International Conference on Advances in Management & Technology (ICAMT- March 2025)

RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of Data Security and Privacy in Healthcare

Manisha M. Chawale [1], Dr. Manish L. Jivtode[2]

[1] Department of Computer Science, SSESA's Science College,Congress Nagar,Nagpur.

[2] Department of Computer Science, Janata Mahavidyalaya, Chandrapur

ABSTRACTThis paper reviews the analysis of data security and privacy concerning various cryptographic techniques, emphasizing their applicability and importance, particularly in maintaining patient confidentiality in healthcare. It examines algorithms such as DES, 3DES, AES, Blowfish, RSA, and ECC, highlighting their role in encrypting and decrypting medical data. The research identifies significant challenges researchers face in protecting sensitive patient information from misuse and leakage. It compares symmetric algorithms like AES, DES, and 3DES with asymmetric algorithms like RSA and ECC, along with emerging techniques like homomorphic encryption. The study evaluates the role of encryption in healthcare, aiming to address security issues in the healthcare system and propose potential solutions. Kewords— Big Data Security, Privacy Electronic Health Records.Cryptography,AES,DES, 3DES,RSA, ECC,2FA,Homomorphic Encryption.

INTRODUCTION:

Big data is utilized to predict diseases before they arise by analyzing medical records. Many public health systems globally are now implementing electronic patient records and advanced medical imaging. This approach enables healthcare establishments to address future market needs and trends. Big data offers significant opportunities for epidemiologists, physicians, and health policy experts to make informed decisions that enhance patient care. Medical data, characterized by its volume, rapid growth, diverse structures, and high value, is a crucial type of big data. The effective collection, management, and analysis of this extensive medical information are vital for uncovering its potential benefits [1] Medical information is a significant type of big data characterized by its vastness, rapid growth, diverse structure, and high application value. Handling and analyzing large amounts of medical data facilitate advancements in clinical research, health management, and public health, but also raise privacy concerns globally. Over 24 million patient records from different countries are now easily accessible online, containing sensitive personal and medical details such as names, dates of birth, examination dates, and test results. The compromised data poses risks, including potential reputational harm, phishing, and social engineering efforts, as well as automated processing to extract valuable identities. [2]. Triple Data Encryption Standard (3DES) is derived from the original Data Encryption Standard (DES) and was developed in the mid-1970s with a 56-bit key. While 3DES offers strong security, its effective strength is only 112 bits due to vulnerabilities such as meet-in-the-middle attacks. The encryption process is slower than DES, but when used correctly, it provides significantly enhanced security. The encryption and decryption process involves three steps: encryption with the first key, decryption with the second key, and encryption with a third key [3].

2. OVERVIEW OF CRYPTOGRAPHY:

Cryptography is a method of protecting information by converting it into an unreadable form, preventing unauthorized access. It involves transforming plain data into cipher text using cryptographic techniques and a specific key, a process known as Encryption. The receiver uses the known key to convert the cipher text back to plain text, which is referred to as Decryption. shown in following Figure 1[4].

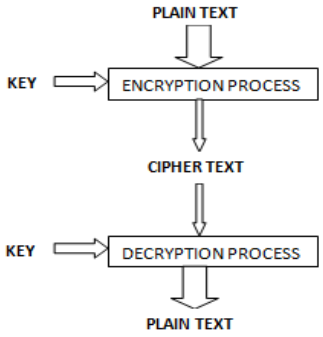

Figure 1 : Process of Cryptography

2.1 AES (Advanced Encryption Standard)

AES, or Advanced Encryption Standard, was developed by Vincent Rijmen and Joan Daeman in 2001 after NIST aimed to improve upon the weaknesses of DES. It is a symmetric encryption algorithm that comes in three variants: AES-128, AES-192, and AES-256, which correspond to key sizes of 128, 192, and 256 bits, respectively. The number of rounds for encryption varies by key size, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The AES process involves the use of round keys, which are applied to perform mathematical operations on data formatted in specific block sizes [5]**.**

