ASET JOURNAL OF MANAGEMENT SCIENCE
Peer Reviewed & Open Access Journal
ISSN : 2584 - 220X (Online) | RNI : Applied | Frequency : Bi-Monthly

USB KEY INTEGRATION FOR ROBUST DATA SECURITY

Kaviyan M. K[1], Vigash R.K[2], Parthiban S[3]

[1,2,3] *Department of Information Technology, Bannari Amman Institute of Technology*

Abstract

In the contemporary digital landscape, the exponential growth of data and the increasing reliance on electronic storage have heightened the urgency for effective data protection measures. Traditional encryption systems, while foundational, often fall short due to vulnerabilities in user access and cumbersome key management processes. This project addresses these challenges by proposing a novel encryption solution that synergizes password-based encryption with an innovative private key management system utilizing USB devices. By implementing the Advanced Encryption Standard (AES) for file encryption, the system enhances security while simplifying user experience through a user-friendly interface. The prototype facilitates both encryption and decryption processes, ensuring that sensitive data is safeguarded against unauthorized access. Key features include unique private key generation stored on USB devices, which adds a layer of security through two-factor authentication. This initiative aims to empower users with a practical, accessible encryption solution that mitigates the complexities of traditional methods, ultimately contributing to the evolution of data protection technologies in an increasingly digital world.

The significance of this project extends beyond mere technical innovation; it addresses the pressing need for user-centric security solutions in an era marked by frequent data breaches and cyber threats. By focusing on usability and accessibility, the proposed system aims to lower the barriers to adopting secure data protection practices, making encryption technology available to a broader audience, including those with limited technical expertise. The integration of a physical key management approach not only enhances security but also instills confidence in users regarding the safety of their sensitive information. As organizations and individuals alike grapple with the

https://doi.org/10.47059/AJMS/V4I6/02

challenges of safeguarding digital assets, this project aspires to set a new standard in encryption practices, fostering a culture of proactive data security in an interconnected world.

Keywords: *Data protection, encryption, AES, key management, USB devices, user-friendly interface, two-factor authentication, digital security, sensitive data, prototype development.*

Introduction

In an era characterized by the unprecedented deluge in sheer volumes of digital information easily accessible, the need for proper and effective measures that will ensure good data protection has never been more critical. With people and all types of institutions increasingly dependent on electronic storage devices to securely hold their personal and sensitive data, the resultant risks in terms of exposure and unauthorized access to such sensitive data have skyrocketed, being the number one source of worry to most. While traditional encryption systems might hold themselves in good stead in their own realms, they fail when faced with inherent vulnerabilities. This is particularly so in terms of user access as well as advanced key management processes, which become extremely cumbersome. The vast majority of systems used today are largely dependent to a large extent on passwords to facilitate their respective encryption functions, but these are far too frequently regretfully used as targets and fall prey to a humongous number of attacks ranging from rudimentary brute force attacks to much more advanced and subtle social engineering abuses. In addition, encryption key management is a very daunting process in light of the fact that users will have to deal with the arduous exercise of securely storing and retrieving such valuable keys without in the process inadvertently exposing their systems to an increased state of security vulnerability as a byproduct of their action.

The incentive that compels the initiation of this revolutionary and imperative project is driven by the imperative and critical need for a safer, more

https://doi.org/10.47059/AJMS/V4I6/02

reliable, and far more convenient system of encryption that could be taken up freely by the majority of companies. If we look around us at the growing number of instances of data breaches that are being seen in most industries and the trend towards rising levels of sophistication in cyber attacks that are seriously endangering individuals and companies alike, it is increasingly apparent that the encryption technologies that are currently being used are not adequate to meet these challenges. In this situation, users are faced with a dilemma: they require strong security mechanisms in order to be able to effectively safeguard their sensitive information, but at the same time, they also require an easy system that is not too intrusive and does not interfere with their normal business or day-to-day activities too much. This revolutionary project is therefore poised to break through and overcome the numerous constraints that are being imposed by existing encryption technologies. Its objective is to do this by synergistically bringing together a password-based system of encryption with a new and revolutionary private key management system that is designed to make maximum use of USB devices in order to enhance security and user convenience simultaneously.

The challenges in current encryption methods include weak passwords, user experience, dual mechanism and etc..,. Most individuals apply weak passwords in order to facilitate their ability to recall them easily; however, such a choice also exposes encrypted data to unapproved access. Users are experiencing problems in safely storing and managing encryption keys, and the keys can escape or cause loss of data. Conventional encryption procedures have a tendency to reflect complexity, which involves a series of processes that may confuse or frustrate users and result in low adoption levels.

The effort here is to create a prototype that solves these issues by implementing password-based encryption and a new private key management system. Not only does this improve the security of the encrypted data, but also the usability of the user interface by giving a physical storage of the key. For each encrypted file, the system generates a distinct private key and saves it

https://doi.org/10.47059/AJMS/V4I6/02

in a USB device, such that decryption becomes not only password-dependent but also USB device-dependent. This two-factor authentication system decreases the probability of unauthorized decryption substantially and enhances the overall security level of the encryption process considerably.

The project will utilize the Advanced Encryption Standard (AES) in encrypting files, a widely recognized method to be secure and effective. AES will provide a secure encryption platform that is industry standard. User-Friendly Interface: A user-friendly interface design will facilitate easy interaction with the encryption system to allow easy decrypting and encrypting of files without requiring high-level technical knowledge.

