FMDB *Transactions on Sustainable Computing Systems*

Fortifying Data Security: A Multifaceted Approach with MFA, Cryptography, and Steganography

K. Daniel Jasper[1,*], R. Neha[2], András Szeberényi[3]

[1,2]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[3]Department of Business, Communication and Tourism, Institute of Marketing and Communication Science, Budapest Metropolitan University, Budapest, Nagy Lajos Király Útja, Hungary.
dk9127@srmist.edu.in[1], rr2499@srmist.edu.in[2], aszeberenyi@metropolitan.hu[3]

Abstract: Multi-factor authentication is a useful method of strengthening authentication to avoid brute force attacks and make a strong layer of protection. Verifications and validations have been incorporated into this multi-factor authentication technique in order to make it more human-centric. The technique of concealing or encoding information in such a way that only the recipient of a message is able to read it is referred to as cryptographic algorithms. By manually managing a key and replacing the alphabet and digits with specific characters, only authorised individuals will be able to use it, which will result in the data being more secure and private. Steganography is the method that is used for the second verification, which involves evading detection. Steganography is a methodology that encodes essential data into a file or message that appears to be harmless. It will be impossible to discover the sensitive material once it reaches its final destination since it will be extracted from a file or communication that appears to be completely normal. Steganography adds an additional layer of protection to sensitive information when it is combined with encryption. This procedure is included because it is necessary to add an additional layer of protection to this project in order to improve the safety of the data. Additionally, the Figma tool was utilised as a design output measure for this project.

Keywords: Multi-factor Authentication; Cryptography; Steganography; Cipher Text; Encryption and Decryption; Data Security and Confidentiality; Integrity and Availability; Fortifying Data Security.

Received on: 27/01/2023, **Revised on:** 13/04/2023, **Accepted on:** 02/06/2023, **Published on:** 26/11/2023

Cited by: K. Daniel Jasper, R. Neha, and A. Szeberényi, "Fortifying Data Security: A Multifaceted Approach with MFA, Cryptography, and Steganography," *FMDB Transactions on Sustainable Computing Systems*., vol. 1, no. 2, pp. 98–111, 2023.

1. Introduction

Cryptography is the art and science of encoding messages so only the intended recipient can decipher them. Cryptography is an age-old practise still used today for encoding communications in many digital forms, including bank cards, passwords, and online shopping [12]. Encryption keys of 128 and 256 bits are examples of modern cryptography techniques that utilise algorithms and cyphers to encrypt and decrypt data. Advanced Encryption Standard (AES) and other modern cyphers are nearly impenetrable [13]. Encoding data such that only the intended recipient can decipher and process it is known as cryptography [14]. Computer science, mathematics, engineering, and other branches of science come together in this cybersecurity profession called cryptology to construct elaborate codes that conceal a message's actual meaning [15]. Even though cryptography has its roots in ancient Egyptian hieroglyphics, it is still essential for protecting data and communications in transit from prying eyes. It safeguards financial transactions, email, web browsing, and data privacy by converting messages into difficult-to-decipher codes using cryptographic keys and digital signing [16]. For cryptography and safe systems, the "CIA triad" describes the three

[*]Corresponding author.

primary objectives [17]. The CIA trinity consists of availability, honesty, and secrecy. All of these stand for crucial characteristics of data and numerous safe systems.

1.1. Confidentiality

The purpose of maintaining confidentiality is to make sure that no one other than authorised parties can access sensitive data. Individuals' awareness of and consent to collecting and using their personal information is also relevant. Confidentiality is compromised when unauthorised parties gain access to information [18]. We employ encryption techniques to guarantee secrecy, which is the connection between cryptography and confidentiality. Depending on the circumstances, the encryption techniques might be either symmetric or asymmetric [19].

1.2. Integrity

This idea is based on the capacity to guarantee that the data is altered according to certain standards. This should ensure the information is authentic and cannot be disproven [20]. Systems are also included. Loss of integrity occurs when data is altered or deleted without authorization from a system. We can ensure integrity using cryptographic hash functions, specifically HMAC [21].

1.3. Availability

Making sure that resources, such as data and services, are easily accessible is what the word "availability" refers to. Furthermore, authorised individuals must not withhold information or services from others. In and of itself, cryptography does not guarantee availability [22]. In most cases, network policies and design are what guarantee availability. For instance, if we use a cloud service such as Google Cloud, Azure, etc., those services guarantee availability because they provide redundancy. This means service is provided using several geographically distributed servers (a.k.a. data servers). In this case, the provider ensures we are available. Another way to guarantee availability is to know what normal traffic looks like for us so that we can take action when there is an attack on our services [23]. In particular, we can use IDS to ensure availability. Common attacks that make our services unavailable are DOS and DDOS attacks (Fig.1).

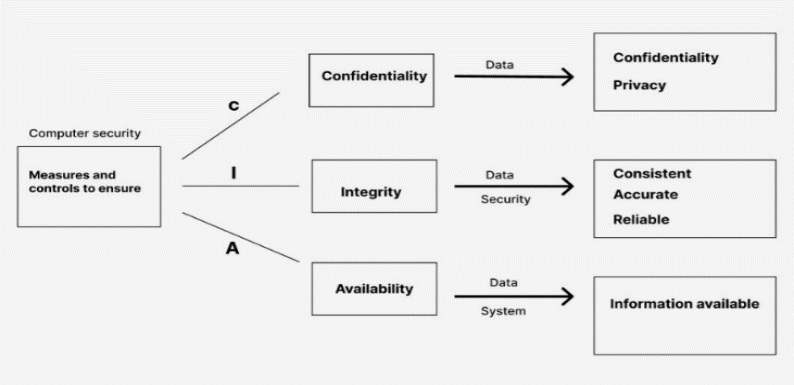

Figure 1: Flowchart of CIA

1.4. Types of Cryptography

Cryptography comes in many forms, each with its advantages and uses. Here are a few examples of the most popular forms of encryption:

Symmetric-key cryptography: Data encryption and decryption with a single key is the essence of this cryptographic method. The sender and receiver utilise the same secret key [24].

Asymmetric-key cryptography: Data encryption and decryption in asymmetric-key cryptography, often called public-key cryptography, involve the use of two keys: a public key and a private key. Anyone can access the public key, but only the owner knows the private key [25].