2.2 AES AND RSA ALGORITHM:

The AES algorithm employs different key lengths that undergo varying rounds of encryption: 10 rounds for a 128-bit key, 12 for a 192-bit key, and 14 for a 256-bit key, making it nearly impossible to crack with brute-force methods using present-day computing power. However, decryption can be slowed down due to the need for distinct codes and tables during the process. The AES algorithm has limitations, including related key attacks, where hackers analyze information to reverse engineer the cryptographic system, and known-key attacks, which occur when an attacker is aware of the keys utilized in the cipher[6] . The text discusses the encryption of data at rest using AES or RSA algorithms, with AES being applied to Electronic Health Record databases. It emphasizes the need for data protection in all phases: data in action (moving across networks), data in use (frequently updated), and data at rest. [7]

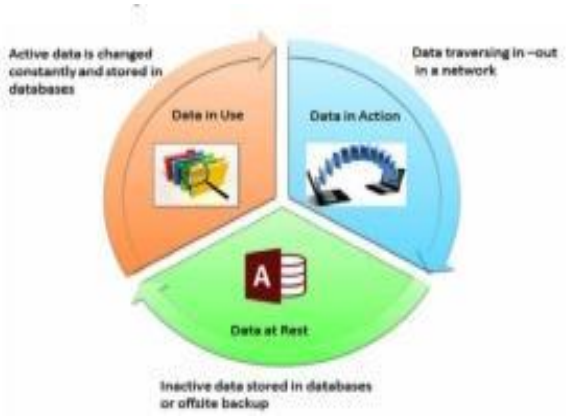

Figure 2:Data in three phases

Data security is crucial for protecting digital information from unauthorized access. Implementing hardware device security for long-term storage helps prevent attacks by malicious users. The security system verifies user identity through a process that involves examining user evidence. Authentication checks the validity of the user's claimed identity. Encryption encodes information, making it accessible only to authorized parties, and involves generating a pseudo-random encryption key. Two main types of encryption used are symmetric and asymmetric encryption[8]RSA is a public key encryption technique, notable as the first algorithm in public-key cryptography and a significant achievement in this field. It consists of three main steps: key generation, encryption, and decryption[9].

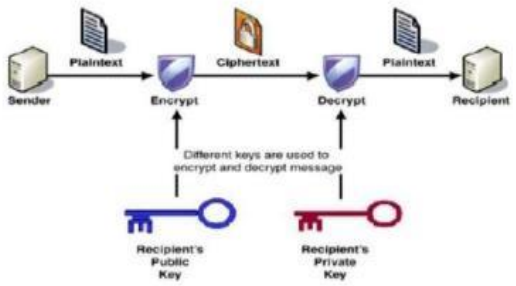

Figure3.RSA Technique

Phase 1: Key Generation

Phase 1 of RSA involves key generation using two keys: a public key for encryption and a private key for decryption. The steps include selecting two distinct large prime numbers P and Q, calculating N as the product of P and Q, and computing z as (P-1)*(Q-1). A public exponent E is then chosen such that it is greater than 1 and less than z, with no common divisors with z. Finally, D is determined to satisfy the relation E*D = 1 (mod z). The resulting keys are the public key (E, N) and the private key (D, N).

Phase 2: Encryption

Phase 2 of encryption involves converting plain text into cipher text using a key and an encryption algorithm. The encryption takes place on the sender's side, utilizing the equation C = M ^ E mod (N), where C represents the cipher text and M represents the plain text or message.

Phase 3: Decryption

Decryption involves transforming Cipher Text back into Plain Text using a decryption algorithm and a key. This process takes place on the receiver's end and utilizes the equation M = C ^ D mod (N) to decrypt the message

2.3 DES/Triple Data EncryptionStandard (3DES) :

Triple Data Encryption Standard (3DES) is an enhancement of the original Data Encryption Standard (DES), developed in the mid-1970s and using a 56-bit key. While it offers enhanced security, effectively providing 112 bits of protection due to vulnerabilities like meet-in-the-middle attacks, it operates three times slower than DES. The process for decryption mirrors the encryption method but is performed in reverse. 3DES utilizes three iterations of the standard DES algorithm and employs a 168-bit key divided into three 56-bit keys [10] 3DES, while providing greater security than DES, effectively offers only 112 bits due to potential meet-in-the-middle attacks and operates slower than DES. The encryption process is performed at the sender's end, where plaintext is encoded using a key to generate ciphertext. 3DES uses a 168-bit key split into three 56-bit keys, involving two encryption and one decryption step. The ciphertext can only be decrypted by those possessing the correct key, allowing them to recover the original data.Fig. 4. Illustration of an encryption and decryption process [11].

