted along with the encrypted data. The recipient can decrypt the symmetric key using their private key and use it to decrypt the actual data, achieving a balance between security and efficiency.

Cryptography plays a vital role in ensuring the confidentiality, integrity, authentication, and non-repudiation of data during its transmission over the internet. By employing encryption algorithms and key management techniques, sensitive information can be protected from unauthorized access, minimizing the risks associated with data transfer [2].

In conclusion, cryptography provides the necessary tools and techniques to secure data during its journey across the internet. Whether through symmetric key encryption or asymmetric key encryption, the confidentiality and integrity of information can be preserved. As technology continues to evolve, cryptography will remain a crucial aspect of data security, enabling secure and reliable communication in the digital age.

II. LITERATURE SURVEY

In the current era, technological advancements have reached a point where the majority of people prefer utilizing the internet as the primary means to transmit information globally. There are various methods available for communicating information through the internet, such as email and chat platforms. The internet enables data transfer to be quick, effortless, and accurate. However, one of the significant challenges associated with transmitting data over the internet is the inherent "security risk," which can result in the compromise or unauthorized access of personal or sensitive information. Therefore, it becomes crucial to prioritize data security as a vital factor during the process of data transfer [1].

Security plays a pivotal role in public networks, and cryptography is instrumental in this domain. Cryptography, an ancient and secure method of information protection in public networks, aims not only to provide confidentiality but also to address other issues, including data integrity, authentication, and non-repudiation [2]. Cryptography refers to the art and science of concealing information during communication, ensuring that only the intended recipient can retrieve the data [2].

Cryptography represents a systematic technique and process for concealing information during communication. It serves as a means to hide information from unauthorized entities. As technology advances, the demand for data security over communication channels has significantly increased.

Encryption is a systematic process of converting plain text messages into ciphertext. The encryption process involves the use of an encryption algorithm and a key to convert the plain text into encrypted form [3]. In a cryptographic system, encryption is performed at the sender's end, ensuring that the message is encrypted before transmission to the receiver.

Decryption, on the other hand, is the reverse process of encryption. It involves converting the encrypted ciphertext back into plaintext. In a cryptographic system, decryption is performed at the receiver's end and requires a decryption algorithm and a key.

Cryptography is broadly categorized into two classes based on the key, which refers to the set of instructions used to convert original text into encrypted text: Asymmetric Key Encryption and Symmetric Key Encryption. Symmetric key encryption utilizes the same key for both encryption and decryption processes. While this system is simple yet powerful, the distribution of the key poses a significant challenge. On the other hand, asymmetric key encryption employs two mathematically related keys: the Public Key and the Private Key. The public key is available to everyone, but data encrypted using a user's public key can only be decrypted by that specific user's private key, whether they are the sender or the receiver.

III. THEORIES

PCs may become unreliable when connected to a global network, particularly the internet [2]. Many websites that are frequently visited are infected with viruses, malware, or similar threats that can compromise personal data stored on a computer. To avoid data replication, theft, visualization, detection, and intrusion, maintaining security is crucial. The essence of PC security lies in ensuring the safety and protection of data within the computer system [13].

PC security encompasses various aspects, including:

1) *Privacy:* It involves the confidentiality of information. The primary objective is to prevent unauthorized individuals from accessing sensitive data. Encryption technology can be employed to achieve prevention, allowing only the data owner to access the actual information.
2) *Confidentiality:* It entails a set of rules or agreements that limit access or impose restrictions on specific types of information. When required to provide evidence of someone's wrongdoing, the data custodian decides whether to disclose the requested information or maintain client confidentiality.
3) *Non-repudiation:* It refers to the ability to ensure that the parties involved in an agreement or communication cannot deny the authenticity of their signature on a document or the sending of a message initiated by them. To disavow means to deny. Over time, efforts have been made to make repudiation impossible in certain circumstances. For example, sending registered mail ensures that the recipient cannot deny receiving a letter. Similarly, legal documents often require witnesses to sign to prevent denial of signing. On the Internet, a digital signature is used not only to verify that a message or document has been electronically signed by the intended person but also, since a digital signature can only be created by one individual, to prevent later denial of providing the signature.
4) *Integrity:* Data integrity refers to the reliability and accuracy of data throughout its lifecycle. It ensures that data remains valid and free from manipulation or corruption.
5) *Authentication:* It is a security measure designed to establish the validity and identity of a transmission, message, or originator, or to verify a person's authorization to access specific categories of information. Authentication is performed to verify the credentials of a user attempting to log in before granting access to the system. It is a critical process for information protection.
6) *Availability:* It ensures that systems, applications, and data are accessible to users when they require them. The most common attack that affects availability is a denial of service, where an attacker disrupts access to data, systems, devices, or other network resources. In an internal vehicle network, a denial of service could lead to an Electronic Control Unit (ECU) being unable to access the necessary data, rendering it nonoperational or even endangering the system. To avoid availability issues, redundancy paths, failover procedures, and intrusion prevention systems that can monitor network traffic patterns and detect abnormalities should be included in the design phase.