1.5. Hash Functions

A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with (Fig.2).

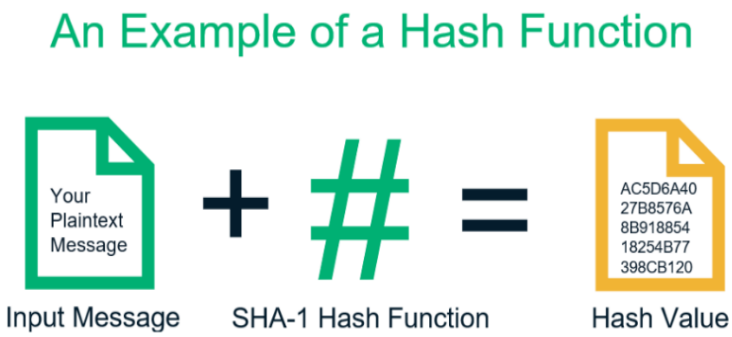

Figure 2: Hash functions [10]

2. Data Security

Data security safeguards digital information throughout its life cycle to protect it from corruption, theft, or unauthorized access. It covers everything: hardware, software, storage devices, user devices, access and administrative controls, and the organization's policies and procedures [26]. Data security uses technology and techniques that make a company's data and usage more transparent. Masking data, encrypting it, and redacting sensitive information are all ways these tools help keep data safe. Organizations can simplify auditing operations and meet the ever-tightening data protection laws with the help of this approach. A business can safeguard its information from cyberattacks by implementing a strong data security management and strategy approach [27].

Additionally, it reduces the likelihood of insider threats and human mistakes, the latter of which is a major contributor to data breaches. A steganography project's data security goals include a wide range of actions to protect private and sensitive data [28]. To improve information security generally, the project employs steganographic techniques to make data more resistant to theft, alteration, eavesdropping, and surveillance. The process of data authentication can also make use of steganography [29]. To ensure that data has not been altered while in transit or storage, it is feasible to check its authenticity by inserting unique identifiers into digital files [30]. Enhance data security by developing and implementing steganographic techniques to protect sensitive information from unauthorized access (Fig.3).

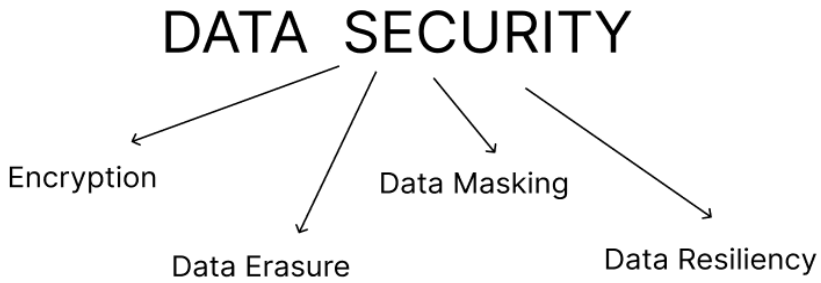

Figure 3: Data security types

2.1. Multi-factor Authentication

Verification methods needed for MFA are ones' unauthorised users cannot possibly have. Since passwords alone cannot guarantee a user's identity, multi-factor authentication (MFA) introduces an extra layer of security. Two-factor authentication is the most popular MFA implementation (2FA) [31]. The idea behind this is that criminals won't be able to fool users with only one piece of evidence, let alone two or more. At least two distinct types of factors are required for proper multi-factor

authentication [32]. It defeats the purpose of an MFA to use two of the same kind. Passwords and security questions are often used together; however, they do not constitute multi-factor authentication (MFA) as they are both knowledge-based. Both permanent and temporary passcodes are acceptable forms of authentication since the passcode serves as proof of ownership for a particular email account or mobile device [33]. Organizations face more dangers and a larger need for security measures as they digitise operations and assume more obligations to store consumer data. Because hackers have long used user login credentials to access vital systems, user identity verification has become crucial [34].

Username and password-based authentication are cumbersome and prone to errors since people may struggle to store, recall, and manage these credentials across several accounts [35]. Many people use the same simple password for all their accounts. Passwords also provide weak security because they are easily obtainable through hacking, phishing, and malware. Attacks like phishing and hacking can cost a pretty penny [36]. The organization's security is enhanced since MFA helps protect systems from unauthorised users and the risks they pose. If businesses are afraid to compel users to comply with stricter security measures, they should consider how users, particularly customers, could value the added protection for their data [37]. Customers are more inclined to trust a vendor's overall security measures when they trust such measures, making multi-factor authentication a significant competitive advantage (Fig.4).

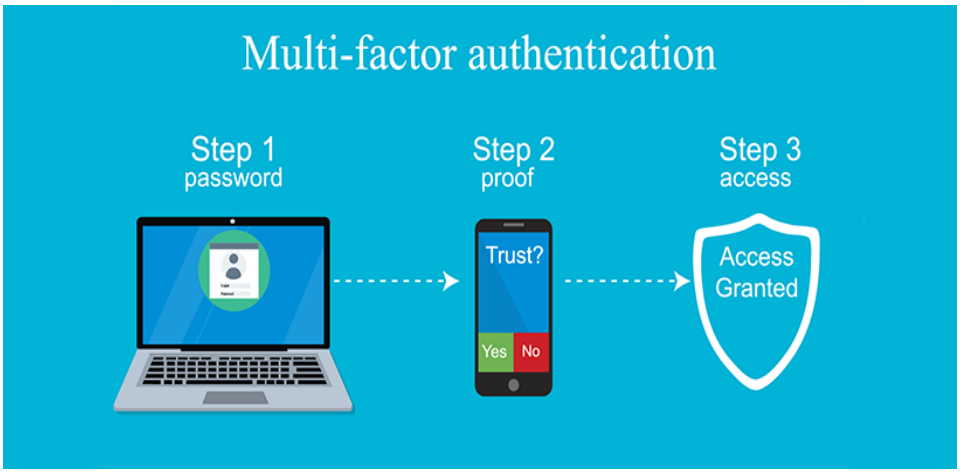

Figure 4: Multi-factor authentication [11]

3. Review of Literature

Cryptography and MFA in Decryption Key Management Cryptography and Multi-factor Authentication (MFA) play pivotal roles in ensuring the confidentiality and security of digital information. It requires users to provide multiple authentication factors, such as something they know (e.g., passwords), something they have (e.g., tokens or smartphones), and something they are, e.g., biometrics. Sinigaglia et al. [1] explore the multifaceted realm of two-factor authentication (2FA). It encompasses an in-depth analysis of various authentication factors, including passwords, tokens, and biometrics. The paper delves into the security strengths and usability aspects of 2FA, offering insights into its effectiveness against common online threats. Additionally, it highlights emerging trends and future directions in the dynamic field of online transaction security.

