PASSWORD MANAGER USING   
 PROTECTION OF CIA TRAIDS

*Abstract*—Confidentiality, integrity, and availability are the three primary principles that the CIA triad, a fundamental idea in information security, uses to describe three key concepts. These three guidelines serve as the fundamental tenets of information security and are crucial for safeguarding private data as well as making sure that vital infrastructure and systems continue to be safe and effective. The term ”confidentiality” describes the safeguarding of private information from unauthorised disclosure. This might include private information, financial information, trade secrets, or any other kind of knowledge that, in the wrong hands, can be exploited for evil. Achieving confidentiality requires the use of several security measures, including access restrictions, encryption, and data loss prevention technologies. Confidentiality is crucial for preserving the privacy and security of persons and organisations.

Integrity is the safeguarding of data against unauthorised erasure or change. The accuracy, consistency, and completeness of the data must be guaranteed, as well as the absence of any alterations or corruption. Integrity, which is accomplished by the use of different security mechanisms like digital signatures, checksums, and access restrictions, is crucial for assuring the dependability and trustworthiness of data. The capacity of crucial resources and systems to continue to function and be reachable by authorised users is referred to as availability. This involves ensuring that infrastructure and systems are ready to use when required and that they won’t be interfered with by nefarious assaults, natural catastrophes, or other unforeseen occurrences. Access controls, redundancy, disaster recovery planning, and other security measures are used to ensure availability, which is crucial for guaranteeing that businesses can keep operating and serving their consumers.

These three ideas together make up the CIA trinity, which is utilised by businesses of all sizes and in all sectors to establish their security goals and create successful security plans. A crucial tool for information security experts, the CIA trinity directs the design, implementation, and administration of security procedures needed to safeguard crucial assets and systems. Balancing the demands of usability and security is one of the major issues faced by the CIA trio. Many times, security precautions can be overly onerous or restrictive, which makes it challenging for users to access the data or systems they need to do their jobs. The efficacy of the security measures themselves may eventually be harmed as a result of this irritation and inefficiency. By adopting security measures that are both efficient and user-friendly, organisations may solve this difficulty by finding ways to balance the demands for security and usability.

Managing the expenses involved with establishing and maintaining security measures is another difficulty faced by the CIA trio. In order to balance the costs of security with the expenses of doing business, organisations must discover ways to adopt and maintain security measures that are not prohibitively expensive [1]. This may entail doing cost-benefit evaluations, ranking security investments according to risk, and creating efficient risk management plans. Keeping up with the continuously changing danger landscape is another issue the CIA trio faces. Organisations must keep current with the most recent security trends and best practises in order to stay ahead of possible attacks since the tools and techniques used by attackers are always changing. To find possible vulnerabilities and fix them before attackers can exploit them, this calls for continual training, education, vulnerability assessments, and penetration testing.

Standardised security procedures and frameworks, ongoing



# Fig. 1: Data Protected by CIA triad

vulnerability assessments and penetration tests, user education and awareness campaigns, compliance management software, and risk management techniques can all be part of these solutions. Standardised security frameworks and protocols offer a starting point for security measures that may be used to safeguard vital assets and systems from a variety of possible attacks. These frameworks, including ISO 27001 and the NIST Cybersecurity context, offer recommendations for putting best practises in information security into practise and give security risks and vulnerabilities a common language and context for discussion. Organisations can find and fix possible vulnerabilities in their systems and infrastructure with the aid of regular vulnerability assessments and penetration testing. Organisations may keep ahead of possible threats by performing routine assessments and taking proactive measures to reduce risks before attackers can take advantage of them [?]. Programmes for user education and awareness are a crucial part of any successful security plan. These applications can instruct users on how to recognise the dangers posed by various security threats and how to protect themselves from them.

Organisations may manage the complicated regulatory environment related to information security with the use of compliance management software. Organisations may make sure they are complying with regulatory standards and avoiding penalties by automating compliance management procedures and offering real-time visibility into compliance status. Finally, good risk management techniques may assist businesses in striking a balance between security and operational expenses. Organisations may identify possible hazards and take affordable actions to minimise them by regularly performing risk assessments and creating risk management strategies [2]. Implementing and maintaining effective security measures, however, presents a number of difficulties, such as juggling the demands of usability and security, controlling costs, and keeping up with the quickly changing threat landscape. Organisations may use a range of solutions to address these issues, including standardised security protocols and frameworks, routine vulnerability assessments and penetration testing, user training and awareness programmes, compliance management tools, and risk management techniques.

