# Data Encryption Mobile Storage Management Procedure Based on Virtual Disk

**S.Saroja Devi,**
Assistant Professor, Department of Information Technology, J.J. College of Engineering and Technology, Trichy, Tamilnadu
**K.Sindhuja,**
Assistant Professor, Department of Information Technology, J.J. College of Engineering and Technology, Trichy, Tamilnadu
**C.Selva Kumar,**
Assistant Professor, Department of Information Technology, J.J. College of Engineering and Technology, Trichy, Tamilnadu

**Abstract**

This research presents a procedure for managing data encryption on mobile storage devices through the implementation of a virtual disk. The proposed procedure involves several steps, including the creation of an encryption roll identification at the beginning of the mobile storage device and the establishment of a virtual magnetic disc encryption roll within the device. When the mobile storage device is inserted into a designated computer, the encryption roll identification is checked. If the identification is incorrect, the device is treated as a regular mobile storage device. However, if the check is successful, the encryption roll information of the virtual disk is examined, and upon passing the verification, the encryption roll is mounted. A virtual disk drive program with an encryption and decryption module is invoked to enable real-time encryption and decryption of the virtual disk's data. The encryption and decryption module automatically encrypts and decrypts data, ensuring the security and reliability of information storage. When the mobile storage device is removed, the virtual disk encryption roll is automatically unloaded. This procedure offers various advantages, including robust information storage, flexible security policy configuration, simplified management of portable storage devices, and efficient and transparent data encryption and decryption processing.

**Keywords**: Data encryption, Mobile storage management, Virtual disk, Encryption roll identification, Real-time encryption, and decryption

**DOI Number: 10.48047/nq.2020.18.8.nq20241** **NeuroQuantology 2020;18(8):295-301**



## Introduction

With the increasing reliance on mobile storage devices for data storage and transfer, ensuring the security and confidentiality of sensitive information has become a critical concern. Data encryption has proven to be an effective approach to protect against unauthorized access and data breaches. However, managing data encryption on mobile storage devices can be challenging due to the need for efficient encryption and decryption processes, secure storage, and convenient management.In this research, we propose a data encryption mobile storage management procedure based on a virtual disk.[1] The procedure leverages the concept of a virtual disk to create an encrypted storage environment within the mobile device. By implementing encryption roll identification and a virtual magnetic disc encryption roll, the

procedure establishes a secure foundation for managing data on the mobile storage device.

The core steps of the proposed procedure involve writing an encryption roll identification at the beginning of the mobile storage device and constructing a virtual magnetic disc encryption roll within the device. The encryption roll identification is checked when the mobile storage device is inserted into a designated computer. If the identification is incorrect, the device is treated as a regular mobile storage device. However, if the check is successful, the encryption roll information of the virtual disk is examined, and upon passing the verification, the encryption roll is mounted.[2]To facilitate the encryption and decryption processes, a virtual disk drive program with an encryption and decryption module is invoked.

This module enables real-time encryption and decryption of data within the virtual disk, ensuring the security and integrity of stored information. Furthermore, the procedure allows for the automatic unloading of the virtual disk encryption roll when the mobile storage device is removed, providing convenience and seamless integration with existing workflows. The figure (**Fig**.1) below shows the steps of data security framework for cloud computing.[3,4]