7) *Cryptography*

Cryptography comprises four fundamental components:

a) *Plaintext:* It refers to a readable message.
b) *Ciphertext:* It is an encrypted, unreadable, and unintelligible message.
c) *Key:* It is a crucial element that defines cryptographic techniques, such as symmetric and asymmetric encryption.
d) *Algorithm:* It is a procedural solution for executing encryption and decryption processes in a system.

8) *Cipher:* In cryptography, a cipher (or encryption algorithm) is a series of well-defined steps used to perform encryption or decryption. Another less common term is encipherment. Enciphering or encoding involves converting data from plaintext into a cipher or code. In non-technical usage, "cipher" is often used interchangeably with "code"; however, the concepts are distinct in cryptography. Traditional cryptography distinguished ciphers from codes. Codes typically substitute variable-length sequences of characters in the output, while ciphers often substitute an equal number of characters from the input.

A. *Gronsfeld Cipher*

The Gronsfeld cipher, also known as the Bronckhorst cipher, was created by José de Bronckhorst, the Earl of Gronsfeld, in 1744. He was a Belgian diplomat who developed this cipher to secure his communications. The Gronsfeld cipher is a type of polyalphabetic cipher, specifically a series of Caesar ciphers, where the shift value is determined by numbers ranging from 0 to 9. It is similar to the Vigenère cipher, but instead of using letters for the key, it employs digits.

In the Gronsfeld cipher, each letter is shifted a certain number of positions based on the secret key. For example, if the secret key is 1234, the shifts will be 1, 2, 3, 4, 1, 2, 3, 4, and so on.

Similar to the Vigenère cipher, the Gronsfeld cipher is vulnerable to letter frequency analysis. Its key strength is more limited compared to the Vigenère cipher because the shifts can only be between 0 and 9. Unless the key is lengthy, it can be cracked using brute force methods.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Gronsfeld Cipher is a cryptography method that works like a Vigenere Cipher. Gronsfeld Cipher uses keys from decimal numbers instead of letters, but sometimes it can uses ASCII as the key substitustion. The key will be repeated periodically with the intention that each plaintext has a key. It has the same length as plaintext. When the user enters a key that is smaller in length than plaintext, the key will automatically be repeated from the beginning for the next plaintext .

There are two models of use of characters in the Gronsfeld algorithm. This algorithm can use 256 ASCII characters or use only 26 alphabetical characters.

The following equations are the formulas used to implement the Gronsfeld algorithm.

- *Encryption*

$E\ (x) = (P\ (x) + K\ (x))\ mod\ 26$

$E\ (x) = (P\ (x) + K\ (x))\ mod\ 256$

- *Decryption*

$D\ (x) = (P\ (x) - K\ (x))\ mod\ 26$

$D\ (x) = (P\ (x) - K\ (x))\ mod\ 256$

B. Vigenere Cipher`

The Vigenere Cipher is a cryptographic technique used to scramble messages consisting of letters from A to Z. It utilizes a simple form of polyalphabetic substitution, which relies on multiple sets of substitution alphabets. The initial encryption of the plaintext is accomplished using the Vigenere square table.