## I. FINDING A PROBLEM

The three core foundations of cybersecurity—confidentiality, integrity, and availability—are described by the well-known CIA triangle. Integrity guarantees that data is true, whole, and unaltered. The capacity to utilise and access data and information systems [3] at any time is referred to as availability. The security of these CIA triads is more crucial than ever in the current digital era. Organisations run the risk of losing sensitive data or being unable to access vital systems due to the sophistication and frequency of cyberattacks. The lack of knowledge and comprehension of the threats posed by cyber assaults is one of the biggest issues that organisations encounter when it comes to defending the CIA trinity.

Many businesses are not completely aware of the ramifications of a cyber assault or how it can affect their daily operations. They can be ignorant of the many cyberattacks that might harm their company, such as ransomware, phishing, or malware. Organisations could also be unaware of the possible expenses linked to a cyber attack [4], such as lost income, legal fees, and expenditures for data recovery. Although the CIA triad is a fundamental idea in information security, organisations encounter a number of difficulties when attempting to implement it successfully.

The following are some of the major issues with the CIA triad:

1. Striking a balance between security and usability: Oneof the main difficulties in putting the CIA trinity into practise is doing so. Access restrictions and other security measures, like encryption, are crucial for safeguarding sensitive data, but they may also be burdensome and challenging to operate. Users may become irritated as a result, which might make it harder for them to do their duties well. For security measures to be effective without slowing productivity, organisations must find a balance between security and usability.
2. Managing Complexity: The complexity of an organization’s information systems rises as a result of the organization’s increased reliance on technology for data processing and storage. Information availability, confidentiality, and integrity may become more challenging as a result. Businesses must be able to handle the complexity of their information systems and put in place security measures that work across a variety of platforms and technologies.
3. Dealing with Emerging Threats: Because cyber threatsare continuously changing, organisations need to be ready to modify their security protocols to deal with them. This necessitates a proactive approach to security, where businesses continuously scan for fresh threats and modify their defences as necessary.
4. Cost: The CIA trinity can be expensive to implement,especially for financially strapped mediumsized companies. The costs of hardware, software, and staff can be high for encryption, access restrictions, and other security measures [5]. Organisations need to be able to weigh the expenses of putting security measures in place against the dangers and repercussions of a security breach.
5. Human mistake: Although technology can help secureinformation, security breaches are nevertheless frequently caused by human mistake. Employees could unintentionally divulge private information or become victims of social engineering schemes or phishing assaults [6]. Organisations must provide staff training and security awareness programmes to inform them of the value of security and to guide them in avoiding typical security traps.
6. Compliance: Many sectors of the economy are subjectto legal obligations for data security and protection. The implementation of certain security measures and ongoing audits and assessments are required for organisations to comply with these rules, which can be difficult and timeconsuming.

In conclusion, while the CIA triad offers a framework for comprehending the essential ideas of information security, organisations must overcome a number of obstacles and issues in order to execute it successfully. Organisations may enhance their capacity to defend sensitive data and systems from cyber attacks by balancing security with usability, managing complexity, addressing emerging risks, controlling costs, limiting human error, and assuring compliance.

