International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Critical Data Encryption: A Deep Study

Isha Sharma[1], Raj Thakur[2]

[1,2]Grad Student, Digital Specialists Engineer, Master in Cyber Law and Information Security, National Law Institute University, Bhopal, India

Abstract

This research offers a thorough analysis of critical data encryption with an emphasis on its relevance in the age of massive digital data and persistent cybersecurity risks. It examines a number of vital data encryption-related topics, such as the development of cryptography over time, strategies for safeguarding crucial data, algorithms for encrypting data, key management, physical storage security, and anticipated developments. End-to-end encryption, strong key management procedures, multi-factor authentication, safe data backups, key rotation, audits, security policies, and complying with regulations are all stressed. Strong encryption algorithms like AES are also important. In order to protect vital data from illegal access and fresh risks, the report emphasizes the ongoing need for vigilance and progress in encryption techniques

IndexTerms: Critical Data, Encryption, Key Management, Physical Storage, Security.

1) INTRODUCTION

1.1) WHAT ENCOMPASS CRITICAL DATA?

Power is embodied in data. Corporations possess valuable data resources and enormous amounts of customer data. Critical data, that the corporations consider necessary for its performance or data that needs to be kept for compliance reasons, is one category of these data. User information, particularly private information protected by data protection regulations, is a prime example of critical information. Every organization is required to determine the data it deems essential. Every department has to be active in identifying vital data, so this isn't just an IT choice.

1.2) STATEMENT OF PROBLEM

In an ever-evolving digital environment, this research aims to explore the difficulties associated with critical data encryption while also offering insights and ways to improve the security of essential data through encryption techniques.

1.3) RESEARCH OBJECTIVE

- To comprehend the nature of critical data
- To understand various modes of encrypting and decrypting critical data
- To appreciate key's meaning, generation, management and its distribution
- To find security measures against various attacks
- To be familiar with security management and it trends

1.4) HYPOTHESIS

The safeguarding of critical data in the age of technology is substantially aided by the efficient application and administration of encryption methods, particularly through strong encryption algorithms, appropriate key management processes, and user awareness.

1.5) RESEARCH QUESTION

- What encryption techniques are most successful at securing critical data?
- How can organizations improve their key management procedures to increase the security of their encryption of critical data?
- What steps may be taken to strengthen the physical security of the data stored on a device against unauthorized access?

1.6) RESEARCH METHODOLOGY

The researcher in this research applies the Doctrinal Research. The researcher had gone through numerous research papers and analyzed multiple critical data encryption techniques and various methods to protect the data of critical nature from the possible threats. The researcher has followed the OSCOLA's 4th Edition with minor modification in citation.

1.7) SCOPE AND LIMITATION

Amongst various modes of protecting critical data are available, the researcher has kept the scope limited to the encryption and physical security management. It has also focused on symmetric and asymmetric mode of encryption. Such is done due to paucity of time and word limits. There have been no experiments due to the nature of research being Doctrinal.

2) BACKGROUND

2.1) IN WHAT WAYS CRITICAL DATA IS DEMARCATED?

As an administration tool, critical data could be specified however the business sees fit. Usually, the meaning must include the following:

- Who: Users for whom the data is essential
- Why: the objective that the data fulfills, such as regulation, statistical analysis, or maximizing client satisfaction
- What: the title and location of the data as well as information related to the data
- Where: The data's original source;
- When: The most recent examination of the data's state

Definitions of critical data could shift as time passes. While outdated important data could cease to be useful, novel sources might be crucial. Every firm should ideally have a routine review procedure to maintain its essential data definitions current.

2.2) HISTORICAL OVERVIEW

A CONCISE UNDERSTANDING

Data encryption has its origins in early civilizations, when signals were hidden using unsophisticated techniques. To construct hidden texts, early encryption methods like the Caesar cipher were utilized by

Julius Caesar which required moving letters. These primitive techniques set the groundwork behind the idea of cryptography and the essential ideas that continue to guide contemporary encryption techniques.

The cipher called Vigenère and other advanced encryption algorithms gained popularity around the medieval era. A number of interconnected Caesar ciphers were used to construct polyalphabetic substitution cipher to increase safety, which was an important development in encryption. In the course of instances involving war and scandalous politics, it was necessary to secure critical military and international communications. This led to advancements in cryptography.