Ibrahim et al. [2] present an innovative approach to multi-factor authentication. It enhances security by combining colour visual cryptography, facial recognition, and dragonfly optimization. The paper likely discusses the advantages of this multifaceted authentication system, which integrates visual cryptography and biometrics. Dragonfly optimization is employed to optimize system performance. This research contributes to the evolving field of multi-factor authentication by combining different factors for enhanced security.

Wang et al. [3] investigate the vulnerabilities and security shortcomings of multi-factor authentication (MFA) schemes in multi-server environments. It likely identifies common weaknesses in MFA implementations across multiple servers and explores potential threats. This research highlights the importance of addressing security gaps in MFA systems to strengthen multi-server network protection, making it valuable to information security.

Ryu et al. [4] state the biometric process's importance. The paper reviews continuous multimodal biometric authentication, emphasizing the significance of ongoing user verification. It provides insights into the security, reliability, and emerging trends in biometric authentication methods, making it a valuable resource in identity verification.

Bezzateev et al. [5] discussed secret sharing using Newton's polynomial as a method for multi-factor authentication within the field of cryptography. It explores how mathematical techniques like Newton's polynomial can be leveraged to enhance security and protect sensitive information in multi-factor authentication systems.

Zhang et al. [6] introduce SMAKA, a secure many-to-many authentication and key agreement scheme for vehicular networks. It addresses the complex authentication and key management needs in vehicular communication, enhancing security and ensuring safe and efficient vehicle data exchange.

Mukherjee et al. [7] present an image steganography technique that leverages the construction of fake DNA sequences to hide information. The method explores a unique approach to covertly embedding data within images, offering potential applications in secure communication and information concealment.

Chai et al. [8] introduce a colour image compression and encryption scheme that combines compressive sensing with a double random encryption strategy. The method aims to compress and secure colour images efficiently, particularly within image management systems. It highlights the integration of compression and encryption for improved data management and security.

Zhou et al. [9] present a novel image encryption algorithm based on Latin square matrices. The algorithm explores a unique approach to secure image data, contributing to image encryption. It is designed to enhance the security of images by applying Latin square matrices.

4. Proposed Method

This method is proposed to avoid brute-force attacks. To avoid brute force attacks, this project brings the concept of Multi-factor authentication with two verifications to access the key of the decryption key to access key. It ensures that only authorized persons can access the key [38]. The first method is based on Cryptography principles, which uses a substitution method that substitutes the 26 alphabets and ten numbers into a symbol given the key; only authorized persons can pass the verification one and go to the next [39]. The steganography method is used to hide data in the form of text, image, audio, etc. In this project, we used hidden data in the form of text-based data and added one more level of security to access the key. The diagram helps you to understand more about the flow of the project (Fig.5).

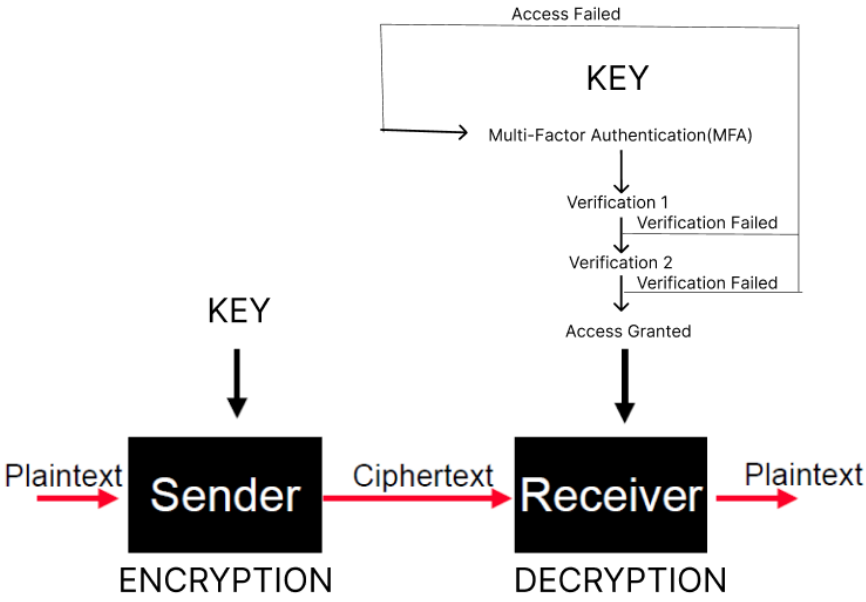

Figure 5: Proposed method

Cryptography is the science and practice of securing information by transforming it into an unreadable format, called Ciphertext, through various mathematical techniques and algorithms [40]. Cryptography aims to protect the confidentiality, integrity, and authenticity of data. Here is an overview of the general process of cryptography:

4.1. Plaintext

Plain text in cryptography refers to the original, unencrypted message or data to be protected. It is the information that is readable and understandable before undergoing encryption [41]. In the encryption process, plain text is transformed into

Ciphertext using cryptographic algorithms and encryption keys to prevent unauthorized access or comprehension by anyone without the proper decryption key [42]. This transformation ensures that sensitive information remains confidential and secure during transmission or storage, even with potential security threats.

4.2. Encryption

Plain text in cryptography refers to the original, unencrypted message or data to be protected. It is the information that is readable and understandable before undergoing encryption [43]-[47]. In the encryption process, plain text is transformed into Ciphertext using cryptographic algorithms and encryption keys to prevent unauthorized access or comprehension by anyone without the proper decryption key [48]. This transformation ensures that sensitive information remains confidential and secure during transmission or storage, even with potential security threats.

4.3 Symmetric Encryption

Plain text in cryptography refers to the original, unencrypted message or data to be protected. It is the information that is readable and understandable before undergoing encryption [49]. In the encryption process, plain text is transformed into Ciphertext using cryptographic algorithms and encryption keys to prevent unauthorized access or comprehension by anyone without the proper decryption key [50]. This transformation ensures that sensitive information remains confidential and secure during transmission or storage, even with potential security threats.