## II. METHOD AND SOLUTION

Here are the Methods and Solutions to the problems which are listed above:-

1. Balancing Security and Usability: Organisations canemploy security measures that are efficient without being overly onerous to balance security with usability. A business may, for instance, establish a two-factor authentication system that asks users for both a password and a one-time code issued by a hardware token or mobile app [7]. Offering user education and awareness programmes is another way to establish good security habits and assist users in avoiding frequent hazards. Users need to be made aware of the value of using secure passwords, how to prevent phishing scams, and how to keep their operating systems patched with the most recent security updates.
2. Managing Complexity: Organisations can put in placesecurity measures that work across several platforms and technologies to manage the complexity of information systems. To guarantee that security procedures are uniform throughout the organisation, one way is to adopt standardised security protocols and frameworks, such as ISO 27001 or NIST [8]. The difficulty of maintaining security across many systems and platforms may be lessened as a result. To find gaps and vulnerabilities in the organization’s systems, frequent vulnerability assessments and penetration testing are an additional option. This enables organisations to prioritise their security spending and can assist in identifying areas that require extra security measures.
3. Addressing new risks: Organisations must take a proactive stance when it comes to security in order to handle new risks. Monitoring for emerging threats and vulnerabilities and putting solutions in place to address them before they can be exploited are some solutions. In order to do this, one must be updated on the most recent threat intelligence and trends and make use of threat intelligence services and information sharing programmes.Another option is to conduct routine security assessments, such as vulnerability scanning and penetration testing, to identify possible threats and weaknesses. Before attackers can take advantage of them, this can assist organisations in identifying and addressing vulnerabilities.



# Fig. 2: Review spam detection comparison of prior research and outcomes, as well as the relative complexity of the method

1. Cost: Organisations can prioritise their security investments depending on the degree of risk associated with certain assets or systems to control the expenses related to executing the CIA trinity. A risk assessment to find high-value assets and possible vulnerabilities, followed by the implementation of security measures to reduce such risks, is one option. This can assist businesses in concentrating their security spending on the regions that are most important to the operation. To lower the cost of adopting and monitoring security measures, another possibility is to make use of cloud-based security services and outsourcing options. This can enable organisations to concentrate on their core business operations while lowering the overhead associated with handling security.
2. Human mistake: Organisations may develop user training and awareness programmes to encourage good security practises and help users avoid typical security risks to lower the chance of a human error. Regular security awareness training may help users understand the value of good security practises and provide them the information they need to avoid frequent hazards. This is one way. To lessen the possible impact of human mistake, access restrictions and user permissions can be implemented. By doing this, users may be sure that they only have access to the systems and information they require to do their work.
3. Compliance: Organisations can create a security framework, such as ISO 27001, and undertake routine audits and assessments to make sure their security measures are efficient and in compliance in order to ensure compliance with regulatory requirements. To find areas where the organization’s security procedures may not be meeting regulatory standards, one way is to undertake routine security audits and assessments. Utilising compliance management software to simplify compliance reporting and paperwork is another option. By doing so, the organisation may maintain compliance with regulatory obligations while lowering the costs related to compliance management.

In conclusion, implementing a comprehensive security strategy that emphasises balancing security with usability, managing complexity, addressing emerging threats, managing costs, mitigating human error, and ensuring compliance is necessary to address the challenges and issues related to the CIA triad. Technical and organisational measures are needed to implement these solutions, including the use of standardised security frameworks and protocols, the implementation of access controls and user permissions, routine vulnerability assessments and penetration testing, and user education and awareness programmes.

## III. METHOLOGY AND RESULT

### A. Password Manager

A password manager is a piece of software made for managing passwords and other sensitive data including login credentials, credit card information, and bank account information. A password manager’s main function is to assist users in creating and managing secure, one-of-a-kind passwords for each of their online accounts, lowering the risk of identity theft and data breaches. Users can establish a strong master password that unlocks their password manager, saving them from having to remember dozens or even hundreds of hard passwords. Passwords and other sensitive data are often encrypted and stored by a password manager either locally on the user’s device or in the cloud using high-tech encryption methods. Additional security features like two-factor authentication, password strength testing, and automatic password changing are also available with many password managers. On a variety of platforms, including desktops, mobile devices, and web browsers, password managers can be used. They frequently interact with online browsers and enable autofill of login information, speeding the login procedure and lowering the possibility of typos and other problems.

### B. Cipher

A cypher is a technique or system for encoding or encrypting data in order to keep it private and secure while it is being sent or stored. A key, also known as a secret code or algorithm, is typically employed in cyphers to transform the original message, also known as plaintext, into an unintelligible form known as ciphertext.Since ancient times, cyphers have been used to protect sensitive data. There are many different types of cyphers, from straightforward substitution cyphers to intricate encryption algorithms.