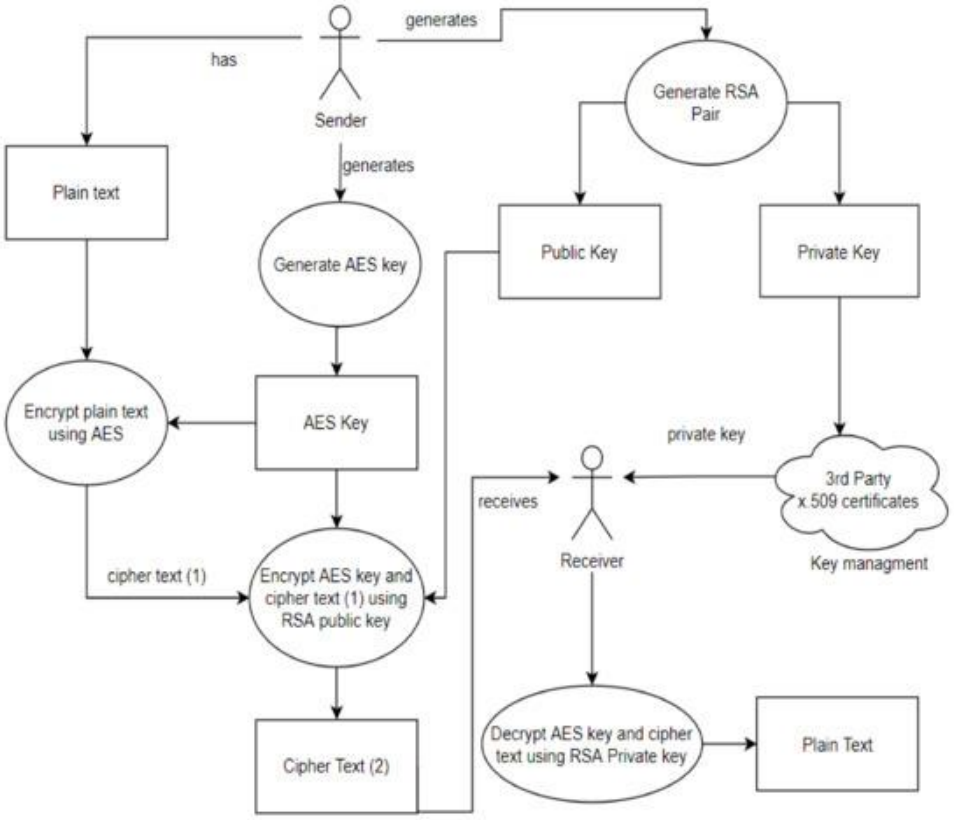


*Fig. 1: Data Security Framework for Cloud Computing*

The proposed procedure offers several advantages over traditional data encryption approaches. Firstly, it ensures the safety and reliability of information storage, protecting sensitive data from unauthorized access. Secondly, it provides flexibility in security policy configuration, allowing users to customize encryption settings based on their specific requirements. Additionally, the procedure simplifies the management of portable storage devices by incorporating the virtual disk

framework, enabling straightforward access and administration of encrypted data.[5]

Furthermore, the procedure demonstrates high efficiency and transparency in data encryption and decryption processing. By leveraging real-time encryption and decryption capabilities, data can be seamlessly accessed and modified within the virtual disk without compromising performance. The automatic unloading feature further enhances the user experience by reducing manual intervention and streamlining the storage device's discharging process. This research proposes a comprehensive data encryption mobile storage management procedure based on a virtual disk. The subsequent sections will delve into the technical details, implementation, and evaluation of the proposed procedure, highlighting its effectiveness in enhancing data security, flexibility, convenience, and efficiency in managing mobile storage devices.[6]

**Related Work**

In the midst of the ongoing digitization and technological advancements, computers have become an integral part of people's lives, influencing various aspects of both personal and professional spheres.[1] One device that has gained significant popularity for its convenience and practicality is the USB flash disk, commonly referred to as a U-disk. With its small and portable design, ample storage capacity, and seamless plug-and-play functionality, the U-disk has become an indispensable tool for data storage and transfer in daily life.[2]However, as the reliance on U-disks continues to grow, so do the concerns surrounding data security. The increasing instances of data leaks and unauthorized access have raised significant alarms, prompting the need for effective solutions to protect sensitive information. In response to this critical issue, encrypted U-disks have emerged as a timely and necessary innovation.[7,8]

Encrypted U-disks encompass a range of implementations, each with its own approach to data security. One common type is simple cipher authentication, where the U-disk employs a basic password-based authentication structure.[4] However, this procedure often falls short in terms of robust data encryption since the actual storage content remains unencrypted. As a result, it provides only limited protection against data breaches.