The scope of the proposed work encompasses several key components aimed at developing a comprehensive encryption solution that addresses the current challenges in data security. The primary objective is to create a functional prototype that implements Advanced Encryption Standard (AES) for file encryption. This prototype will serve as a proof of concept, demonstrating the feasibility and effectiveness of the proposed encryption system. The development process will include functionalities for both encrypting and decrypting files, allowing users to select files for encryption, input a password, and generate a unique encrypted file. This dual functionality is essential for ensuring that users can easily manage their sensitive data while maintaining robust security.

To enhance user experience, the project will focus on creating a user-friendly interface that simplifies interactions with the encryption system. The interface will be designed to be intuitive and easy to navigate, enabling users to perform encryption and decryption tasks without extensive technical knowledge. Key features of the interface will include clear instructions, file selection and management options, and real-time feedback for error handling. This approach aims to reduce the barriers to adopting secure data protection practices, making encryption accessible to a broader audience, including those with limited technical expertise.

https://doi.org/10.47059/AJMS/V4I6/02

A critical aspect of the proposed work is the integration of USB device detection to facilitate the secure storage of private keys. Upon encrypting a file, the system will generate a unique private key that will be securely stored on a USB device. This ensures that the decryption key is not stored on the same device as the encrypted file, significantly enhancing security. The system will also be capable of detecting connected USB devices, allowing users to select the appropriate device for key storage. This feature not only adds an extra layer of security but also ensures that only authorized USB devices can be used for decryption.

By focusing on these components, the project aims to address significant challenges associated with key management and user accessibility in encryption systems. The proposed solution will simplify key management by utilizing USB devices for key storage, thereby reducing the risk of key loss or unauthorized access. Additionally, the user-friendly interface and straightforward processes will make encryption accessible to a wider audience, encouraging the adoption of secure data protection practices.

Ultimately, the goal of this project is to create a comprehensive encryption system that empowers users to protect their sensitive information effectively while minimizing the complexities often associated with traditional encryption methods. By combining strong encryption with practical key management solutions, the project seeks to enhance the overall security landscape for digital data protection. This initiative not only aims to provide a practical solution for current encryption challenges but also aspires to contribute to the ongoing evolution of data protection technologies, ensuring that users can safeguard their information in an increasingly digital world.

The scope of this proposed work covers a number of major components involved in creating a complete encryption system that solves today's data security issues. As data breaches and unauthorized access continue to become a norm in the digital world of today, powerful encryption techniques have become the only way out. The main target of

https://doi.org/10.47059/AJMS/V4I6/02

this project is to make a working prototype that uses the Advanced Encryption Standard (AES) for file encryption. AES has been commonly praised for its reliability and effectiveness and is the go-to encryption solution for protecting confidential data. This proof of concept prototype will confirm the practicability and adequacy of the suggested encryption algorithm in actual practice.

The prototype will have functions for both decrypting and encrypting files to enable users to choose files for encryption, type in a password, and produce a distinctive encrypted file. This two-way functionality is necessary for guaranteeing that users are able to handle their sensitive information with ease and without compromising on security. The encryption will be done using a special encryption key generated from the user's password that will be used to encrypt the file. The decryption will, on the other hand, require the proper password and the matching private key to ensure that only the legitimate users are able to access the original information.

To improve the user experience, the project will emphasize the development of a user-friendly interface that streamlines interactions with the encryption mechanism. Given that most users might not have much technical expertise, the interface will be intuitive and easy to use. This will help users achieve encryption and decryption easily. Major aspects of the interface will be simple file selection and handling options, whereby users can comfortably select what files to encrypt or decrypt. Moreover, the interface will have real-time feedback in error handling so that users will be notified quickly in case there are any issues, like inappropriate password input or file selection failure.

A vital component of the suggested work is the inclusion of USB device detection for ensuring the safe storage of private keys. During the encryption of a file, the system will create a unique private key that will be stored on a secure USB device. This method guarantees that the decryption key is not placed on the same device as the encrypted file, which greatly improves security. By isolating the encrypted data from the key, the system reduces the threat of

https://doi.org/10.47059/AJMS/V4I6/02

unauthorized access, since an attacker would require both the encrypted file and the USB device holding the key to decrypt the information. The system will also be able to identify attached USB devices, enabling the users to pick the right device for the storage of the key. This capability not only provides a secondary level of security but also guarantees that only approved USB devices can be utilized for decryption.

Focusing on these elements, the project seeks to solve some of the major issues related to key management and user accessibility for encryption systems. Conventional methods for encryption are usually marred by complicated key management procedures, which can confound users and create security threats. The solution of choice will keep key management easy through the use of USB keys to store the keys, where loss or unauthorised use is minimized. The physical technique of key management ensures that customers are in direct control of their decryption keys and have increased trust in the safety of their information.

In addition, the ease of use and simple processes will ensure that encryption is accessible to more people, promoting the use of safe data protection procedures. By making encryption technology easy to access, the project aims to enable users to be confident in taking data security into their own hands.