Some common types of ciphers include:

1. Caesar Cipher: a straightforward substitution cypher that involves moving the alphabet’s letters a predetermined number of positions.
2. Vigenere Cipher: a more complicated replacement cypher that encrypts the plaintext using a keyword.
3. AES (Advanced Encryption Standard):a popular symmetric key encryption technique for data encryption and secure transport.
4. RSA (Rivest-Shamir-Adleman):a popular asymmetric key encryption technique for use in digital signatures, secure communication, and other cryptographic applications.

To offer a complete security solution for sensitive information, cyphers can be used in conjunction with other security methods like password protection, digital certificates, and firewalls.

### C. Key

A key is a piece of knowledge used in cryptography to encode or decrypt data using a cypher or encryption technique. As they control how plaintext data is converted into ciphertext, keys are crucial for protecting the confidentiality and integrity of sensitive information.

In cryptography, symmetric keys and asymmetric keys are the two primary key types.

1. Symmetric Keys: The same key is employed in a symmetric key encryption scheme for both encryption and decryption. This implies that a message’s sender and recipient must use the same key. When the sender and the message’s recipient already know one another and the key can be securely exchanged, symmetric keys are frequently employed.
2. Asymmetric Keys: Two distinct keys are utilised for encryption and decryption in an asymmetric key encryption scheme. Although these keys are mathematically connected, it is computationally impossible to determine which key comes first. This means that a communication can be encrypted using the recipient’s public key by the sender, and decrypted using the recipient’s private key. When the sender and the recipient of a communication do not already know one another and a secure key exchange is required, asymmetric keys are frequently utilised.

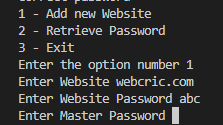
Keys can be of different lengths and complexity, and the strength of a cipher often depends on the strength of the key used. Longer keys and more complex encryption algorithms can provide greater security, but can also be more resourceintensive and slower to execute.

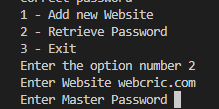
### D. AES-256-GCM cipher

Advanced Encryption Standard, usually known as AES, is a specification for the encryption of electronic data. The number 256 denotes the key’s bit size. Additionally, GCM is a symmetric key cryptographic block cipher’s authenticated mode of operation.AES-256-GCM is a symmetric key encryption cypher that combines the 256-bit key length of the Advanced Encryption Standard (AES) with the Galois/Counter Mode (GCM) of operation. Sensitive data in transit, such as network traffic or data sent over the internet, is frequently secured using this cypher.AES-256 is a block cypher that encrypts data in 128-bit blocks and converts plaintext into ciphertext using a 256-bit key. Due to its strong defence against brute-force and other cryptographic assaults, AES-256 is now regarded as one of the most secure symmetric encryption algorithms available.

Using a combination of the AES encryption algorithm and the Galois Message Authentication Code (GMAC), GCM is a mode of operation that ensures the confidentiality and authenticity of the encrypted data. GCM randomises the encryption process using a special initialization vector (IV), which improves security and stops attackers from spotting trends in the encrypted material.Strong encryption is needed for applications like encrypted email, virtual private networks (VPNs), and other secure communications, and the combination of AES-256 with GCM offers a high level of security and performance. AES-256-GCM can be resource-intensive and may need a lot of processing power to encrypt and decrypt huge amounts of data, which could affect how some apps function.

The Python 3 programming language was used to create the software programme known as The Password Manager. The programme makes use of a number of libraries, including PyCryptodome, PBKDF2, and pickle, to perform its functions.The user is asked to enter their Master Password as soon as the application opens in order to confirm their identity. This step is essential to make sure the user has permission to use the



  
Code Outputs

application’s features. The application presents the user with a selection of options when the user’s identification has been confirmed.The user is prompted to provide any information needed for the operation after choosing an operation from the menu. For instance, if a user wants to add a new password to the application, they will be required to input the password as well as the username or email address for the account, the name of the website or application that the password is linked with, and the password itself.Once the user has entered all the required data, the Password Manager carries out the requested operation. As an illustration, if the user choose to add a new password, the application would securely store the new password using the libraries upon which it was based.