Triple Data Encryption Standard Algorithm: Triple Data Encryption Standard (3DES) is a symmetric-key block cipher developed by the National Institute of Standards and Technology (NIST). It enhances the original Data Encryption Standard (DES) by applying the DES algorithm three times to each data block, using three separate 56-bit keys (K1, K2, K3). This method offers greater security compared to both RSA and DES, addressing the vulnerabilities of DES's shorter key length in the context of modern cryptographic attacks. By encrypting and decrypting data three times with different keys, 3DES significantly reduces the risk of unauthorized access [12]. The study proposes the 3DES method to enhance the security of large healthcare data in cloud computing. It involves

two phases: first, selecting the healthcare data as input, and second, processing this data using 3DES for encryption. 3DES is a popular encryption method that provides strong security using key lengths of 112 or 168 bits. After encryption, the data is stored in cloud environments, and the decryption process to access the data uses the

Same 3DES method[13].

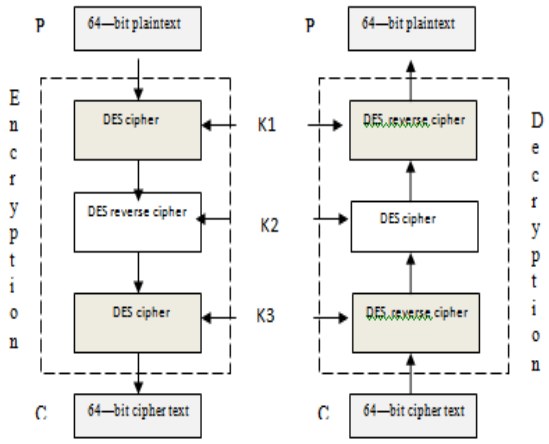

Figure4: Encryption And Decryption Process in 3DES

2.4 Elliptic Curve Cryptography (ECC) Elliptic Curve Cryptography (ECC) is a form of public key cryptography that has gained popularity as a security solution for wireless networks due to its small key size and low computational requirements. A key of 160 bits in ECC is considered to provide security equivalent to a 1024-bit key in RSA ECC offers security comparable to RSA but uses smaller key sizes, enhancing efficiency for mobile and low-power healthcare devices. AES, the latest approved encryption standard, operates with key sizes of 128, 196, and 256 bits, and can be faster than DES. While RSA provides scalable security based on key size, its performance is slower than the three symmetric key algorithms mentioned [14].ECC's asymmetric encryption protects patient data during transmission, while SHA-256 hashing ensures the integrity of stored information. Combining ECC, SHA-256, and multi-authority models enables the enforcement of fine-grained access policies for controlled sharing of patient data among authorized parties. [15].

2.5 BlofishEncryption and Decryption Algorithm: Blowfish is a symmetric-key cryptographic algorithm created by Bruce Schneier in 1993. It is a 64-bit symmetric block cipher that encrypts input in blocks and uses the same key for both encryption and decryption, with key lengths ranging from 32 bits to 448 bits. While it is faster than Triple DES, it is not as fast or efficient as AES. The main processes involved are data encryption and key expansion [16]. The bloated fish algorithm is a symmetric block encryption algorithm designed as a fast alternative to RSA. It consists of two main components: key expansion and data encryption. The algorithm encrypts data using a block encryption method that divides text into 64-bit blocks. It supports variable key lengths from 32 bits to 448 bits, allowing for flexible security in image encryption. The algorithm employs an innovative transformation process that divides the image into random blocks, enhancing the protection level of the encrypted image through various processing and encryption techniques. [17]. The Blowfish algorithm is noted for its efficiency in low power consumption and security, and it is publicly available. In contrast, other encryption algorithms are partially available or kept secret by governments. This makes Blowfish a suitable choice for implementation in ARM-based Wearable Medical Devices for improved performance [18].