Vigenere square table [14].`

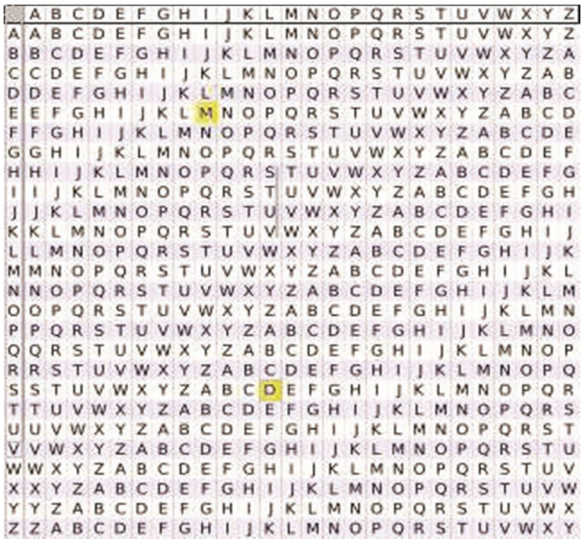


Fig. 1: Vigenere Square Table`

- *Encryption*

To encrypt the plaintext, each letter in the plaintext is combined with the corresponding letter from the key. For example, if the plaintext letter is 'S' and the key letter is 'L', their intersection in the Vigenere square table results in the output letter 'D'. Similarly, by following this process for each letter, the entire message can be encoded. The plaintext (P) and key (K) are added and then taken modulus 26.

The plaintext (P) and key (K) are added modulus 26.

Ei = [Pi + Ki] mod 26 (1)

Using (1), one may convert plaintext into ciphertext as shown below.

Plaintext: SECURITY Key: LIONLION Ciphertext: D M Q H C Q H L

©IJRASET: All Rights are Reserved

- *Decryption*

Decryption involves finding the row corresponding to the key and the column corresponding to the ciphertext letter. The plaintext is obtained from the intersection of the row and column. For example, using the key 'LIONLION' (row L) and the ciphertext letter 'D' (column), the resulting plaintext letter is 'S'. By applying this process to all the ciphertext letters, the original plaintext can be retrieved. The Vigenere table can be viewed logarithmically by converting alphabets [A-Z] into numbers [0-25].

Di = (Ei - Ki + 26) mod 26 (2)

C. Polybius Square Cipher

The Polybius square is a 5x5 grid filled with letters used for encryption. It allows the conversion of letters into numbers. To make the encryption more challenging, the table can be randomized and shared with the recipient.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fig. 2: Polybius Square

In order to fit the 26 letters of the alphabet into the 25 cells of the table, the letters 'I' and 'J' are usually combined into a single cell. Originally, this was not a problem as the ancient Greek alphabet had 24 letters. If a language has a larger alphabet, a table of a larger size can be used. [15].

- *Encryption*

Example: D is placed in row 1 and column 4, so it results in output coded as 14; O is placed in row 3, column 3, it is result output coded as 34. So, Encrypted message result message DOG as 14, 34, 23.

- *Decryption*

Polybius decryption requires knowing the grid and consists of a substitution of a couple of coordinates by the corresponding letter in the grid.

Example: 12 visualize for 1st line and 2nd column, as result letter B, 45 visualize for 4th line and 5th column that result U and continues as same.

IV. METHODOLOGY

1) *Research the Database of Drugs and their Effects:* Start by researching information about various drugs and their effects. This can be done by consulting various medical databases and resources, as well as researching drug-related news articles and reports. Anonymously.
2) *Develop a user Interface:* Create a user interface (UI) for the app using Flutter. This should make it easy for users to report drug use anonymously. Consider using a simple, intuitive design that will be easy to use.
3) *Design a Database:* Design a database to store the data that is collected from the app. This should include information such as the type of drug, the amount used, and any side effects that the user has experienced.
4) *Create a Reporting System:* Create a reporting system that will allow users to submit reports anonymously. Ensure that the system is secure and encrypted and that it collects only the necessary data. **5. Test and launch the app:** Test the app to ensure that all of the features are working correctly. Once everything is working, launch the app and make it available to users. Make sure to continue to monitor the app for any potential issues.
5) *Test and Launch the App:* Test the app to ensure that all of the features are working correctly. Once everything is working, launch the app and make it available to users. Make sure to continue to monitor the app for any potential issues.

Steps

a) Create the project: Create a new project in Flutter and choose the right UI components for your app.
b) Design the User Interface: Design the user interface of the app to make it easy for users to report drugs anonymously.
c) Develop the Backend: Develop the backend of the app to store the data from the users and to deliver it to relevant authorities.
d) Integrate Security Features: Implement security features such as encryption and user authentication to prevent unauthorized access to confidential data.
e) Test the App: Test the app extensively to make sure it works properly and that the reported data is accurate.
f) Deploy the App: Deploy the app to the appropriate store and make it available to users.
g) Monitor and Maintain: Monitor the app and maintain it regularly to ensure it is up-to-date and secure.