Technological advances in processing speed and encryption have accelerated the development of cryptography. The Data Encryption Standard (DES) and its contemporary, the Advanced Encryption Standard (AES), transformed the industry by providing enhanced safety and extensive applicability across several areas. Entrepreneurs such as Martin Hellman introduced public-key cryptography, ushering in a new age that allowed for safe transmission and the exchange of private data without the need for encryption keys

3) MODES OF PROTECTING CRITICAL DATA

A. Access Control: Use access control methods and instruments to limit who has access to information. The least privilege concept (individuals have just the minimum privileges required to complete their activities) and role-based access control (RBAC) are examples of user authentication.

B. Encryption: Information must be transformed to an encrypted format so that it is capable of being read or comprehended only using appropriate decryption key. This makes sure that regardless of whether unauthorized individuals obtain the data, they will not be able to decipher it or utilize it. Asymmetric encryption uses both private as well as public key pairs, whereas symmetric encryption uses a single key for encryption and decryption.

C. Firewalls: Network safety tools called firewalls track and regulate traffic that comes into as well as leaves the network. By screening communications in accordance with pre-established security standards, they may be utilized to prevent unwanted manipulation of sensitive data.

D. Intrusion Detection and Prevention Systems (IDPS): IDPS tools keep an eye on device or network activity for any indications of fraudulent activity or vulnerabilities in security. They are able to spot unusual conduct, provide alerts, and take measures to avoid invasions.

E. Backup and Recovery: Consistently create data backups while maintaining a reliable data restoration strategy in place. This guarantees that data may be retrieved via backups regardless of whether it becomes unavailable due to hardware malfunctions, cyberattacks, or other calamities.

F. Data Masking: Also referred to as information concealment or data anonymization, which includes substituting private data with fictitious or jumbled data yet retaining the layout and arrangement of the original data. When creating and evaluating new software, this is frequently used to secure private information.

G. Physical Security: Guarantee that physical safety measures have been put in effect to safeguard information housed on physical equipment, such as storage and server devices. Secure data centers, entry restrictions, and monitoring are part of this.

H. **Security Awareness and Training:** Train employees and clients on data safety guidelines, such as understanding how to spot phishing scams, create passwords that are secure, and stay away from exposing confidential data.
I. **Multi-factor authentication (MFA):** prior to allowing users access to information or systems, MFA requires users to submit various types of authentication. Usually, this entails a combination of something they are aware of (like a password) and something they own (like a smartphone or protection token).
J. **Security Patching and Updates:** Stay updated with the most recent security patches for programs, platforms, and apps to fix identified risks that might be used by the attackers for exploitation.

4) Encryption Algorithms and Key

In order to turn plain text into cipher text and then back again using both decryption and encryption, a cryptography algorithm is used. A sort of cipher used for data secrecy and consistency in a computer application is the cryptography encryption algorithm. The plaintext is changed into cipher text using an encryption key and transferred through a network, like the Internet, to a location where the recipient will decrypt it.

4.1) The Key: Meaning, generation, management and its distribution

A key is an essential component of information that is employed in cryptography to encrypt and decode data. The development, maintenance, and transmission of keys are crucial components of protecting the accessibility, confidentiality and integrity of confidential information since keys are vital to the security of cryptographic systems.

Here is a summary of important connected ideas and procedures:

A) Key Types:

- **Symmetric Key:** In symmetric cryptography, the encryption and decryption processes use a single key. Although symmetric cryptography is often quicker, safe key distribution is still necessary. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two such examples.
- **Asymmetric Key (Public-Key):** Asymmetric cryptography makes use of sets of keys—a public key for encryption and a private key for decryption. Private keys have to be kept confidential, but public keys can be freely shared. RSA and ECC (Elliptic Curve Cryptography) are two examples.

B) Key Generation:

- **Symmetric Key Generation:** Randomly generated numbers are frequently used to produce symmetric keys. The key's integrity depends on the level of randomization. Keys must be sufficiently lengthy to withstand brute-force attacks.
- **Asymmetric Key Pair Generation:** Mathematical procedures are used to produce asymmetric key pairs. The matching public key is obtained from the private key, which is kept confidential.