2.6 Two-factor authentication(2FA)

Two-factor authentication enhances security by requiring two methods to verify a user's identity, making it harder for cyber criminals to access devices or accounts. This two-step verification process addresses the limitations of traditional username and password systems and has become increasingly popular globally to protect millions of users and assets from cyber-attacks [19]. A Personal Health Record (PHR) is a health record managed by patients that maintains their health data. Its purpose is to provide an accurate summary while securing sensitive information through two levels of authentication. PHRs are stored on third-party servers, which raises privacy concerns. To address this issue, it is recommended to encrypt PHR files before uploading them to the cloud. Additionally, challenges such as scalable key management and access control exist. To improve scalability, multiple security domains (public and personal) are introduced, allowing for differentiated access privileges based on roles and data attributes. This approach enhances privacy preservation through effective key distribution[20]. Research on the usability of two-factor authentication (2FA) has focused on identifying the best applications and their structure. Studies examine aspects such as response times, ease of setup, and user complexity. Notably, 2FA is increasingly important in areas with heightened security concerns. The forensic investigation of fifteen 2FA applications involved four main phases: scenario creation and testing, data acquisition, data analysis, and 2FA bypass[21].

2.7HomoeopathicEncryption:

Homomorphic encryption technology offers a solution for protecting the privacy of cloud-based electronic medical records by allowing computations on encrypted data without the need for decryption. This approach ensures privacy during data processing and effectively prevents data leakage from malicious attacks through the localization of user keys. Additionally, the study introduces a hybrid encryption scheme and a method for ciphertext digest-based searching and statistics to minimize the computational load associated with decrypting all electronic medical records [22]. The rise of big data in health research and personalized medicine has resulted in hospitals and healthcare institutions increasingly collecting data. As a result, ensuring patient privacy, especially in data sharing between these entities, has become a major concern. Currently, it is uncertain whether the GDPR allows for general or broad consent for research projects [23]. Homomorphic Encryption, introduced by Gentry in 2009, represents a major advancement in cryptographic technology. It significantly increases the generation of public and private keys during encryption in the errors setting. This technique is crucial for preserving privacy and has extensive applications in data protection, query processing, and secure data aggregation. As privacy concerns escalate in the digital age, Homomorphic Encryption provides an effective means of protecting both personal and enterprise data, especially in query processing and secure data aggregation. [24]. The text discusses the use of Fully Homomorphic Encryption (FHE) for performing queries and analytics on a privacy-preserving patient-location database. It specifically utilizes the ElGamal algorithm from FHE methods. The proposed approach is simulated to demonstrate its accuracy and effectiveness in identifying potential patient contacts based on queries. Notably, this method allows computations on encrypted data without decryption, a feature lacking in current public-health surveillance systems[25]

Summaryof Algorithm Comparison in Healthcare:

SR.NO	Algorithm	Type	Key Size	Secur	Performance	Efficiency	Healthcar Use
				iy			

1.	**AES**	Symmetric	128, 192, 256 bit	Very high	Fast	Fast, efficient	EHR encryption, medical devices, HIPAA
2.	**RSA**	Asymmetric	1024-4096 bits	Slow	Slow	Slow, computationally heavy	Secure transmission, authentication
3.	**DES/ 3DES**	Symmetric	56 (DES), 168 (3DES	Slow	Slow	Slower than AES	Older systems, legacy encryption
4.	**ECC**	Asymmetric	256, 384, 521 bit	Very fast	Very fast	More efficient than RSA	Mobile health apps, authentication
5.	**Blowfish**	Symmetric	32-448 bits	Fast	Fast	Faster than 3DES, less efficient than AES	Lower-power systems, legacy apps
6.	**2FA**	Symmetric	128, 192, 256 bit	High	Moderate	Minimal impact	User authentication, access control
7.	**Homomorphic Encryption**	Advanced	Varies	Very high	Very slow	Computationally heavy	Cloud-based analytics, privacy-preserving computations