V. IMPLEMENTATION

The implementation of drug reporting applications using Flutter can be done in the following steps:

1) *Create a New Project:* Create a new project in Flutter and name it appropriately.
2) *Design the UI:* Design the user interface and layout for the application. Make sure that all the necessary elements are included such as a text field for entering the drug name, a dropdown for selecting the type of drug, a form for submitting the report, and a submit button.[5] The authentication and authorization part can be implemented using Firebase Authentication. Firebase Authentication is an authentication service provided by Google that allows users to sign in using their email address or phone number. Firebase Authentication also provides various methods of authentication such as OAuth, SMS, and social media providers. The user can be authenticated and authorized using Firebase Authentication.[5]
3) *Add Data Validation:* Add validation to the form fields such as checking for valid drug names and types.
4) *Connect to the API:* Connect the application to the backend API to submit the drug report.
5) *Implement the API:* Implement the API to handle the drug report requests.
6) Test the application: Test the application to make sure everything is working as expected.
7) *Implement two-factor Authentication:* Two-factor authentication is a security measure that requires a user to provide two pieces of evidence to gain access to an account. This can be done by using a mobile phone number or email address for authentication
8) Encrypt data: Encrypt the data that is being transferred between the client and the server.
9) *Use a Secure Connection:* Use a secure SSL connection for all communication between the client and the server.
10) *Implement a Privacy Policy:* Implement a privacy policy that clearly outlines how user data is used, stored, and shared.[5]
11) *Deploy the Application:* Deploy the application to the app store and play store.To make the drug reporting application more secure and anonymous, the following measures can be taken:

VI. CONCLUSION

Drug abuse is a serious and growing problem in the world today. Anonymous reporting of drug use can be an effective tool in helping to fight against and reduce the prevalence of drug abuse. Furthermore, anonymous reporting can provide individuals with an opportunity to get help without fear of repercussions. Ultimately, anonymous reporting can be a powerful tool in helping to reduce drug abuse and help individuals to get the help they need.