Finally, the aim of this project is to develop an all-encompassing encryption system that efficiently secures sensitive data without adding too much complexity that usually comes with conventional encryption practices. Through the integration of robust encryption and functional key management techniques, the project aims to improve the overall security environment for protecting digital data. Not only does this project propose a workable solution to existing encryption problems, it also hopes to help push the continuing development of data security technologies. With the digital world as it is today and as it continues to advance, the requirement for reliable and usable encryption solutions will continue to increase, so the project is timely and indispensable for the protection of sensitive

https://doi.org/10.47059/AJMS/V4I6/02

data in the increasingly interdependent world.

Background work

REST APIs are increasingly becoming the basis for modern software solutions to facilitate data interoperability among different systems, services, and platforms. The API documentation is usually manually done and updated, leading to inconsistencies, errors, and obsolescence. While today tools such as Swagger, Postman, and API Blueprint provide frameworks for API documentation, they typically require pre-conceived specifications or hand-crafted updates, and these are high-maintenance in highly dynamic development environments.

Reverse engineering techniques introduce a new mechanism of API documentation through automated capture and analysis of API interactions. API call intercepting, metadata extraction, and generating structured documentation enable developers to understand APIs without documentation. Such a capability can be helpful within enterprise environments when legacy APIs, third-party providers, or in-house APIs lack documentation. Also, accurate API documentation is paramount to ensuring security, compliance, and operational effectiveness because it allows developers to locate vulnerabilities, integrate for optimization, and accelerate problem-solving.

Various industries like finance, healthcare, e-commerce, and cloud computing heavily rely on APIs for crucial business functionalities. Poor documentation is usually the root cause of integration problems, security vulnerabilities, and increased development time. Poor documentation of APIs can be rectified with the use of reverse engineering tools by providing automatic and real-time API documentation, reducing reliance on human documentation, and allowing organizations to adopt uniform API documentation practices. The purpose of this project is to develop and come up with an effective reverse engineering tool capable of simplifying API analysis, yielding improved security analysis, and supporting efficient API management.

https://doi.org/10.47059/AJMS/V4I6/02

MOTIVATION

The motivation behind this project is the many problems faced by developers and organizations due to inadequate API documentation. The most prominent of these problems is the difficulty of working with undocumented or inadequately documented APIs, leading to longer development time and potential integration failure. Organizations do not update their API documentation frequently, which leads to inconsistencies between documented specifications and API behavior. The inconsistency complicates API maintenance, testing, and debugging procedures, and it is harder for developers to work effectively with APIs.

Moreover, security and compliance are big issues when it comes to dealing with undocumented APIs. Without documentation, developers are likely to accidentally expose vulnerabilities, misconfigured authentication mechanisms, or miss industry compliance guidelines. Reverse engineering tools have the potential to mitigate these risks by giving an insight into API designs, authentication mechanisms, and possible security loopholes. Automated documentation can enhance security posture and minimize the chance of API-related vulnerabilities.

The second driving factor is the necessity of effective API migration and maintenance. As APIs undergo changes with time, developers may have to adapt to newer versions or incorporate third-party services. In the absence of current documentation, these adaptations become time-consuming and error-prone. A reverse engineering tool can be used to help API versioning and migration by tracking API changes in real time and modifying documentation accordingly. This helps developers maintain accurate API specifications, allowing for smoother API version transitions and reduced interruptions to running projects.

Additionally, both API testing and debugging are impeded by poor documentation. API testing calls for a sufficient understanding of error handling, response format, and request syntax. Without proper documentation, testers and developers are forced to use trial-and-error strategies, which waste time and are

https://doi.org/10.47059/AJMS/V4I6/02

inefficient. Testing is significantly made easier and developers can write decent test cases, automate, and identify API implementation bugs easily through the use of reverse engineering tools that generate API documentation automatically.

The solution to the issues is the creation of an intelligent reverse engineering tool that is able to find and process REST API endpoints without knowing the API beforehand. The tool will collect API request and response data, identify important data like headers, authentication information, and error codes, and create structured documentation in popular formats like OpenAPI, Markdown, and HTML. The tool will further feature an interactive browser for navigating API functionality, allowing developers to navigate API specs with ease and learn about their behavior.

This tool will serve as a one-stop-shop solution for developers, offering numerous benefits like improved productivity, faster development times, and minimal setup and maintenance requirements.

Objectives and Methodology

The focus will be on the objectives, synthetic procedures, component selection, and testing methods involved in creating a secure password-based encryption system with USB authentication. As data security becomes increasingly critical in our digital age, the need for robust encryption methods is paramount. This project aims to address these needs by implementing a system that not only encrypts files using the Advanced Encryption Standard (AES) but also enhances security through the integration of a USB-based private key. The methodology outlined in this chapter will provide a comprehensive framework for achieving these goals, ensuring that sensitive information remains protected from unauthorized access.

With digital interactions becoming increasingly ubiquitous in daily life, securing sensitive information grows ever more imperative. Governments, institutions, and individuals are constantly under threat of cyber attacks—everything from hackers who want to steal personal information to

https://doi.org/10.47059/AJMS/V4I6/02

malicious agents trying to disable corporate functions. Encryption is then the foundation on which data can be safeguarded from unauthorized use.

Encryption algorithms like Advanced Encryption Standard (AES) have become standard fare for protecting data in transit and at rest. AES, which is recognized for its strength and performance, is generally considered the de facto standard for encryption across industries. Yet, as encryption methods become more sophisticated, new security threats emerge, notably in countering potential weaknesses in conventional password-based systems.