C) Effective Key Management practices:

- **Backup:** Critical keys should always be backed up to avoid data from being lost in the event of key destruction or damage. Backup keys need to be kept in a safe place.

- **Access Control:** To limit key access to authorized people exclusively, strong access control measures must be in force.
- **Storage:** Keys, in particular private keys, have to be kept in an appropriate place. Keys are shielded from unwanted access with the use of hardware security modules (HSMs) and secure key storage systems.
- **Rotation:** To reduce dangers related to prolonged usage, keys ought to be turned on a regular basis. Outdated keys are deleted or securely preserved while new ones are produced.
- **Key Versioning:** It's crucial for safety to maintain track of key versions and make sure that outdated keys are substituted with more recent ones.

D) Key Distribution:

- **Symmetric Key Distribution:** It might be difficult to distribute symmetric keys safely. Key distribution centers (KDCs), Diffie-Hellman key exchange, and secure channels are a few examples of techniques.
- **Asymetric Key Distribution:** Since public keys cannot be kept hidden, they may be freely circulated. To stop attacks involving people in between, it is essential to ensure the validity of public keys.

- **KEY REVOCATION**: Programs should cease utilizing a key if it has been leaked or is not further required.
- **KEY EXCHANGE PROTOCOLS**: Cryptographic protocols like IPsec, TLS/SSL, and SSH offer ways to exchange keys safely across secure connections.
- **KEY LIFECYCLE MANAGEMENT**: A defined key lifetime must be established, from generation to retirement, in order to effectively manage keys.

5) CRYPTOGRAPHY AND ITS TYPES

The study and application of ways for protecting interactions, data, and information in a manner that is unintelligible by outsiders is known as cryptography. It uses codes to safeguard data and messages so that only the intended audience is able to comprehend it.

Symmetric key encryption, asymmetric key encryption, and public-key encryption are the three basic subcategories of cryptography.

A. Symmetric key encryption employs a single key for both the encryption and decryption. Both sides are required to maintain the secrecy of the keys utilized for this sort of encryption, leaving them open to attackers. Public key systems most frequently employ symmetric keys.

B. Asymmetric key encryption: In this method, a pair of keys are used in rather than one. For encryption and decryption, separate keys are employed. Since they may be used more than once and are utilized just once per communication, these keys are not required to be kept confidential. Public-key systems are frequently employed with asymmetric keys.

C. Public-key encryption: Public-key systems employ two mathematically connected keys that are unable to be deduced from one another without knowledge of the other keys (a method referred to as factoring). As a result, regardless of whether someone discovers your private key, they may only be able to generate your public key (and vice versa).

6) TECHNIQUES USED FOR CRYPTOGRAPHY

The most commonly used techniques in cryptography are Symmetric Key Cryptography, Asymmetric Key Cryptography, Hashing, Secret Sharing, Digital Signatures, Elliptic Curve Cryptography, Quantum Cryptography, Steganography, Zero-Knowledge Proofs, Homomorphic Encryption.[1]

A. SYMMETRIC KEY CRYPTOGRAPHY

The same key is used by the symmetric encryption technique to encode and decode data. A pre-shared secret key must be held between the sender and the recipient of the communication in order to convert plaintext into encrypted text and vice versa.

For instance, in order to avoid malevolent parties from prying into their communications, Ram and Shyam must share one encryption key in order for Ram to send Shyam a straightforward message. If Ram encrypts the text "I am right" with a particular substitution cipher, Shyam will need to be informed of the substitution shift in order to decipher the text once it has reached Shyam.

WHERE IS SYMMETRIC KEY CRYPTOGRAPHY USED?

The full procedure will be summarized as follows:

Step 1: Ram and Shyam choose a shared key in the first step.

Step 2: Ram gives the private encryption key, or the other way around.

Ram encrypts the original text in step 3 using the secret key.

Step 5: Shyam uses the private key to decipher the text that was previously with Shyam

Step 4: Ram transmits the encrypted message to Shyam.

By using the aforementioned procedure, Ram and Shyam may speak confidentially without worrying about onlookers on the trip. No outsider who has accessed the plain text that has been encrypted can decipher it as only the two of them know the secret key required to encrypt and decode it.