4.4 Asymmetric Encryption

Data encryption and decryption in asymmetric encryption, sometimes called public-key cryptography, entails the employment of a pair of keys [51]-[54]. A pair of keys consists of a public key that anybody can share and a private key that the owner keeps hidden. Asymmetric encryption entails the sender encrypting data using the recipient's public key. The data is decrypted by the receiver using their private key. Thanks to this method, two people can safely communicate with each other without sharing a secret key. Opting for asymmetric encryption instead of symmetric, which reuses the key for encryption and decryption, offers numerous benefits [55]-[59].

4.5 Ciphertext

Plain text in cryptography refers to the original, unencrypted message or data to be protected. It is the information in its readable and understandable form before undergoing encryption. In the encryption process, plain text is transformed into Ciphertext using cryptographic algorithms and encryption keys to prevent unauthorized access or comprehension by anyone without the proper decryption key [60]. This transformation ensures that sensitive information remains confidential and secure during transmission or storage, even with potential security threats.

4.6. Transmission or Storage

The Ciphertext can be safely transmitted over networks or stored in databases or devices. Even if an attacker intercepts the Ciphertext, they should not be able to decipher it without knowing the decryption key.

Transmission: Cryptographic techniques encrypt data before it's sent over networks or communication channels. This ensures that even if intercepted by unauthorized entities, the data remains unintelligible without the decryption key. Secure communication protocols, such as SSL/TLS for web traffic, employ encryption to safeguard sensitive information during transmission [61].

Storage: Cryptography also safeguards data at rest, such as stored on servers, databases, or physical media. This involves encrypting data before it's saved, making it inaccessible to anyone without the appropriate decryption key. Encryption of stored data is crucial in protecting sensitive information, especially in data breaches or unauthorized access to physical storage devices.

Cryptographic algorithms and key management practices are pivotal in maintaining data confidentiality, integrity, and security in transmission and storage.

4.7. Decryption

Plain text in cryptography refers to the original, unencrypted message or data to be protected. It is the information in its readable and understandable form before undergoing encryption. In the encryption process, plain text is transformed into Ciphertext using cryptographic algorithms and encryption keys to prevent unauthorized access or comprehension by anyone without the proper decryption key. This transformation ensures that sensitive information remains confidential and secure during transmission or storage, even with potential security threats.

4.8. Key Generation

First, you would generate a secret key, a string of characters, numbers, or symbols. For simplicity, let us use a basic key like "KEY123" as an example, in the key maps to another character in a known, predetermined manner. This rule could be as simple as shifting each character by a fixed number of positions in the alphabet. Key generation in cryptography is creating cryptographic keys for encryption and decryption. The key generation process typically involves utilizing cryptographic algorithms and random or pseudorandom sources to generate keys with a high degree of unpredictability. The length of the key is a crucial factor, as longer keys generally provide stronger security. Proper key management practices are essential to safeguard keys from unauthorized access or compromise. In many cryptographic systems, secure key distribution is a significant concern, as securely delivering keys to authorized parties is vital for data protection. Key generation also includes periodic key renewal to minimize risks associated with long-term key compromise (Table 1).

Table 1: Verification 1 (Key Verification using Substitution Method)

Alphabets & Numbers	Substitution rule
A	(•.•)
B	(^ ^)
C	|•!•|
D	{^*^}
E	[<+>]
F	{^=^}
G	€• •€
H	{? ?}
I	\• •/
J	{-^-}
K	{<• •>}
L	(<•~•>)
M	(•!•)
N	[•!•]
O	{^!^}
P	:'(
Q	:')
R	-(^=^)-
S	+{^+^}+
T	(+ • +)
U	{<•>}
V	[^<>^]
W	|^~^|
X	|^••^|
Y	(• •)
Z	(•~•)
0	₹
1	&
2	@
3	%
4	#
5	£
6	€
7	?
8	!
9	0

Algorithm

STEP 1: ANALYSE THE BASIC KEY FOR EXAMPLE "KEY123"

STEP 2: USING THE SUBSTITUTION METHOD, CONVERT THE BASIC KEY INTO CIPHER TEXT.

STEP 3: CONVERT “KEY123” AS “{<•_•>}[<+>](•_•)&@%”

STEP 4: ENTER THE SUBSTITUTED VALUE AND CHECK WHETHER THE COMBINATIONS ARE MATCHED. IF THE COMBINATIONS ARE MATCHED, THE LOGIN IS SUCCESSFUL.

STEP 5: ELSE, IF THE COMBINATIONS DON’T MATCH LOGIN IS FAILED

STEP 6: REPEAT THE PROCESS UNTIL THE COMBINATIONS ARE MATCHED AND THE USER GETS LOGGED SUCCESSFULLY.

STEP 7: IF THE MATCH IS SUCCESSFUL IT WILL TAKE THE USER TO THE SECOND VERIFICATION.

Example Substitution Rule:
Example Plain Text: Key123
Substituted Cipher text: that specifies how each character {<•_•>}[<+>](•_•)&@%
would provide the key (e.g., "KEY123").

Substitution Check: The system would apply the same substitution rule to the provided key to transform it. Access is granted if the transformed key matches the predetermined key; otherwise, access is denied.

User Provides: "KEY123"

Substitution Check: "K" becomes "{<•_•>}" "E" becomes "[<+>]" "Y" becomes "(•_•)" and so on.

Transformed Key: “{<•_•>}[<+>](•_•)&@%”

Comparison: The system would compare the transformed key ("{<•_•>}[<+>](•_•)&@%") with the predetermined key ("KEY123"). If they match, the user is granted access.

4.9. Verification 2 (Security Using Steganography)

Steganography is derived from Johannes Trithemus's (1462-1516) finding entitled “Steganographia.” It comes from the Greek words (στεγανό-ς, γραφ-ειν) meaning “covered Steganography algorithms create covert communication channels and protect the confidentiality of messages embedded in cover images. A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message to be undetected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used with encryption to conceal or protect data. Watermarking algorithms embed invisible marks in images for further image authentication and proof of authorship. Avoid a process that involves hiding a message in an appropriate carrier, like an image or audio. It is of Greek origin and means "covered or hidden writing." The carrier can be sent to a receiver without anyone except the authenticated receiver knowing the existence of this information. For example, steganography could hide a message inside another file using encryption for extra security.