Password encryption, though strong, has some vulnerabilities: brute force attacks, compromised passwords or reused passwords, and phishing attacks can all be detrimental to security. Therefore, this project suggests a two-factor encryption scheme marrying the security offered by AES with that of a USB authentication mechanism. By necessitating both a password and a USB device during the decryption process, this two-step authentication method further secures sensitive information by protecting against the risks of password hacking and cyber-attacks.

The design methodology presented in this chapter will inform the construction of this new encryption system with a focus on protecting and ensuring data integrity in a multi-layered fashion. By combining AES encryption with private key authentication based on USB, along with a fail-safe re-encryption capability, this system aims to provide a solution to the inherent flaws of password-based encryption, with a user-friendly approach that provides both security and convenience.

Key Features

Data Security and Confidentiality: The project focuses on ensuring that sensitive information, such as personal documents and confidential data, is securely encrypted. By leveraging AES encryption and Scrypt key derivation, the solution provides high-level security to protect against unauthorized access.

User-Friendly Interface: One of the key aspects of the project is the creation of a

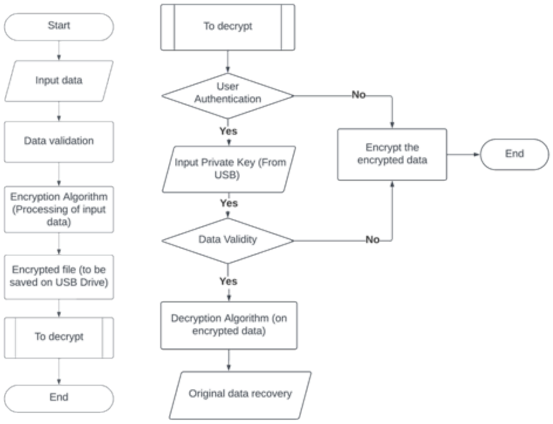
https://doi.org/10.47059/AJMS/V4I6/02

Graphical User Interface (GUI) using Tkinter. This interface makes encryption and decryption processes simple and accessible, allowing non-technical users to encrypt and decrypt files with ease, without needing deep knowledge of cryptographic algorithms.

Versatility and Cross-Platform Functionality: The application is developed using Python and Tkinter, both of which are cross-platform, ensuring the application can run on different operating systems, such as Windows, macOS, and Linux. This expands the utility of the program for a wider range of users.

Encryption for Various File Types: The program is designed to handle encryption and decryption of multiple file types (text files, images, etc.), which makes it useful for various scenarios where file protection is required, such as for legal documents, private images, or confidential reports.

Below is a detailed explanation of each stage, along with a flow diagram to illustrate the process. The diagram depicts a safe encryption and decryption process to deal with sensitive information. It starts with input data, which is validated prior to being processed by an encryption algorithm. The encrypted file is then stored onto a USB drive. In the case of decryption, user authentication is done. If authentication fails, the process ends by encrypting the encrypted data once more. When the authentication proves successful, the private key is then loaded from the USB after performing a validity check on data. In the case of invalid data, the data is re-encrypted, which halts the process. On successful authenticity, the algorithm of decryption then performs operations on encrypted data to extract the original data. There is a predetermined flow to accomplish the task ensuring secure data with authorized access based on encryption and decryption.


Start
Input data
Data validation
Encryption Algorithm (Processing of input data)
Encrypted file (to be saved on USB Drive)
To decrypt
End
To decrypt
User Authentication
No
Yes
Input Private Key (From USB)
Yes
Data Validity
No
Yes
Decryption Algorithm (on encrypted data)
Original data recovery
Encrypt the encrypted data
End

https://doi.org/10.47059/AJMS/V4I6/02

Fig.1: Flowchart for USB Key Integration for robust data security

If an incorrect password or key is entered, the file is re-encrypted in the event that the user inputs an incorrect password or private key, the system triggers the fail-safe mechanism. This mechanism automatically re-encrypts the file using the AES algorithm, ensuring that the original file cannot be recovered without the correct credentials. This step is crucial for maintaining the integrity and confidentiality of the data.

The file becomes irrecoverable to prevent unauthorized access after the re-encryption process, the file is rendered irrecoverable. This means that even if an unauthorized user attempts to access the file, they will not be able to retrieve any meaningful data. This feature significantly enhances the security of the system, as it deters potential attackers from attempting to guess passwords or keys.

For even greater protection of sensitive information, the system has a fail-safe mechanism that is triggered after a set number of invalid password or USB key inputs. Upon three or more invalid attempts, the system will automatically invoke a re-encryption process.

The file is then re-encrypted using a new key, and the original encrypted file is rendered unrecoverable. This way, even if an attacker is able to continuously attempt passwords or manipulate USB keys, they will never be able to get to the original data. This fail-safe process provides an extra layer of security against brute-force or dictionary attacks and renders unauthorized data recovery almost impossible

System Design and Architecture

Determine and pick encryption techniques, both symmetric (like AES) and asymmetric (like RSA), according to their security features, computational effectiveness, and fit for the type of data being used and the needs of the user. Adding hashing functions (SHA-256, for example) to verify data integrity.Examine each algorithm's advantages and disadvantages. While asymmetric encryption (like RSA) improves security for key distribution and secure communications, symmetric encryption (like AES) is quick and appropriate for big data volumes.