Table1: Summary Comparison Table of Encryption Algorithms for Healthcare

4.CONCLUSION:

AES is the preferred choice for general-purpose encryption in healthcare due to its speed, security, and compliance with standards like HIPAA.**RSA** and **ECC** are excellent for secure communication and digital signatures but are less efficient than AES.**3DES** and **Blowfish** are outdated and should be avoided in modern healthcare applications.**Homomorphic Encryption** is a promising emerging technology that could revolutionize.privacy-preserving computations but is not yet widely deployed due to efficiency challenges.**2FA** and **tokenization** complement encryption by enhancing access control and further securing patient data. The choice of encryption algorithm depends on use cases, regulatory requirements, and system architecture. AES and ECC are recommended based on specific applications, Researchers are also exploring the potential of homomorphic encryption for next-generation privacy-preserving solutions in healthcare. The focus is on identifying algorithms that meet performance and security needs while complying with legal and regulatory standards such as HIPAA and GDPR.

REFERENCES

[1].Senthilkumar , Bharatendara K Rai, Amruta Gunasekaran,Chandrakumarmangalam " Big Data in Healthcare Management: A Review of Literature", American Journal of Theoretical and Applied Business 2018; 4(2)

[2]. Gaurav Dhiman , SapnaJuneja , HamidrezaMohafez 4 , Ibrahim El-Bayoumy , Lokesh

Kumar Sharma 6," Federated Learning Approach to Protect Healthcare Data overBig Data Scenario" Sustainability 2022, 14, 2500. https://doi.org/10.3390/su14052500, https://www.mdpi.com/journal/sustainability

[3]. BABATUNDE, A.O.1, TAIWO, A. J.1, DADA, E. G.2 "Information Security In Health Care Centre Using Cryptography And Steganography".

[4].Pooja Singh, R.K. Chauhan "A Survey on Comparisons of Cryptographic Algorithms Using:"CertainParameters in WSN"International Journal of Electrical and Computer Engineering (IJECE)Vol. 7, No. 4, August 2017, pp. 2232~2240 ISSN: 2088-8708, homepage:http://iaesjournal.com/online/index.php/IJECE

[5]Agnes K. Muthaura1 & John Kandiri "Data Protection in Healthcare Information Systems Using Cryptographic Algorithm with Base64 512 bits" 2958-7999, Vol. 4 (2) 2024

https://doi.org/10.62049/jkncu.v4i2.10

[6] Shraddha M. Dudhani1, Santosh S. Lomte2 " Performance Analysis of Data Encryption Algorithms for Secure EHR Transmission" DOI: https://doi.org/10.26438/ijcse/v7i2.363366 | Available online at: www.ijcseonline.org Accepted: 16/Feb/2019, Published: 28/Feb/2019

[7]MuralikrishnaIyyanki "Cryptography in the Healthcare Sector With Modernized Cyber Security"K. G. Reddy College of Engineering and Technology, Hyderabad, India DOI: 10.4018/978-1-7998-2253-0.ch008.

[8]XueyingZhang,etal.,"Energy efficiency of encryption schemes applied to wireless sensor networks", Security and Communication Networks, John Wiley & Sons, Ltd., 2011

[9]Prof.Dr.Alaa Hussein Al-Hamami and IbrahemAbdallahAldarisehalaa_hamami@yahoo.com ibrahem_aldariseh@yahoo.com "Enhanced Method for RSA Cryptosystem Algorithm"2012 International Conference on Advanced Computer Science Applications and Technologies978-0-7695-4959-0/13 $25.00 © 2013 IEEE DOI 10.1109/ACSAT.2012.102.

[10]Ajinkya Dongare, Suchitra Theurkar, Manjushri Sonkamble, Varsha Rodge, Mr. Ramkrushna Maheshwar "Enabling Authorized Encrypted Search for Multi-Authority Medical Databases using 3DES" International Journal for Research in Applied Science & Engineering Technology (IJRASET)ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue VII July 2020

[11]Kazeem B. Adedeji, Nnamdi, Nwulu, Clinton Aigbavboa and Saheed L. Gbadamosi

"Assessment of Encryption and Decryption Schemes for Secure Data Transmission in Healthcare Systems"July 25,2020 at 19:20:50 UTC from IEEE Xplore.