The recipient could then extract and decrypt the encrypted message using a given key. Cryptography and steganography are ways of securing data transfer over the Internet. Cryptography scrambles a message to conceal its contents; steganography conceals the existence of a message. It is not enough to simply encipher the traffic, as criminals detect and react to the presence of encrypted communications in steganography; the text to be concealed is called embedded data. A cover is an innocuous medium to hide embedded data, such as text, image, audio, or video files. The key (optional) used in the embedding process is called stego-key. A stego-key controls the hiding process to restrict the detection and/or recovery of embedded data to the parties who know it. This approach uses a pre-existing meaningful piece of English text as a cover file to hide the secret bits. The proposed encipher algorithm scrambles the message using a one-time secret key. The resulting cipher text is then hidden in the cover file by an embedding algorithm using a stego key.

Example:

Simple **E**ncrypt **C**orrect **R**eading **E**xactly **T**wice

Message Hidden: Secret

The proposed method involves the integration of hidden text within the structure of a coherent narrative. This narrative can consist of paragraphs, articles, or any textual content, making it particularly effective for online communications or publication on the web. The method draws inspiration from traditional literature, where meaningful information is cleverly embedded within the text, undetectable to an untrained eye.

Algorithm for Extracting Data from Stego Text

Begin

Input: Stego_Text, Secret_Key;

Examine Stego_Text;

Decode Secret_Key in Stego_Text;

Output: Secret_Message;

End

STEP 1: Analyse the Stego_text.

STEP 2: Extract the secret_key from stego_text.

STEP 3: Be precise about the output secret_key.

STEP 4: Invade the secret_key in the given login space.

STEP 5: The decrypted message cannot be viewed since there are only three login attempts after three failed login attempts.

5. Future Scope

The substitution method, a fundamental concept in cryptography, holds immense promise within the broader context of a project that integrates Multi-Factor Authentication (MFA), cryptographic algorithms, and steganography. This method, which involves replacing elements in a message with other elements, offers the project unique opportunities and significant scope. This extensive paragraph explores the potential applications, advantages, and key considerations for employing the substitution method in this comprehensive security framework. The scope of steganography within a project that integrates Multi-Factor Authentication (MFA), cryptographic algorithms, and steganography is extensive. It can potentially enhance data security, privacy, and confidentiality in various domains. This comprehensive paragraph explores the multifaceted scope of steganography within this project.

5.1. Enhanced Data Confidentiality

The substitution method provides an additional layer of security by systematically and reversibly replacing elements in a message with others. When integrated into our MFA, cryptographic, and steganographic framework, it ensures that the data remains unintelligible without the correct substitution keys even if Unauthorized access occurs. This enhances data confidentiality, particularly when sensitive information is transmitted or stored.

5.2. Robust Encryption

Substitution ciphers can serve as an effective tool for encrypting data within the project. By incorporating this method, we can transform plaintext information into Ciphertext using algorithms like the Caesar cipher or more advanced methods like the Vigenère cipher. This encryption is essential to the project's cryptographic component and contributes to the overall data protection strategy.

5.3. Integration with MFA

The substitution method aligns seamlessly with MFA's objective of requiring multiple authentication factors for access. In this context, it can encrypt and protect the user's authentication data, such as passwords or tokens. Integrating the substitution method ensures that others remain secure even if one authentication factor is compromised.

5.4. Steganography Enhancement

Substitution techniques can enhance the steganographic aspect of the project. By embedding secret data within seemingly innocuous data carriers (e.g., images or audio files) using substitution methods, we introduce a concealed layer of security. This ensures that even if steganographic content is intercepted, it remains cryptic to unauthorized parties.

5.5. Key Management

Managing the substitution keys is a crucial aspect of this method's implementation. Robust key management protocols and practices will be essential to ensure that keys remain secure and accessible only to authorized entities. The project can explore advanced key management techniques to enhance overall security.

5.6. Detecting Unauthorized Access

Steganography can serve as a mechanism to detect unauthorized access or tampering with data. By embedding markers or watermarks within data using steganographic methods, the project can verify the authenticity of the information and identify any alterations, ensuring data integrity.

5.7. Research and Advancements

The field of steganography is dynamic and continues to evolve. This project presents an opportunity to contribute to steganographic research and innovation by exploring novel techniques and methods. Advancements in steganography can further fortify data security and privacy.

6. Results and Discussions

This project enhanced data security by integrating MFA, cryptographic algorithms, and steganography. MFA improved user authentication, reducing vulnerabilities and maintaining a positive user experience. Cryptographic algorithms ensured robust data encryption and efficient decryption while emphasizing the importance of key management. Steganography facilitated covert data exchange, verified data integrity, and enhanced multimedia content protection. It also ensured compliance with data privacy regulations. Discussions highlighted the seamless integration of these components and emphasized future directions in advanced authentication, cryptographic advancements, innovative steganography techniques, and user education. In conclusion, this multifaceted approach significantly fortified data security and confidentiality. Enhanced security in this project is primarily achieved through integrating multiple security layers, including Multi-factor Authentication (MFA), cryptographic algorithms, and steganography. Here's how each component contributes to enhanced security

6.1. Multi-factor Authentication (MFA)

MFA significantly enhances security by requiring users to provide multiple authentication factors for access. This approach reduces the vulnerability to common attacks and unauthorized access. Users must provide "something they know," "something they have," and "something they are." MFA ensures that even if one authentication factor is compromised, the additional layers of security prevent unauthorized access.

6.2. Cryptographic Algorithms

Cryptographic algorithms, including symmetric and asymmetric encryption, are pivotal in securing data. They ensure data is encrypted before transmission and storage, making it unintelligible to unauthorized users. This encryption guarantees data confidentiality and integrity, protecting it from potential breaches or theft (Fig.6).