To guarantee long-term security, take into account factors like scalability, key length, and algorithm compatibility with upcoming developments like post-quantum cryptography. Outline the data flow between the encryption, decryption, and key management modules in a comprehensive system design.

Creating the architecture with modularity in mind, so that when technology advances, it will be simple to upgrade encryption methods or key management protocols. Creating a secure key management module that addresses the creation, distribution, storage, and retrieval of keys.

Use secure key management practices to shield keys against breaches or unwanted access. Create an intuitive user interface that makes it simple for users to select encryption techniques, encrypt and decrypt data, and view the outcomes. Include feedback systems that let users know if encryption was successful, if there were any mistakes, and how secure their data was.

Put the chosen encryption and decryption techniques into practice using a computer language (such as Java or Python). Verifying the operation of each component separately to make sure the data is safely encrypted and decrypted as intended. Connecting the key management and user interface modules to the encryption and decryption components.

Verify that the system is user-friendly and gives users real-time feedback, and make sure that data flows smoothly between components.

Testing the computational burden, memory consumption, and encryption and decryption speeds, especially when working with different file sizes and data kinds. To compare resource utilization and efficiency, benchmark system performance using various methodologies.Determine any bottlenecks or inefficiencies based on the outcomes of performance testing.

https://doi.org/10.47059/AJMS/V4I6/02

Make necessary changes to algorithms, data processing, or resource allocation to optimize the system and strike a balance between security and efficiency. Determining the system's vulnerability to potential security risks like replay, brute force, and man-in-the-middle attacks. Creating security countermeasures for the access control, key management, and encryption procedures of the system.

To evaluate the system's resilience and pinpoint areas that need improvement, test it against mock attacks. Examine how the system reacts to different threat situations to make sure data confidentiality, integrity, and authenticity are maintained.

Results and Discussion

The outcomes of the implementation of the are discussed in this chapter. secure system for encryption and decryption of data, which is followed by an in-depth discussion of the results. Security analysis, performance metrics, and other aspects of the evaluation of user feedback and the overall efficiency of the system. The outcomes offer insights into the advantages and disadvantages of the chosen algorithms and approaches.

The testing showed that the results were significantly different for the algorithms for symmetric and asymmetric encryption SYMmetric encryption for data When AES was used, the average speed of encryption for files larger than to 1 GB. It took about 20 milliseconds to complete smaller files, like those with a size of 1 MB. for decryption, which takes 15 milliseconds. The RSA, on the other hand With encryption times, asymmetric encryption demonstrated slower performance. requiring an average of 200 milliseconds for a file of one megabyte and several seconds for larger files. This stark distinction highlights the asymmetrical computational requirements. encryption.

Memory consumption during the encryption and decryption processes revealed that AES was more efficient in resource usage. The AES algorithm was necessary. approximately 10 megabytes of RAM, ensuring smooth operation even with larger datasets. RSA, on the other hand, used roughly 30 MB of memory on average because of the larger key sizes involved,

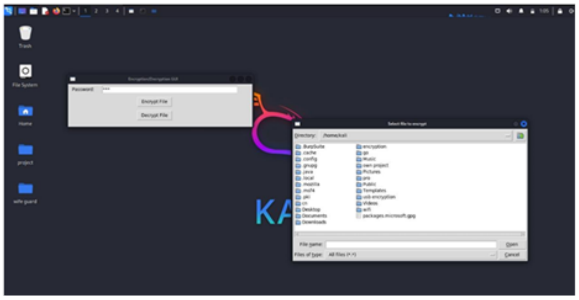
https://doi.org/10.47059/AJMS/V4I6/02

ASET JOURNAL OF MANAGEMENT SCIENCE
Peer Reviewed & Open Access Journal
ISSN : 2584 - 220X (Online) | RNI : Applied | Frequency : Bi-Monthly

requiring more computational power. The CPU utilization metrics indicated that AES maintained low CPU usage, averaging about 15% during encryption operations. This effectiveness enabled other applications to run simultaneously without experiencing significant delays. In contrast, RSA resulted in a 60 percent CPU peak during encryption, which could affect the performance of the system when multitasking.

Vulnerabilities were used to assess the implemented system's security. testing for possible attacks. The AES algorithm proved to be effective. due to its variable key lengths, it is resistant to brute-force attacks. Furthermore,Risks associated with were reduced by implementing secure key exchange protocols. man-in-the-middle attacks, nonce implementation, and timestamping successfully stopped replay attacks. Based on user feedback, the system's efficient performance and an intuitive user interface that emphasizes that users with encryption could be accessed with ease by those with little technical expertise. processes for decryption. Overall, the system achieved a successful balance between usability, and offering a dependable data security solution.