Another type of encrypted U-disk involves hardware encryption. This approach utilizes a dedicated control chip embedded within the U-disk to enable real-time encryption and decryption of data.[5] While hardware encryption offers a higher level of security, it requires specialized encryption and decryption chips, making the production costlier. Consequently, this procedure is more commonly adopted by organizations with specific security requirements or government agencies dealing with sensitive information.[9]



The third and most prevalent type of encrypted U-disk is software cryptography. This approach involves encrypting the data stored on the U-disk using either built-in encryption software or supplementary software tools. This software-based encryption allows users to protect their data without the need for additional hardware components.[6] As a result, software encryption U-disks have gained popularity among civilian enterprises, institutions, and individual users seeking an accessible and cost-effective solution for data security.Initially, software encryption U-disks were primarily used by government agencies and security-conscious organizations, given the heightened sensitivity of their data. However, with the increasing awareness of data privacy and the potential consequences of data breaches, software encryption U-disks have become widely adopted in various sectors. These U-disks provide users with enhanced privacy protection by encrypting the stored data, making it significantly more challenging for unauthorized individuals to access or decipher the information.[10]

By employing software cryptography, these U-disks cater to the diverse data security needs of different entities and individuals. They offer peace of mind for personal users who wish to safeguard their sensitive information, such as personal documents, financial data, or personal photographs. Simultaneously, they meet the rigorous data security requirements of businesses and institutions, protecting valuable intellectual property, confidential documents, or client information.[8]In summary, encrypted U-disks, especially those employing software cryptography, have become an indispensable tool for ensuring data security in an increasingly digital world. They offer a practical and cost-effective solution for protecting sensitive information, addressing the growing concerns surrounding data leaks and unauthorized access.[9] As technology advances further, the evolution of encrypted U-disks is likely to continue, providing even more robust and sophisticated data security measures to meet the ever-growing demand for privacy and confidentiality.[11]

**Research Objective**

The objective of this research is to develop a data encryption mobile storage management procedure based on a virtual disk. The aim is to enhance the security and reliability of information storage on mobile storage devices while providing flexibility in security policy configuration. Additionally, the research aims to simplify the management of portable storage devices and achieve high efficiency and transparency in data encryption and decryption processes.

**Data Encryption Mobile Storage Management Procedure for Virtual Disk**

This research introduces a data encryption mobile storage management procedure focused on virtual disks. The procedure offers a comprehensive approach to safeguarding data on mobile storage devices. The implementation steps of the procedure are outlined as follows:

Creation of Virtual Disk Encrypted Volume: A virtual disk encrypted volume is established by writing an encrypted volume identification at the head of the mobile storage device. The virtual disk encrypted volume information header is encrypted using a user-defined password. This header contains essential data, such as the data encryption and decryption keys, operating strategy information, and virtual disk file structure details.

Encrypted Volume Mark Verification: When the mobile storage device is inserted into a designated computer, the encrypted volume mark is checked for correctness. If the mark is incorrect, the device is recognized as an ordinary mobile storage device. Otherwise, the structure proceeds to the next step, assuming it is an encrypted mobile storage device.



Password Decryption and Verification: The user input's password is used to decrypt the virtual disk encrypted volume information header on the encrypted mobile storage device. The decrypted header is then verified. If the verification succeeds, the process proceeds to the next step. Otherwise, it returns to step 3) or forbids the mounting of the virtual disk encryption volume and exits.

Mounting and Encryption of Virtual Disk: The virtual disk encryption volume is mounted using the primary and secondary keys obtained from decrypting the virtual disk encrypted volume information header. A specified computing machine calls the virtual disk driver, which incorporates an encryption/decryption module. This module enables reading and writing of the virtual disk encrypted volume based on user instructions. The encryption/decryption module utilizes the primary and secondary double secret keys to perform automatic real-time encryption and decryption of the virtual disk's content. Finally, the virtual disk encrypted volume is automatically unloaded when the encrypted mobile storage device is removed. The figure (**Fig**.2) below illustrates a tool for data encryption.