From secure surfing to banking apps, symmetric encryption is crucial in numerous everyday online transactions. Here are a few of these functions:

Applications-Symmetric_Encryption.

- **Payment Software:**

prior to completing their operations, most financial services and payment apps need verification of personally identifying information. It aids in foretelling the appropriate data to stop fraud and criminality.

- **Securing Data at Rest:**

Symmetric encryption is used to secure private data that a company or website keeps about its users or about the organization themselves. This is carried out to stop any spying carried out by external hackers or irate workers within the business who could be attempting to obtain crucial data.

- **SSL/TLS Handshake:**

Private information that a business or site maintains concerning its customers or regarding the firm itself is protected using symmetric encryption. This is done to prevent any surveillance by external or furious

[1] This research restrictively focus on Symmetric Key Cryptography, Asymmetric Key Cryptography.

within employees who could be trying to get their hands on important data.

TYPES OF CIPHERS BEING USED IN SYMMETRIC ALGORITHMS

Stream Ciphers and Block Ciphers are the two types of ciphers can be used in symmetric algorithms.

1. Stream Ciphers

Algorithms that encrypt fundamental data one byte or bit at a moment are known as stream ciphers. You generate a binary key using a bit stream creation process, then you encrypt the plain text with it.
Following are the steps involved in employing stream ciphers for encryption and decryption:

- Obtain the encryption of the plaintext.
- Use the bit stream creation technique to produce a binary key.
- Using the created binary key as an XOR operation, combine the plaintext with the key.
- The encrypted text is produced as the result.
- Use the same key to perform XOR operations on the encrypted text to recover the plaintext.

The three most used stream ciphers are PANAMA, SALSA, and RC-4.**Block Ciphers**

Block ciphers work on and encrypt data in fixed-size blocks that are either 64 or 128 bits in size. Typical block ciphers are:

1.1 Data Encryption Standard (DES):

Data Encryption Standard (DES), a symmetric-key block cipher algorithm, was once a popular choice for secure data encryption and decryption. DES, which was created by IBM in the 1970s and subsequently approved by the US government as a federal standard, was a key component of that era's security framework for electronic communications and data
The essential qualities and traits of DES are listed below:

- **Block Cipher:** As a block cipher, DES processes data in discrete, fixed-size blocks. Each block in the case of DES is 64 bits (8 bytes) long.
- **Key Length:** A 56-bit key is used by DES. The other 8 bits are utilized for parity checks rather than real encryption, hence the accurate key length is instead thought to be 56 bits. DES is no longer regarded as safe against contemporary computer powers due to its comparatively low key length, which renders it susceptible to brute-force assaults.
- **Substitution-Permutation Network:** A substitution-permutation network (SPN) is a sophisticated structure that is used by DES to convert a plain text block into an encrypted output block. This network is made up of several rounds of mutation and swap operations.
- **Fixed Number of Rounds:** For every information block, DES uses 16 rounds of encryption. Bitwise operations like substitution (S-boxes), permutation (P-boxes), and bitwise XOR operations are combined in each round.
- **Security:** The 56-bit key space has been subjected to comprehensive assaults (brute force) thanks to improvements in computer power over time. Due to this growing vulnerability, Triple DES (3DES) and the Advanced Encryption Standard (AES) were introduced to take the role of DES. In order to increase security, these more recent algorithms employ longer key lengths and more intricate architectures.

- **Legacy Usage:** For new cryptographic programs, DES ought not to be utilized because it is regarded as being outdated. It is still used in older technologies, thus it should be upgraded wherever feasible with a more robust method.

1.2 Triple DES (3DES):

The symmetric-key block cipher technique known as Triple DES, or 3DES, was created as an improvement and extension to the original Data Encryption Standard (DES). Triple Data Encryption Algorithm (TDEA) or Triple DEA are other names for 3DES.