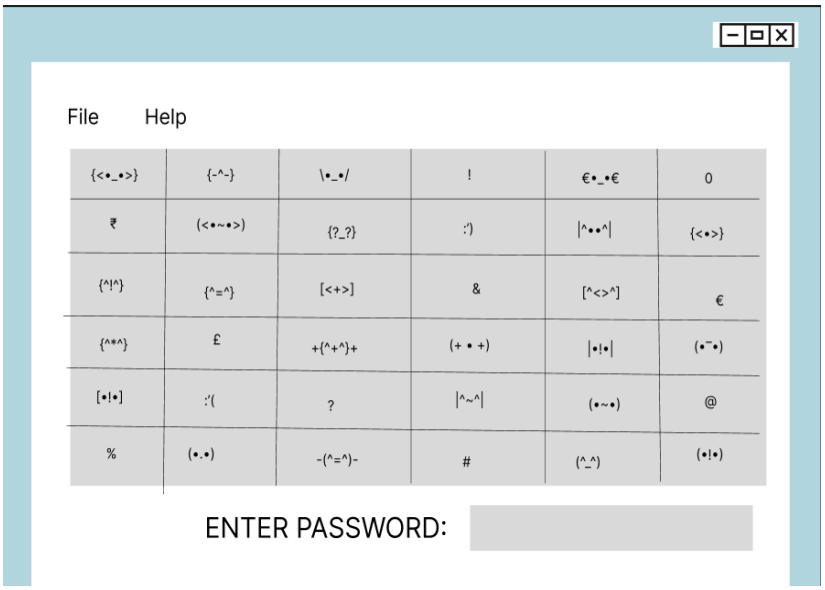

Figure 6: Entering the key using the substitution method

6. 3. Steganography

Steganography adds an extra layer of security by concealing information, such as images or audio files, within seemingly innocuous data carriers. This covert method enables the secure transmission of sensitive data without arousing suspicion.

Steganography contributes to data confidentiality and verifies data integrity by embedding markers or watermarks (Figs. 7 and 8).

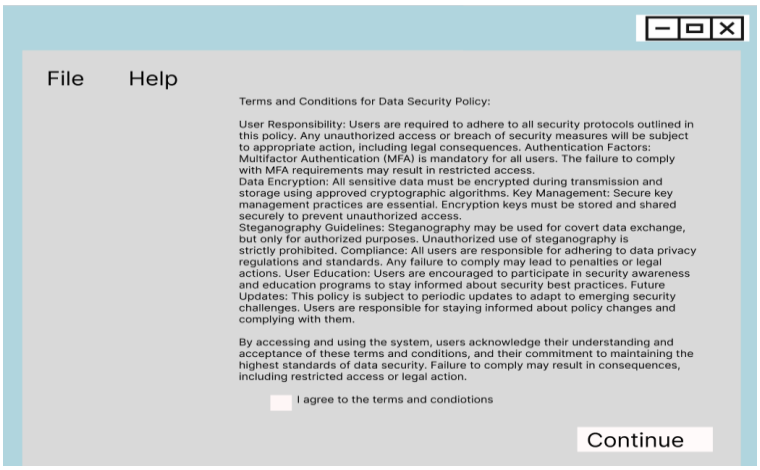

Figure 7: Identifying the hidden message for the text paragraph

Figure 8: Entering the secret message found in the text paragraph

The integrated security framework within the project ensures that even if one layer is breached, the other layers remain intact, significantly reducing the risk of unauthorized access, data breaches, or tampering. This comprehensive approach addresses vulnerabilities and enhances security in an interconnected, data-driven world. The discussions following the results underscored the successful integration of these components into a holistic and layered approach to security. The multifaceted framework significantly improved data protection and confidentiality by addressing vulnerabilities associated with single methods. The project's synergy between MFA, cryptographic algorithms, and steganography created a robust security infrastructure well-equipped to safeguard sensitive information. The project also recognized the importance of future research and development to evolve and adapt to emerging security challenges continuously, emphasizing advanced authentication factors, cryptographic enhancements, innovative steganography techniques, and user education. In conclusion, the project's multifaceted approach effectively enhances security by addressing vulnerabilities associated with individual methods, ensuring data confidentiality, and protecting sensitive information from unauthorized access or tampering.

7. Conclusion

In conclusion, the steganography project presents a compelling and multifaceted field of study and application. Steganography, with its capacity to conceal information within seemingly innocuous data, offers many benefits, including enhanced data security, privacy preservation, digital watermarking, and secure communication. Its potential extends to various sectors, from cybersecurity and digital forensics to content protection and authentication. However, the project also underscores the need for responsible and ethical use of steganography. Its misuse for illicit purposes, privacy concerns, and the evolving landscape of steganalysis present challenges that require careful consideration. Furthermore, steganography's legal and regulatory aspects require a comprehensive understanding of its implications in different jurisdictions. The future scope of projects involving steganography is promising, as data security, privacy, and authentication remain critical concerns in an increasingly digitized world. As technology advances, steganography will adapt and evolve, finding applications in emerging technologies and addressing new challenges, such as deepfakes and misinformation. In this context, ethical and legal compliance, user education, and a commitment to ethical use are pivotal to ensuring that steganography remains a valuable tool in information security and privacy protection. Through responsible implementation and continued research, steganography will fulfil its potential as

data protection. This project ensures that the correct person gets access to the data without being misused and enhances data privacy among organizations and the principles implemented in this project.

Acknowledgement: I am deeply grateful to my co-authors for their expertise and dedication, which greatly enriches this work. Special thanks to my friends for their unwavering support and encouragement throughout the research process.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding

Conflicts of Interest Statement: The authors have no conflicts of interest to declare. This work represents a new contribution by the authors, and all citations and references are appropriately included based on the information utilized.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants. Confidentiality measures were implemented to safeguard participant privacy.