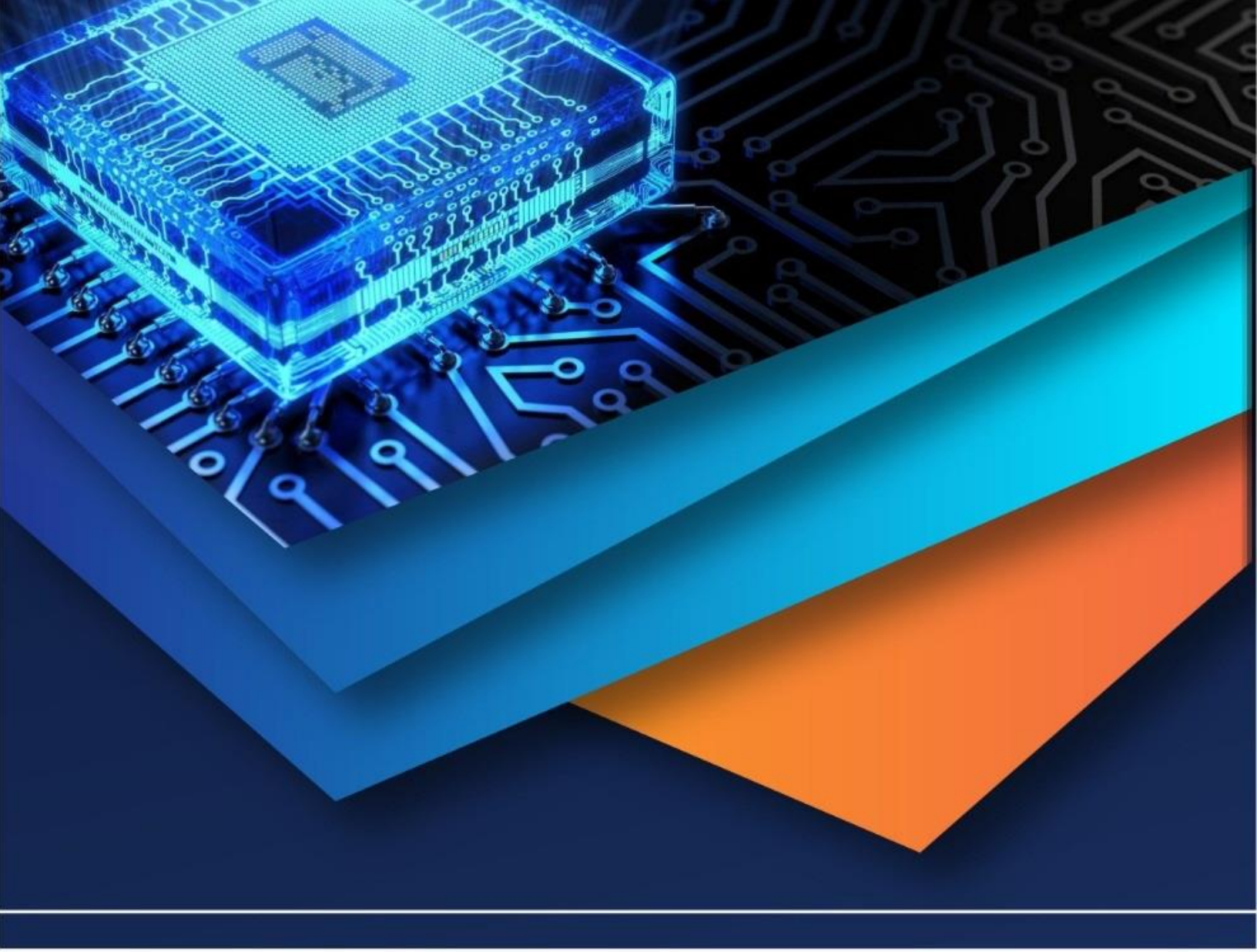
VII. FUTURE WORK

Real-time notifications: Send alerts to physicians and pharmacists when a patient may be at risk of an adverse reaction to a particular drug. Automated data entry: Reduce manual data entry by automating the process of collecting, validating, and submitting data to the reporting system. Drug interaction checker: Compare the patient's current medications to ensure no interactions exist. Patient education materials: Provide resources to patients that are tailored to their individual needs, such as information about drug side effects, dietary recommendations, and lifestyle changes. Machine learning algorithms: Utilize machine learning algorithms to detect patterns in drug-related data, which can be used to improve drug safety. Analytics and reporting: Generate reports for drug safety monitoring, such as trends in adverse reactions or correlations between drugs and adverse events. Integration with electronic health records (EHRs): Automatically capture patient data from EHRs to streamline drug reporting processes. Using flutter for developing drug reporting applications can be beneficial in terms of user experience and development speed. However, developers must be aware of the challenges that they may face when using this technology, including security, accessibility, and compatibility. With the right tools and strategies, these challenges can be overcome, allowing developers to create effective and efficient drug reporting application.[1,2,5]

©IJRASET: All Rights are Reserved

REFERENCES

[1] S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, "A research paper on new hybrid cryptography algorithm."
[2] K. Jakimoski, "Security techniques for data protection in cloud computing," International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.
[3] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigenere cipher for` data security," Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.
[4] P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.
[5] A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., "An extended hybridization of vigenere and caesar cipher techniques for secure com-´ munication," Procedia Computer Science, vol. 92, pp. 355–360, 2016.
[6] J. Chen and J. S. Rosenthal, "Decrypting classical cipher text using markov chain monte carlo," Statistics and Computing, vol. 22, no. 2, pp. 397–413, 2012.
[7] M. B. Pramanik, "Implementation of cryptography technique using columnar transposition," International Journal of Computer Applications, vol. 975, p. 8887, 2014.
[8] C. Sanchez-Avila and R. Sanchez-Reillol, "The rijndael block cipher (aes proposal): a comparison with des," in Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186). IEEE, 2001, pp. 229–234.
[9] Q.-A. Kester, "A cryptosystem based on vigenere cipher with varying` key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, no. 10, pp. 108–113, 2012.
[10] C. Bhardwaj, "Modification of vigenere cipher by random numbers,` punctuations & mathematical symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278–0661, 2012.
[11] F. M. S. Ali and F. H. Sarhan, "Enhancing security of vigenere cipher` by stream cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 1–4, 2014.
[12] P. Gutmann, Cryptographic security architecture: design and verification. Springer Science & Business Media, 2003.
[13] A. P. U. Siahaan, "Protection of important data and information using gronsfeld cipher," 2018.
[14] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using vigenere cipher and goldbach codes algorithm,"` Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.
[15] M. Maity, "A modified version of polybius cipher using magic square and western music notes," International Journal For Technological Research In Engineering, ISSN, pp. 2347–4718, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)