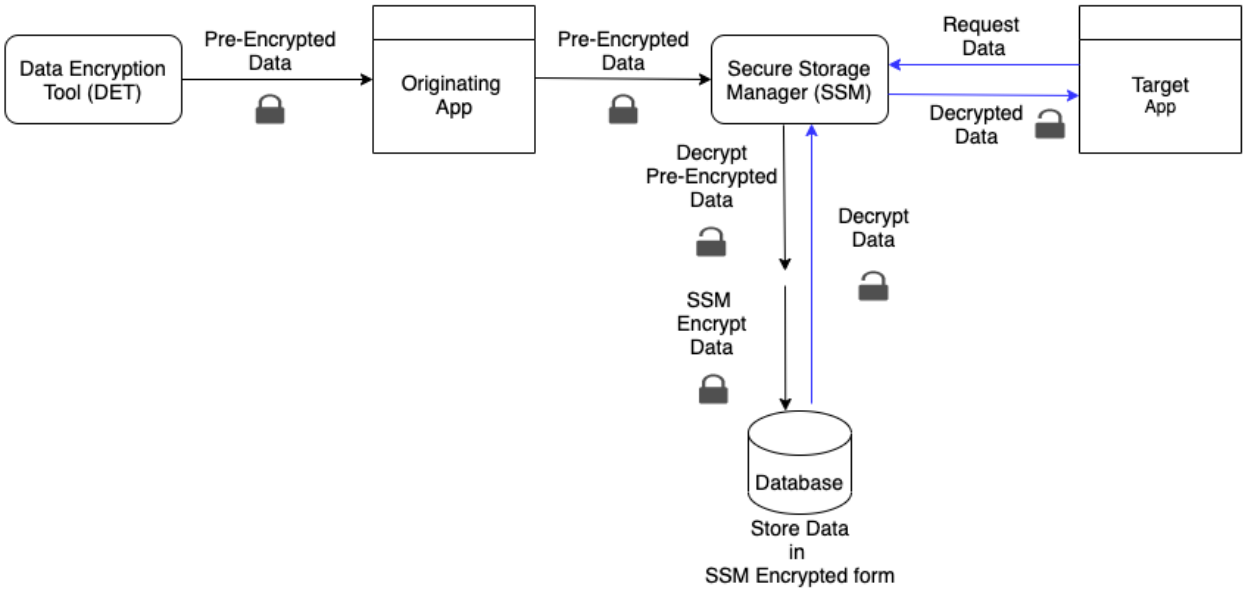


*Fig. 2: Tool for Data Encryption*



The proposed procedure provides a comprehensive solution for secure data storage on mobile devices. By leveraging virtual disks and encryption techniques, it offers enhanced data protection, ensuring the confidentiality and integrity of stored information. The procedure's utilization of encryption/decryption modules enables seamless and automatic encryption and decryption of data in real-time, minimizing user intervention. Overall, this research contributes to the development of efficient and reliable data encryption procedures for mobile storage management.

**Conclusion**

In this research, we have proposed a data encryption mobile storage management procedure based on a virtual disk. The procedure addresses the growing concerns surrounding data security on mobile storage devices, offering a comprehensive solution to protect sensitive information. By leveraging virtual disks and encryption techniques, the procedure ensures the confidentiality, integrity, and reliability of stored data.Through the implementation steps outlined in this research, we have established a robust framework for managing encrypted mobile storage devices. The creation of virtual disk encrypted volumes, along with the encryption of the volume information header using user-defined passwords, provides a strong foundation for secure data storage. This approach enhances the safety and reliability of information storage, mitigating the risk of unauthorized access or data breaches.The verification of the encrypted volume mark during device insertion adds an extra layer of security. If the mark is incorrect, the device is recognized as an ordinary mobile storage device, preventing unauthorized access to the encrypted data. This step ensures that only authorized users can access the encrypted volume, further enhancing data protection.The password decryption and verification process is a critical component of the proposed procedure. By decrypting the virtual disk encrypted volume information header using the user's input password, we enable access to the encrypted data. The verification of the decrypted header ensures the integrity and authenticity of the data, preventing unauthorized modifications or tampering. This step reinforces the security of the encrypted mobile storage device and strengthens the overall data protection measures.