References

1. F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, “A survey on multi-factor authentication for online banking in the wild,” Comput. Secur., vol. 95, no. 101745, p. 101745, 2020.
2. D. R. Ibrahim, J. S. Teh, and R. Abdullah, “Multi-factor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization,” Inf. Secur. J. Glob. Perspect., vol. 30, no. 3, pp. 149–159, 2021.
3. D. Wang, X. Zhang, Z. Zhang, and P. Wang, “Understanding security failures of multi-factor authentication schemes for multi-server environments,” Comput. Secur., vol. 88, no. 101619, p. 101619, 2020.
4. R. Ryu, S. Yeom, S.-H. Kim, and D. Herbert, “Continuous multimodal biometric authentication schemes: A systematic review,” IEEE Access, vol. 9, pp. 34541–34557, 2021.
5. S. Bezzateev, V. Davydov, and A. Ometov, “On secret sharing with Newton’s polynomial for multi-factor authentication,” Cryptography, vol. 4, no. 4, p. 34, 2020.
6. J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, “SMAKA: Secure many-to-many authentication and key agreement scheme for vehicular networks,” IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 1810–1824, 2021.
7. S. Mukherjee, S. Sarkar, and S. Mukhopadhyay, “An image steganography technique based on fake DNA sequence construction,” in Algorithms for Intelligent Systems, Singapore: Springer Nature Singapore, pp. 613–621,2022.
8. X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, “Color image compression and encryption scheme based on compressive sensing and double random encryption strategy,” Signal Processing, vol. 176, no. 107684, p. 107684, 2020.
9. Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, “Image encryption algorithm with circle index table scrambling and partition diffusion,” Nonlinear Dyn., vol. 103, no. 2, pp. 2043–2061, 2021.
10. Sectigostore.com. [Online]. Available: https://sectigostore.com/blog/wp-content/uploads/2020/12/hash-function-in-cryptography-1024x440.png. [Accessed: 09-Nov-2023].
11. Uakron.edu. [Online]. Available: https://www.uakron.edu/dA/5791b4aa-523b-47a5-a91f-bd179b250fc0/MFA.png. [Accessed: 09-Nov-2023].
12. A. Jain, K. K. Ramachandran, S. Sharma, T. Sharma, P. Pareek, and B. Pant, “Detailed investigation of influence of machine learning (ML) and big data on digital transformation in marketing,” in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022.
13. A. K. Bhardwaj, S. Rangineni, and D. Marupaka, “Assessment of Technical Information Quality using Machine Learning,” International Journal of Computer Trends and Technology, vol. 71, no. 9, pp. 33–40, 2023.
14. A. Mittal, K. K. Ramachandran, K. K. Lakshmi, N. N. Hasbullah, M. Ravichand, and M. Lourens, “Human-cantered Artificial Intelligence in Education, present and future opportunities,” in 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.
15. A. Sarwar Zamani et al., “Cloud Network Design and Requirements for the Virtualization System for IoT Networks”,” IJCSNS International Journal of Computer Science and Network Security, vol. 22, no. 11, 2022.
16. A. Shameem, K. K. Ramachandran, A. Sharma, R. Singh, F. J. Selvaraj, and G. Manoharan, “The rising importance of AI in boosting the efficiency of online advertising in developing countries,” in 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.
17. Amit Bhanushali, "Challenges and Solutions in Implementing Continuous Integration and Continuous Testing for Agile Quality Assurance,” International Journal of Science and Research (IJSR), Vol. 12, no.10, pp. 1626-1644, 2023.

18. B. Nagarjuna, K. K. Ramachandran, A. Nautiyal, S. P. Singh, B. B. Nayak, and P. Ganguly, “Sustainability in the field of Supply Chain Using Technolgy: A deep review,” in 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.
19. C. H. Patel, D. Undaviya, H. Dave, S. Degadwala, and D. Vyas, “EfficientNetB0 for brain stroke classification on computed tomography scan,” in 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2023.
20. D. D. Pandya, A. Jadeja, S. Degadwala, and D. Vyas, “Diagnostic Criteria for Depression based on Both Static and Dynamic Visual Features,” in 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 635–639,2023.
21. D. D. Pandya, A. K. Patel, J. M. Purohit, M. N. Bhuptani, S. Degadwala, and D. Vyas, “Forecasting number of Indian startups using supervised learning regression models,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023.
22. D. D. Pandya, S. K. Patel, A. H. Qureshi, A. J. Goswami, S. Degadwala, and D. Vyas, “Multi-class classification of vector borne diseases using convolution neural network,” in 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2023.
23. D. Marupaka, S. Rangineni, and A. K. Bhardwaj, “Data Pipeline Engineering in The Insurance Industry: A Critical Analysis Of Etl Frameworks, Integration Strategies, And Scalability,” International Journal Of Creative Research Thoughts, vol. 11, no. 6, pp. 530–539, 2023.
24. D. Rathod, K. Patel, A. J. Goswami, S. Degadwala, and D. Vyas, “Exploring drug sentiment analysis with machine learning techniques,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023.
25. D. Vyas and V. V. Kapadia, “Evaluation of adversarial attacks and detection on transfer learning model,” in 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), 2023.
26. F. A. Khan, A. Abubakar, M. Mahmoud, M. A. Al-Khasawneh, and A. A. Alarood, “BSCL: blockchain-oriented SDN controlled cloud based Li-fi communication architecture for smart city network,” International Journal of Engineering & Technology, vol. 7, pp. 10–14419, 2018.
27. F. Ahamad, D. K. Lobiyal, S. Degadwala, and D. Vyas, “Inspecting and finding faults in railway tracks using wireless sensor networks,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023.
28. G. Saravana Kumar, K. K. Ramachandran, S. Sharma, R. Ramesh, K. Qureshi, and K. V. B. Ganesh, “AI-assisted resource allocation for improved business efficiency and profitability,” in 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.
29. H. Lakhani, D. Undaviya, H. Dave, S. Degadwala, and D. Vyas, “PET-MRI sequence fusion using convolution neural network,” in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023.
30. I. Ahmad, S. A. Ali Shah, and M. Ahmad Al-Khasawneh, “Performance analysis of intrusion detection systems for smartphone security enhancements,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021.
31. I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile Hospitalization,” Int. J. Comput. Appl., vol. 80, no. 13, pp. 18–23, 2013.
32. I. M. Alfadli, F. M. Ghabban, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, “CIPM: Common identification process model for database forensics field,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021.
33. K. K. Ramachandran, K. K. Lakshmi, J. Singh, A. Prusty, J. Panduro-Ramirez, and M. Lourens, The impact of the metaverse on organizational culture and communication. 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2023.
34. K. K. Ramachandran, K. K., K. Singh, Ramesh, C. Ganesh, and S. Kumar, “Machine learning approaches for statistical analysis of customer satisfaction in service management,” in 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.
35. Kaushikkumar Patel “A Review on Enhancing Data Quality for Optimal Data Analytics Performance,” International Journal of Computer Sciences and Engineering, vol. 11, no. 10, pp. 51–58, 2023.
36. Kulbir, Singh, "Artificial Intelligence & Cloud in Healthcare: Analyzing Challenges and Solutions Within Regulatory Boundaries," SSRG International Journal of Computer Science and Engineering, vol. 10, no. 9, pp. 1-9, 2023.
37. L. T. Reddi, “Transforming Management Accounting: Analyzing The Impacts Of Integrated Sap Implementation,” International Research Journal of Modernization in Engineering Technology and Science, vol. 5, no. 8, pp. 1786–1793, 2023.
38. L. Thammareddi, M. Kuppam, K. Patel, D. Marupaka, and A. Bhanushali, “An extensive examination of the DevOps pipelines and insightful exploration,” International Journal of Computer Engineering and Technology, vol. 14, no. 3, pp. 76–90, 2023.
39. M. Akbar, I. Ahmad, M. Mirza, M. Ali, and P. Barmavatu, “Enhanced authentication for de-duplication of big data on cloud storage system using machine learning approach,” Cluster Comput., 2023.