The operation’s output is then printed for the user to see. This message could be a confirmation that the procedure was successful or it could show information about a password that the user has obtained from the application. A secure and dependable tool for handling passwords and other sensitive information is password managers. Users may manage their passwords easily thanks to its simple user interface and usage of the PyCryptodome, PBKDF2, and pickle libraries, which guarantee that user data is secured and shielded from unauthorised access.

## IV. ANALYSIS AND OUTCOME EXPECTIONS

The precise actions taken by an organisation will determine the outcomes and analysis of applying the solutions linked to the issues and difficulties related to the CIA trinity. However, the following are some typical results that businesses can anticipate when using these solutions:

1. Improved Security Posture: Improving an organization’s security posture entails lowering the probability and severity of security events. Organisations may make sure that their security procedures are uniform and successful across a variety of systems and platforms by putting into practise standardised security protocols and frameworks. Implementing the ISO 27001 framework, for instance, offers a structured approach to information security management, assisting organisations in identifying and managing their security risks in a methodical and thorough manner. Organisations may also find possible vulnerabilities and fix them before they can be exploited by attackers with the use of frequent vulnerability assessments and penetration testing. Programmes for user education and awareness may assist ensure that users are knowledgeable of sound security procedures and can steer clear of typical security hazards, such falling for phishing schemes or using weak passwords [9].
2. Enhanced Resilience: Increasing an organization’s resilience involves making it capable of carrying on business in the event of security incidents. Organisations may adopt security measures that are efficient without being overly onerous by striking a balance between security and usability. This can guarantee that users can do their tasks without being hampered by too onerous security procedures. Additionally, frequent vulnerability assessments and penetration testing may assist organisations in locating vulnerabilities and addressing them before they can be used by attackers, making it more challenging for attackers to access the organization’s systems.
3. Better Risk Management: Effective risk management of security risks entails analysing possible vulnerabilities and putting in place the necessary security safeguards to lessen those risks. Organisations may identify valuable assets and possible weaknesses through risk assessments, and then put security measures in place to reduce the risks. Organisations can concentrate their resources on the areas that are most important to the company by prioritising security investments depending on the amount of risk associated with particular assets or systems. Organisations may make sure they can maintain a strong security posture without going bankrupt by controlling the expenses involved with executing the CIA trifecta. Effective risk management entails a thorough approach to security that takes into account organisational and technological aspects as well as the organization’s larger commercial environment.
4. Increased Compliance: A crucial element of efficient security management is compliance with legal regulations. Organisations may make sure that their security procedures are efficient and in compliance by establishing a security framework, like ISO 27001, and carrying out routine audits and assessments. Software for compliance management can assist in streamlining compliance reporting and paperwork, lowering the administrative burden of compliance management. Organisations can decrease their exposure to the legal and financial dangers of non-compliance while also increasing their overall security posture by increasing their compliance with regulatory regulations [10].

In conclusion, putting the CIA triad’s challenges and problems into practise can help organisations strengthen their security posture, become more resilient to security incidents, manage their security risks more effectively, and adhere to regulatory requirements better. Organisations may guarantee the confidentiality, integrity, and accessibility of their vital assets and systems by attaining these results.

## V. CONCLUSIONS

In conclusion, the CIA triad is a fundamental idea in information security that identifies three key principles: confidentiality, integrity, and availability. These concepts are crucial for protecting crucial assets and systems. Although these ideas are simple in theory, there are several difficulties and obstacles related to efficiently putting them into practise. Organisations may employ a range of strategies and solutions, nevertheless, to get beyond these obstacles and get the required results. Organisations may strengthen their security posture and lessen the probability and severity of security events by establishing standardised security protocols and frameworks, performing routine vulnerability assessments and penetration tests, and implementing user training and awareness programmes [11]. This can guarantee that vital assets and systems are safe and guarded against theft, damage, and unauthorised access. A crucial element of efficient security management is boosting resilience. Organisations may do this by striking a balance between security and usability, putting in place the necessary security measures, and carrying out frequent vulnerability assessments and penetration tests to find and fix possible flaws before attackers can take advantage of them. By doing this, organisations may lessen the effects of security events and carry on with business as usual in the event of a disruption. Another crucial element of efficient security management is improved risk management. Organisations can make sure they are able to maintain an effective security posture while also being mindful of costs and business priorities by conducting risk assessments. Effective risk management entails a thorough approach to security that takes into account organisational and technological aspects as well as the organization’s larger commercial environment.