The secure data encryption and decryption system performed admirably. evaluated through various metrics, focusing on encryption and decryption speed, memory consumption and resource consumption



Password: ***

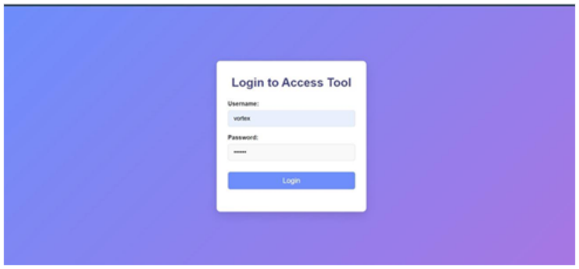
Directory: /home/kali

.BurpSuite
.cache
.config
.gnupg
.java
.local
.mozilla
.msf4
.pki
.ssh
Desktop
Documents
Downloads
encryption
go
Music
own project
Pictures
pro
Public
Templates
usb encryption
Videos
wifi
packages.microsoft.gpg

File name:

Files of type: All Files (*.*)

Fig.2: Tool’s UI



Login to Access Tool

Username: vortex

Password: ••••••

Fig.3: Choosing password for the file to encrypt

https://doi.org/10.47059/AJMS/V4I6/02

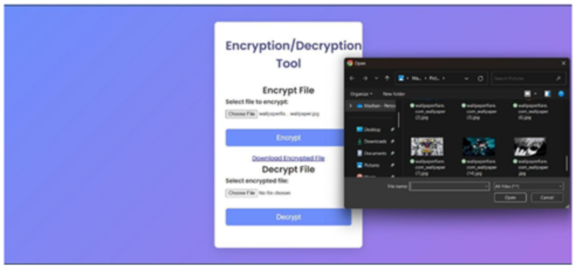


Fig.4: Encryption and Decryption

The secure data encryption and its evaluation and implementation The decryption system produced a number of significant results that contribute to the comprehension of encryption techniques and their real-world applications. The performance and security of the system will benefit greatly from these findings. of systems that use encryption. Comparative study with other types of deep learning models or conventional approaches used to predict apple leaf disease demonstrates the efficacy of transfer learning methods. The outcomes indicate that traditional methods consistently outperform transfer learning in terms of prediction accuracy, capacity for generalization, and resistance to variations in the environment. The highlights of this comparative analysis are benefits of using transfer learning, especially in situations where limited labeled data or dynamic environmental conditions.

The findings from this project suggest several avenues for future research. investigating hybrid encryption techniques that take advantage of Performance could be improved by symmetric and asymmetric algorithms alike. while preserving a high level of security. Furthermore, examining the impact of emerging technologies, such as quantum computing, on current encryption standards will be essential to prepare for potential future threats. Finally, further studies on user behavior regarding encryption practices could provide valuable insights into boosting cryptographic user engagement systems.

Strengths and Limitations

The proposed work's significance, strengths, and weaknesses Using MobileNetV2 and transfer learning, apple leaf disease prediction can be laid out as follows:

The development of the secure data encryption and decryption system in an increasingly digital world, carries significant implications for data security. world. As organizations and individuals alike face escalating threats to their sensitive data, the requirement for robust encryption solutions has never been greater. been more critical. By making a contribution to the field of cryptography, this project providing:

Enhanced Data Protection: The proposed system makes use of cutting-edge encryption algorithms that protect sensitive data and guarantee integrity, authenticity, and confidentiality. This is especially important for businesses that handle important information, like healthcare, government, and finance.

User Accessibility: The user-friendly interface makes it possible for non-technical users to easily use encryption techniques, fostering a culture of awareness of data security. By making the encryption process easier, this Work encourages more people to use safe data handling methods.

Performance Insights: The project offers useful insights into the performance characteristics of various encryption algorithms, directing future implementations with regard to security and efficiency trade-offs. This is crucial for developers and organizations seeking to enhance their data security measures.

The strengths include:

Robust Algorithm Selection: By combining the two symmetric algorithms (AES) and RSA asymmetric encryption techniques, the system achieves balancing speed and safety, addressing a variety of data protection requirements The system as a whole benefits from this layered strategy. resilience.

Comprehensive Security Analysis: A thorough review of security threats and vulnerabilities demonstrates the system’s ability to withstand common attack vectors, boosting confidence in its durability. The implementation of secure key management protocols improves the security posture further.

Performance Optimization: The results indicate efficient performance with low consumption of resources, making the system suitable for many different settings, including those with inadequate computing

https://doi.org/10.47059/AJMS/V4I6/02

power This flexibility is necessary for applications of the present day that demand efficiency in addition to security.

The limitations include:

User Dependency and Compliance: How Well the The encryption system is largely dependent on users following best practices. for data security. It is possible for users to disregard security protocols, such as updating encryption keys and maintaining strong passwords regularly, or comprehending how to handle encrypted data appropriately. Such carelessness may jeopardize the system's overall security.

Scalability Issues: There may be difficulties with the current implementation. when you need to scale to handle large datasets or a lot of transaction volumes, particularly in environments for businesses. whereas AES performs well with large and moderately sized data. processing requirements could necessitate further optimizations.

Limited Threat Model: The security analysis primarily addresses brute force and man-in-the-middle attacks are common attack vectors. attacks. However, the rapidly changing cybersecurity landscape new vulnerabilities may be introduced by threats that are not covered in this work. To adapt to, future updates and evaluations will be required. emerging dangers, such as advanced persistent dangers (APTs), also called zero-day exploits.

Dependence on Key Management Practices: Key management that is safe is necessary for efficient encryption. If keys are stored improperly, the entire encryption system's security was shared or generated. could be violated. The proposed work does not go into great detail. into the complexities of key management practices, which can vary significantly among various use cases and environments.