The mounting and encryption of the virtual disk enables seamless access and management of the encrypted data. By utilizing the virtual disk driver program with an encryption/decryption module, we facilitate real-time encryption and decryption of data within the virtual disk. This ensures that the data remains protected during both storage and retrieval processes, providing a transparent and efficient experience for users.One of the notable advantages of the proposed procedure is its flexibility in security policy configuration. Users can customize encryption settings based on their specific requirements, tailoring the security measures to meet their unique needs. This adaptability makes the procedure suitable for a wide range of scenarios, catering to diverse data security demands.

Additionally, the automatic unloading feature of the virtual disk encrypted volume upon device removal adds convenience to the overall storage management process. Users can easily disconnect the encrypted mobile storage device without the need for manual unmounting, streamlining workflows and reducing the risk of accidental data exposure.In conclusion, the data encryption mobile storage management procedure based on a virtual disk presented in this research provides a comprehensive and effective solution for safeguarding data on mobile storage devices.

By leveraging encryption, virtual disk technology, and robust management processes, the procedure ensures the safety, reliability, and flexibility of information storage. It addresses the growing concerns surrounding data security, especially in the context of mobile devices, offering users peace of mind and empowering them to protect their sensitive information effectively. As the digital landscape continues to evolve, the proposed procedure paves the way for enhanced data protection and secure mobile storage management.

**References**

1. A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung and S. E. Venegas-Andraca, "Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 118-131, March 2020, doi: 10.1109/TNSM.2020.2969863.
2. Sood, S.K. Mobile fog based secure cloud-IoT framework for enterprise multimedia security. Multimed Tools Appl 79, 10717–10732 (2020). https://doi.org/10.1007/s11042-019-08573-2
3. Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., &Buyya, R. (2017). Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. Future Generation Computer Systems, 72, 273-287. https://doi.org/10.1016/j.future.2016.08.018
4. Jung, KD., Moon, SJ. & Kim, JM. Data access control method for multimedia content data sharing and security based on XMDR-DAI in mobile cloud storage. Multimed Tools Appl 76, 19983–19999 (2017). https://doi.org/10.1007/s11042-016-4016-8
5. Shiza Hasan, Muhammad Awais, and Munam Ali Shah. 2018. Full Disk Encryption: A Comparison on Data Management Attributes. In Proceedings of the 2nd International Conference on Information System and Data Mining (ICISDM '18). Association for Computing Machinery, New York, NY, USA, 39–43. https://doi.org/10.1145/3206098.3206118
6. H. Song, J. Li and H. Li, "A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption," in IEEE Access, vol. 9, pp. 63745-63751, 2021, doi: 10.1109/ACCESS.2021.3075340.
7. Usman, M., Ahmad Jan, M., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds.

Information Sciences, 387, 90-102. https://doi.org/10.1016/j.ins.2016.08.059

8. Mohiuddin, I., Almogren, A., Al Qurishi, M., Hassan, M. M., Al Rassan, I., & Fortino, G. (2018). Secure distributed adaptive bin packing algorithm for cloud storage. Future Generation Computer Systems, 90, 307-316. https://doi.org/10.1016/j.future.2018.08.013
9. Cheng, Y., Fu, X., Du, X., Luo, B., &Guizani, M. (2017). A lightweight live memory forensic approach based on hardware virtualization. Information Sciences, 379, 23-41. https://doi.org/10.1016/j.ins.2016.07.019
10. R. Chaudhary, N. Kumar and S. Zeadally, "Network Service Chaining in Fog and Cloud Computing for the 5G Environment: Data Management and Security Challenges," in IEEE Communications Magazine, vol. 55, no. 11, pp. 114-122, Nov. 2017, doi: 10.1109/MCOM.2017.1700102.
11. Altuwaijri, H., &Ghouzali, S. (2020). Android data storage security: A review. Journal of King Saud University - Computer and Information Sciences, 32(5), 543-552. https://doi.org/10.1016/j.jksuci.2018.07.004