These are Triple DES's salient qualities and traits:

- **Block Cipher:** Similar to DES, Triple DES operates on data in fixed-size blocks as a block cipher. Every block has a length of 64 bits, or 8 bytes.
- **Key Length:** Triple DES keys are used in the Triple DES encryption method, which encrypts data with the initial key, decrypts it using the subsequent key, and then re-encrypts it with the final key. Each key is 56 bits long, for a total key length of 168 bits (56 bits multiplied by 3).
- **Multiple Rounds:** Triple DES uses a particular sequence to repeatedly apply the DES algorithm. EDE (Encrypt-Decrypt-Encrypt), commonly referred to as 3TDEA, is among the most popular method of operation. In this method, the initial key is used to initially encrypt data, the subsequent key is utilized to decrypt it, and the final key to re-encrypt it. 48 rounds are normally required for this process—16 rounds for each of the three DES processes.
- **Security:** Given its higher key length compared to the original DES, Triple DES provides much more protection. It is substantially less susceptible to brute-force assaults than ordinary DES because to its 168-bit effective key length. However, it is important to keep in mind that when compared to more recent encryption techniques like the Advanced Encryption Standard (AES), 3DES is regarded as being rather sluggish and less safe.
- **Legacy Usage:** Although 3DES is thought to be more reliable than DES, it has stopped being seen to be cutting edge. Better security and performance are provided by contemporary encryption technologies like AES. However, 3DES is still employed in some legacy applications as well as systems where better encryption is impractical or when backward compatibility with previous systems is necessary.

1.3 Advanced Encryption Standard (AES):

The Advanced Encryption Standard, sometimes known as AES, is a popular symmetric-key block cipher method for the safe encryption and decryption of data. It is regarded as one of the many reliable and effective encryption algorithms currently in use. The Data Encryption Standard (DES), which was out of date, was replaced by AES as a standard by the U.S. National Institute of Standards and Technology (NIST) in 2001.

The main traits and qualities of AES are listed below:

- **Block Cipher:** AES works with data blocks of a defined size since it is a block cipher. AES processes data in 128-bit (16-byte) chunks.
- **Key Lengths:** AES provides keys with lengths ranging from 128 bits to 256 bits. The security of the encryption is directly impacted by the key length. Longer keys offer more security but need more computing power.

- **Rounds:** AES uses a sequence of rounds to process data. There are 10 rounds for AES-128, 12 rounds for AES-192, and 14 rounds for AES-256, depending on the length of the key. A number of mathematical operations are performed throughout each round, including key mixing (AddRoundKey), permutation (ShiftRows and MixColumns), and substitution (S-box).
- **Security:** AES has resisted intensive cryptanalysis and is renowned for its security. The difficulty of AES's mathematical operations and the key length determine how secure it is. For the majority of applications, AES-128 is regarded as safe, and AES-192 and AES-256 offer even greater degrees of security.
- **Efficiency:** AES is built with computational efficiency in mind and is hardware-optimized for current computing platforms. Secure communications, data encryption at rest (such as disk encryption), and secure data movement over the internet (such as in protocols like TLS and VPNs) are just a few of the many areas where it is utilized.
- **Standardization:** AES is a global standard that has been embraced by businesses, organizations, and governments all across the world. Its uniformity has helped it become widely used and accepted.

7. PHYSICAL STORAGE OF CRITICAL DATA ENCRYPTION

Critical data physical storage Cryptography is the process of using encryption methods to protect data that is kept on computers or hardware. The objective is to safeguard information against theft, loss, or illegal access to the storage device or server. The following techniques can be used to improve the physical storage safety of data on computers or machines:

Full Disk Encryption (FDE):

- Encrypt Entire Drives: This makes sure that all data on the disk is encrypted automatically and that decryption only takes place when a device has been properly validated.
- Use Trusted Encryption Solutions: To manage encryption keys and safeguard data at rest, use trusted encryption software or hardware solutions like BitLocker (for Windows), FileVault (for macOS), or hardware security modules (HSMs).

1. Data-at-Rest Encryption:

- Selective Encryption: Rather of encrypting the whole disk, just certain documents, folders, or drives holding vital information should be encrypted. This method gives precise control over the encryption.
- Strong Key Protection: Keep encryption keys safe by using hardware security modules (HSMs) and maintain them independently from information
- Implement key rotation procedures to replace encryption keys on a regular basis. The danger of long-term key exposure is reduced as a result.