Resource Limitations in Low-Power Devices: Even though the system is optimized for performance, resource-intensive operations, especially those connected to asymmetric encryption might be unsuitable for low-power devices (e.g., IoT devices). The computational requirements of RSA and algorithms like it could be a hindrance. performance in such

https://doi.org/10.47059/AJMS/V4I6/02

settings, requiring investigation of alternatives that use light cryptography.

Potential Vulnerability to Quantum Computing: Even though the Current encryption algorithms are thought to be safe from traditional computing attacks, quantum computing's introduction presents a potential threat to conventional methods of cryptography This method currently does not employ post-quantum cryptography measures, putting it at risk from future quantum attacks.

Contextual Adaptability: The design of the proposed system includes a general method for encrypting and decrypting data, which may not be completely address the specific regulatory and compliance requirements of different business sectors (for instance, government, finance, and healthcare).

Future Works

Even though this project met its goals, there are still a number of areas that might be improved and investigated further to increase the system's resilience, flexibility, and security against new threats. The following areas could be the subject of future study and development:

Hybrid Encryption Approaches: In order to increase security and performance, future research could investigate the integration of hybrid encryption systems, which combine symmetric and asymmetric encryption inside a single procedure. System efficiency and security can be improved by hybrid systems, such as those that employ RSA for secure key exchanges and AES for data encryption.

Post-Quantum Cryptography: As quantum computing capabilities advance, conventional encryption methods like RSA and AES might become less effective. Researching post-quantum cryptography methods, such lattice-based encryption, can guarantee long-term data security by preparing the system for impending quantum attacks.

Enhanced Key Management: Given the need for safe key management, more sophisticated key management solutions may be developed in the future, maybe utilizing hardware-based security modules or decentralized approaches. By doing this, the risks related to key distribution and

https://doi.org/10.47059/AJMS/V4I6/02

storage would be reduced, strengthening the system's defenses against attacks involving keys.

Scalability Optimization: Future research could concentrate on streamlining the encryption and decryption procedures for high transaction volumes in order to support enterprise-level applications and bigger datasets. To preserve performance in a variety of settings, this may entail load balancing, parallel processing, or algorithmic improvements.

Machine Learning for Security Monitoring: An extra degree of security can be added by incorporating machine learning algorithms to monitor encryption operations in real-time and identify anomalous activity and possible security breaches. This could enable proactive threat mitigation and increase the system's responsiveness to new attacks.

Adaptation for Low-Power and IoT Devices: Future research could examine resource-efficient, lightweight encryption techniques that preserve security and allow the system to function well on low-power devices, such those seen in Internet of Things networks. The encryption system's variety of applications would increase if it were optimized for such devices.

User Education and Guidance: The interface's user education features, like tutorials, best practices, and warnings for weak encryption settings, could be the subject of future improvements. Users can avoid mistakes and improve overall security efficacy by being taught the value of encryption techniques.

Testing in Diverse Real-World Scenarios:A more thorough assessment of the system's advantages and disadvantages would be possible by extending testing across other environments and data kinds. Variations in network latency, device compatibility, and stress tests for extended operation are possible additional testing scenarios.

Compliance with Industry Standards: The system may be more applicable in sectors with strict data protection regulations if it is customized to satisfy certain regulatory criteria, such as GDPR in the EU or HIPAA in the healthcare sector. Creating adaptable security policies in accordance

https://doi.org/10.47059/AJMS/V4I6/02

with legal requirements may be one way to do this.

Conclusion

Confidentiality, integrity, and sensitive data authentication were the main goals of this project, which successfully created and assessed a secure data encryption and decryption system. The system exhibits a balanced approach to security and performance by combining symmetric (AES) and asymmetric (RSA) encryption techniques. The findings demonstrated that while RSA improves security for key exchanges and short data transactions, AES offers quick encryption and decryption speeds, making it appropriate for managing huge data volumes. Additionally, the system included an intuitive user interface that allowed users with different technical backgrounds to use it.

Because of strong key management procedures and encryption algorithms, the system is resistant to conventional attack vectors like brute-force and man-in-the-middle assaults, according to the project's security research. Furthermore, AES and RSA resource efficiency under modest usage was highlighted by performance valuations; nevertheless, scaling for bigger datasets revealed constraints. User comments also emphasized how crucial usability is to encouraging safe data handling procedures. All things considered, the project offers a dependable, easily accessible, and safe encryption solution for contemporary data security requirements.