40. M. D. M. Akhtar, A. S. A. Shatat, S. A. H. Ahamad, S. Dilshad, and F. Samdani, Eds., "Optimized cascaded CNN for intelligent rainfall prediction model: a research towards Statistic based machine learning," Theoretical Issues in Ergonomics Science, vol. 24, no. 5, pp. 564–2022.
41. M. D. M. Akhtar, R. S. Ali, A. S. A. Shatat, and S. A. Hameed, Eds., IoMT-based smart healthcare monitoring system using adaptive wavelet entropy deep feature fusion and improved RNN", Multimedia Tools and Applications. Springer Nature, 2022.
42. M. Farooq, "Artificial Intelligence-Based Approach on Cybersecurity Challenges and Opportunities in The Internet of Things & Edge Computing Devices," International Journal of Engineering and Computer Science, vol. 12, no. 07, pp. 25763–25768, Jul. 2023, doi: https://doi.org/10.18535/ijecs/v12i07.4744.
43. M. M. Abbassy and A. Abo-Alnadr, "Rule-based emotion AI in Arabic customer review," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 9, 2019.
44. M. Md et al., "Stock market prediction based on statistical data using machine learning algorithms"," Journal of King Saud University - Science, vol. 34, no. 2, 2022.
45. M. Sabugaa, B. Senapati, Y. Kupriyanov, Y. Danilova, S. Irgasheva, and E. Potekhina, "Evaluation of the prognostic significance and accuracy of screening tests for alcohol dependence based on the results of building a multilayer perceptron," in Artificial Intelligence Application in Networks and Systems, Cham: Springer International Publishing, pp. 240–245, 2023.
46. M. Suryadevera, S. Rangineni, and S. Venkata, "Optimizing Efficiency and Performance: Investigating Data Pipelines for Artificial Intelligence Model Development and Practical Applications," International Journal of Science and Research, vol. 12, no. 7, pp. 1330–1340, 2023.
47. N. C. Sattaru, D. Umrao, K. K. Ramachandran, K. K. Karthick, M. Tiwari, and S. Kumar, "Machine learning as a predictive technology and its impact on digital pricing and cryptocurrency markets," in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022.
48. R. A. Sadek, D. M. Abd-alazeem, and M. M. Abbassy, "A new energy-efficient multi-hop routing protocol for heterogeneous wireless sensor networks," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 11, 2021.
49. R. Raman, K. Joshi, G. Saravana Kumar, K. K. Ramachandran, S. Bothe, and S. Trivedi, "Benefits of implementing an ad-hoc network for hospitality businesses with IOT smart devices," in 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.
50. S. A. A. Shah, M. A. Al-Khasawneh, and M. I. Uddin, "Review of weapon detection techniques within the scope of street-crimes," in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE, 2021, pp. 26–37,2021.
51. S. A. A. Shah, M. A. Al-Khasawneh, and M. I. Uddin, "Street-crimes Modelled Arms Recognition Technique (SMART): Using VGG," in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE, pp. 38–44, 2021.
52. S. Chahal, "Unlocking Educational Excellence: A Digital Transformation Approach through Business Process Optimization and the Role of Agile Project Management to Overcome Barriers to Successful Transformation," Journal of Economics & Management Research, vol. 193, no. 4, pp. 2–5, 2023.
53. S. Degadwala, D. Vyas, D. D. Pandya, and H. Dave, "Multi-class pneumonia classification using transfer deep learning methods," in 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2023.
54. S. Köseoğlu, W. M. Ead, and M. M. Abbassy, "Basics of Financial Data Analytics," Financial Data Analytics, pp. 23–57, 2022.
55. S. Parate, L. ThammaReddi, S. Agarwal, and M. Suryadevara, "Analyzing the Impact of Open Data Ecosystems and Standardized Interfaces on Product Development and Innovation," International Journal of Advanced Research in Science, Communication and Technology, vol. 3, no. 1, pp. 476–485, 2023.
56. S. Rangineni, A. Bhanushali, M. Suryadevara, S. Venkata, and K. Peddireddy, "A Review on Enhancing Data Quality for Optimal Data Analytics Performance," International Journal of Computer Sciences and Engineering, vol. 11, no. 10, pp. 51–58, 2023.
57. S. Rangineni, A. K. Bhardwaj, and D. Marupaka, "An Overview and Critical Analysis of Recent Advances in Challenges Faced in Building Data Engineering Pipelines for Streaming Media," The Review of Contemporary Scientific and Academic Studies, vol. 3, no. 6, 2023.
58. Shashank, Agarwal, Siddharth Sharma, Sachin Parate "Exploring the Untapped Potential of Synthetic data: A Comprehensive Review," International Journal of Computer Trends and Technology, vol. 71, no. 6, pp. 86-90, 2023.
59. V. Desai, S. Degadwala, and D. Vyas, "Multi-categories vehicle detection for urban traffic management," in 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), 2023.
60. W. Ead and M. Abbassy, "Intelligent systems of machine learning approaches for developing E-services portals," EAI Endorsed Trans. Energy Web, p. 167292, 2018.
61. Y. F. Saputra and M. A. Al-Khasawneh, "Big data analytics: Schizophrenia prediction on Apache spark," in Communications in Computer and Information Science, Singapore: Springer Singapore, pp. 508–522, 2021.