Effective security management also requires compliance with legal and regulatory obligations. Organisations may make sure that their security procedures are efficient and in compliance by establishing a security framework, like ISO 27001, and carrying out routine audits and assessments. Software for compliance management can assist in streamlining compliance reporting and paperwork, lowering the administrative burden of compliance management. Organisations can decrease their exposure to the legal and financial dangers of noncompliance while also increasing their overall security posture by increasing their compliance with regulatory regulations. Implementing the solutions for the issues and challenges brought on by the CIA triad can, in general, assist organisations in achieving the goals of a better security posture, increased resilience, better risk management, and improved compliance. These results can assist organisations in ensuring the confidentiality, integrity, and accessibility of their vital assets and systems, hence lowering the risk of security events and minimising their potential effects when they do occur. Organisations should promote a security-conscious culture among their employees in addition to the approaches and fixes covered above [12]. This might entail establishing clear-cut security rules and processes as well as giving staff members continual training and instruction. Organisations may guarantee that all workers are knowledgeable about sound security procedures and capable of actively contributing to the upkeep of the security of vital assets and systems by establishing a culture of security. The CIA triad, which describes three fundamental principles crucial for protecting vital assets and systems, is a key idea in information security. Although effectively putting these principles into practise comes with a number of difficulties and problems, there are also many different approaches and solutions that organisations can use to get past these obstacles and achieve the desired outcomes of improved security posture, increased resilience, better risk management, and improved compliance. Organisations can ensure the confidentiality, integrity, and accessibility of their crucial assets and systems by putting these strategies into practise and cultivating a culture of security. This lowers the risk of security incidents occurring and lessens the potential impact of those incidents that do occur.

## REFERENCES

1. Elaine Barker, WC Barker, WE Burr, WT Polk, and ME Smid. Sp 80057 part 1 rev. 4 recommendation for key management part 1: General. *NIST special publication*, 800:57, 2016.
2. Khando Khando, Shang Gao, Sirajul M Islam, and Ali Salman. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106:102267, 2021.
3. Douglas Robert Stinson and Maura Paterson. *Cryptography: theory and practice*. CRC press, 2018.
4. Laura Jaime and Joao Barata. Using floss to implement cobit for i&t˜ governance. 2022.
5. SANS Institute. 6. training on security awareness: A step-by-step guide. Taken from the “Guide” section of https://www.sans.org/securityawareness-training, 2021.
6. The National Institute of Standards and Technology’s (NIST) Computer Security Resource Centre. Implementation tiers of the nist cybersecurity framework. https://www.nist.gov/cyberframework/implementingcybersecurity-framework, 2021.
7. Douglas Robert Stinson and Maura Paterson. *Cryptography: theory and practice*. CRC press, 2018.
8. National Institute of Standards and Technology (NIST). Organisation, mission, and information system perspectives on managing information security risk. https://www.nist.gov/publications/managing-informationsecurity-risk-organization-mission-and-information-system, 2020. [Online; accessed 29-April-2023].
9. John Halamka, Ari Juels, Adam Stubblefield, and Jonathan Westhues. The security implications of verichip cloning. *Journal of the American Medical Informatics Association*, 13(6):601–607, 2006.
10. John Halamka, Ari Juels, Adam Stubblefield, and Jonathan Westhues. The security implications of verichip cloning. *Journal of the American Medical Informatics Association*, 13(6):601–607, 2006.
11. Evandro Leonel Pereira, Aristides Sebastiao Lopes Carneiro, Eder˜ Ruschel, Marcio De Lima Corcovado, Jordan Da Silva Paiva, and Francisco Eduardo Medved. Measures to improve the cybersecurity of critical infrastructure in brazil. *Annals of Disaster Risk Sciences: ADRS*, 3(1):0–0, 2020.
12. Alex Neelankavil Devassy and Dhanith Krishna. Safeguarding blockchains from adversarial tactics. In *Blockchain for Industry 4.0*, pages 63–90. CRC Press.