2. Access Control and Authentication:

- Physical Access Control: Limit access to servers and storage devices physically by using closed server rooms, biometric or card-based access control systems, and security cameras.
- Secure Boot: Enable secure boot procedures on servers to make certain only highly trustworthy and authorized software can be used, decreasing the possibility of unwanted access to data.

- Multi-Factor Authentication (MFA): Utilize MFA to access sensitive data, which requires more authentication than just a username and password.

3. **Secure Disposal:**

- Data Erasure: To make certain that no confidential information is left behind when dismantling storage devices or servers, use reliable information erasure techniques. Use specialist software or services for data erasure.
- Physical Destruction: To avoid recovery of data, physically demolish servers or storage devices that are no longer in use and contain sensitive data.

8. SECURITY MANAGEMENT AND FUTURE TREND

According to the corporation's unique requirements and circumstances, along with the type of data that needs securing, encryption may be the most effective solution for protecting sensitive information. However, some recommendations and factors for using encryption to safeguard important data include:

1. **Use Strong Encryption Algorithms**: Employ powerful encryption algorithms Use encryption techniques with strong, well-tested key lengths, such as AES (Advanced Encryption Standard). Avoid use old or insecure encryption techniques.
2. **Implement End-to-End Encryption:** Use end-to-end encryption to make sure that data is encrypted from the source to the destination while it is in transit. This is crucial for private information transfers and conversations.
3. **Implement strong key management practices**: Use sound key management procedures to safeguard encryption keys. Use secure key management tools or keep keys in encrypted computer modules.
4. **Multi-Factor Authentication (MFA):** Apply MFA to get access to systems, apps, and data repositories. By doing this, additional protection is added to guarantee that only people with permission may access sensitive data.
5. **Secure Data Backups**: Make sure that crucial data copies of backups are encrypted. Backup data should be safely stored, preferably elsewhere or in a different secure data location.
6. **Regular Key Rotation**: Establish key rotation procedures on an ongoing basis to replace encryption keys. Continuous key risk of exposure is decreased as a result.
7. **Auditing and Monitoring:** Establish monitoring and auditing procedures to monitor encrypted data access and identify unwanted or suspicious activity.
8. **Security Policies and Training:** Create and implement security and encryption rules inside your company. Employees should get frequent security standards training.
9. **Compliance with Regulations:** Verify that the encryption procedures comply with all applicable confidentiality laws and legal obligations, including the GDPR, HIPAA, and any industry-specific standards.

9. FUTURE TRENDS

Regarding data encryption trends in the future, a number of significant developments are anticipated to influence the market:

1. **Homomorphic Encryption :** This type of encryption enables processing of information even though it is still encrypted. With the ability to enable safe computing on encrypted data, this cutting-edge technology presents fresh opportunities for secure data analytics and compute outsourcing.
2. **Cloud-Based Encryption Services:** To make encryption installation and upkeep in cloud settings simpler, organizations are turning more frequently to cloud-based encryption services and key management tools.
3. **Zero Trust Architecture**: Regularly authentication, least privilege access, and micro-segmentation are three zero trust security concepts that are gaining popularity. An important part of these designs is encryption.
4. **Data-Centric Security:** Corporations are concentrating on securing the data themselves through strategies like data masking, tokenization, and dynamic data protection instead of just relying on exterior defenses.

10. Conclusion and Suggestion

The security of critical data is now crucial for both companies and people in an age characterised by the explosion of digital data and ongoing risk of cyber attacks. This paper has illuminated the numerous parts of crucial data encryption by delving into the complex worlds of cryptography and network security. Critical data encryption's relevance does not lessen as technology develops. To protect the security, integrity, and availability of their utmost sensitive data, companies and people must remain up to date on new encryption trends and best practices.

For the same various techniques and procedures like use of strong, well-vetted encryption algorithms like AES (Advanced Encryption Standard) with appropriate key lengths, end-to-end encryption for data in transit to ensure that it remains encrypted from the source to the destination, strong key management practices, multi-Factor Authentication, Secure Data Backups, Regular Key Rotation, Auditing and Monitoring, Security Policies and Training must be undertaken. By implementing these suggestions and continuously improving encryption practices, enhancement of the security of critical data and better protect it from unauthorized access and potential threats can be ensured.