References

1. AES-Based Encryption Algorithms for Text and Image Dr. Shweta Singh, Vandana Yadav Journal: International Journal of Computer Applications, 2015
2. Kumar and K. Singh, "A Hybrid Approach to Text and Image Encryption Using AES and DNA Cryptography," International Journal of Information Technology and Computer Science
3. Kavita Gupta, Sunita Sahu Journal: International Journal of Network

Security & Its Applications (IJNSA) 2018

4. M. Dhivya, A. Pravin Journal: International Journal of Recent Technology and Engineering (IJRTE)Year: 2019
5. M. Banupriya, R. Vijayakumar Journal: Journal of Emerging Technologies and Innovative Research (JETIR) Year: 2019
6. M. Asim, A. K. Khan, M. Imran Journal: Journal of Information Security Research, 2015.
7. M. Asim, A. K. Khan, M. Imran Journal: Journal of Information Security Research, 2015.
8. M. Dey, S. S. Chowdhury, and S. Biswas, "A Secure Image and Text Encryption Scheme Based on RSA and Chaotic Systems," International Journal of Computer Network and Information Security,
9. N. K. Pareek and V. Patidar, "Image Encryption Using Chaotic Logistic Map," Journal of Information Security and Applications,
10. R. Islam and M. Abdur, "Text and Image Encryption Using Blowfish Algorithm in Multimodal System," Journal of Computational and Theoretical Nanoscience, 2019.
11. Catherine, S., Kiruthiga, V., & Gabriel, R. (2024). Effective Brand Building in Metaverse Platform: Consumer-Based Brand Equity in a Virtual World (CBBE). In Omnichannel Approach to Co-Creating Customer Experiences Through Metaverse Platforms (pp. 39-48). IGI Global Scientific Publishing.
12. Catherine, S., Ramasundaram, G., Nimmagadda, M. R., & Suresh, N. V. (2025). Roots, Routes, and Identity: How Culture Shapes Heritage Travel. In Multiple-Criteria Decision-Making (MCDM) Techniques and Statistics in Marketing (pp. 343-352). IGI Global Scientific Publishing.
13. Catherine, S., Suresh, N. V., Mangaiyarkarasi, T., & Jenefa, L. (2025). Unveiling the Enigma of Shadow: Ethical Difficulties in the Field of AI. In Navigating Data Science: Unleashing the Creative Potential of Artificial Intelligence

https://doi.org/10.47059/AJMS/V4I6/02

(pp. 57-67). Emerald Publishing Limited.

14. Gokila, S., Helen, D., Alemu, A. M., & Suresh, N. V. (2024, November). Scaling Approach Over Learning Layer of Deep Learning Model to Reduce the FALSE Error in Binary Classification. In 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1294-1300). IEEE.
15. Helen, D., & Suresh, N. V. (2024). Generative AI in Healthcare: Opportunities, Challenges, and Future Perspectives. Revolutionizing the Healthcare Sector with AI, 79-90.
16. Kalaivani, M., Suganya, V., Suresh, N. V., & Catherine, S. (2025). The Next Wave in Marketing: Data Science in the Age of Generative AI. In Navigating Data Science (pp. 13-26). Emerald Publishing Limited.
17. Poongavanam, S., Srinivasan, R., Arivazhagan, D., & Suresh, N. V. (2023). Medical Inflation-Issues and Impact. Chettinad Health City Medical Journal (E-2278-2044 & P-2277-8845), 12(2), 122-124.
18. Suganya, V., & Suresh, N. V. (2024). Potential Mental and Physical Health Impacts of Spending Extended Periods in the Metaverse: An Analysis. In Creator's Economy in Metaverse Platforms: Empowering Stakeholders Through Omnichannel Approach (pp. 225-232). IGI Global.
19. Suresh, N. V., & Rexy, V. A. M. (2024, February). An Empirical Study on Empowering Women through Self Help Groups. In 3rd International Conference on Reinventing Business Practices, Start-ups and Sustainability (ICRBSS 2023) (pp. 957-964). Atlantis Press.
20. Suresh, N. V., Catherine, S., Selvakumar, A., & Sridhar, G. Transparency and accountability in big data analytics: Addressing ethical challenges in decision-making processes. In Digital Transformation and Sustainability of Business (pp. 742-745). CRC Press.
21. Suresh, N. V., Karthikeyan, M., Sridhar, G., & Selvakumar, A.

https://doi.org/10.47059/AJMS/V4I6/02

(2025). Sustainable urban planning through AI-driven smart infrastructure: A comprehensive review. Digital Transformation and Sustainability of Business, 178-180.

22. Suresh, N. V., Manoj, G., Rajkumar, M. D., & Kanagasabai, B. (2024). Fundamental anomalies as a mediator in the relationship between heuristics and investment decisions. International Journal of Applied Management Science, 16(4), 383-396.
23. Suresh, N. V., Selvakumar, A., Sridhar, G., & Jain, V. (2025). Dynamic Pricing Strategies Implementing Machine Learning Algorithms in E-Commerce. In Building Business Models with Machine Learning (pp. 129-136). IGI Global Scientific Publishing.
24. Suresh, N. V., Selvakumar, A., Sridhar, G., & Trivedi, S. (2024). A Research Study on the Ethical Considerations in Harnessing Basic Science for Business Innovation. In Unleashing the Power of Basic Science in Business (pp. 55-64). IGI Global.
25. Suresh, N. V., Shanmugam, R., Selvakumar, A., & Sridhar, G. Patient-centric care optimization: Strategies for enhancing communication and efficiency in healthcare settings through cross-functional collaboration. In Digital Transformation and Sustainability of Business (pp. 738-741). CRC Press.
26. Suresh, N. V., Sridhar, J., Selvakumar, A., & Catherine, S. (2024). Machine Learning Applications in Healthcare: Improving Patient Outcomes, Diagnostic Accuracy, and Operational Efficiency. In AI Healthcare Applications and Security, Ethical, and Legal Considerations (pp. 1-9). IGI Global

https://doi.org/10.47059/AJMS/V4I6/02