[12] Dr. S. Sadesh,Narmatha M ,Sakthidharanya P. R,Naveen G "Enhancing Security Mechanism in Healthcare using Triple DES"International Journal of Engineering Research & Technology (IJERT)ISSN: 2278-0181 Published by, www.ijert.org RTICCT - 2020.

[13] WidAkeel Awadh, Mohammed S. Hashim, Ali Salah Alasady Department of Computer Information Systems, University of Basrah " Implementing the Triple-Data Encryption Standard for Secure and Efficient Healthcare Data Storage in Cloud Computing Environments" https://doi.org/10.31449/inf.v48i6.5641 Informatica**48** (2024) 173-184 **173**

[14]YoungsilLee,EskoAlasaarela, HoonJaeLee "Secure Key management Scheme based on ECC algorithm for Patient's Medical Information in Healthcare System"978-1-4799-3689-2/14/$31.00 ©2014 IEEE.

[15].Ensteih Silvia1, Mohd Tajuddin1 "E-Health Privacy and Security through ECC, SHA-25 and Multi-Authority Approaches"JOURNAL OF Information Technology and Cryptography Double Blind Peer Reviewed Journal DOI: https://doi.org/10.48001/JoITC ,Volume-1, Issue-1, Jan-Jun-2024.

[16]NoahOluwatobiAkande,ChristianaOluwakemiAbikoye "Electronic Medical Information Encryption Using Modified Blowfish Algorithm",Springer Nature Switzerland AG 2019S. Misra et al. (Eds.): ICCSA 2019, LNCS 11623, pp. 166–179, 2019.

https://doi.org/10.1007/978-3-030-24308-1_14.

[17]Amandeep Kaur ,Gurjeet Singh Assistant Proffesor "A Random Selective Block Encryption Technique for Secure Image CryptographyUsingBlowfishagorithm",978-1-5386-1974-2/18/$31.00 ©2018 IEEE.

[20]. R. RaghulVaikundam, D. Sangeetha,V. Vaidehi,R.Srinandhakumar,V.SubhashIgnatius,"A Cloud based Two Layered Access Control with Decentralized Anonymous Authentication in Health Care"978-1-7281-0353-2/18/$31.00 ©2018 IEEE.

[21].Jessica Berrios a, Elias Mosher a , Sankofa Benzo a , CinthyaGrajeda a , Ibrahim Baggili

"Factorizing 2FA: Forensic analysis of two-factor authentication applications"Volume 45, Supplement,July2023,301569,https://doi.org/10.1016/j.fsidi.2023.301569

[22]. Liaoran Xu; Chenyang Zhao; Weili Jiang; Jun Ye; Yan Zhao; Zhengqi Zhang "Secure Encryption Scheme for Medical Data based on Homomorphic

m IEEE Xplore.

"IEEE *Xplore*: 22 September 2023DOI:10.1109/ICDSNS58469.2023.10245348.

[23] James Scheibner, Marcello Ienca1 and Efy Vayena1,"Health data privacy through homomorphic encryption and distributed ledger computing: an ethical-legal qualitative expert assessment study" Scheibner et al. BMC MedicalEthics(2022)23:121 https://doi.org/10.1186/s12910-022-00852-2.

[24] Chris Gilbert, Mercy Abiola Gilbert "The Effectiveness of Homomorphic Encryption in Protecting Data Privacy"International Journal of Research Publication and Reviews, Vol 5, no 11, pp 3235-3256 November 2024.

[25]Koushikinha, PrathamMajumder†andSubhas K. Ghosh,"Fully Homomorphic Encryption based Privacy-Preserving Data Acquisition and Computation for Contact Tracing"Authorized licensed use limited to: IEEE Xplore. Downloaded on May 14,2021 at 00:32:46 UTC fro