Cryptography Practices in Healthcare System: A Review

Theophilus Bamise AJALA[1*], Adeniyi AKANNI[1], Olajide ADEGUNWA[1], Rashid Kehinde OLOKO[1], John Oluwadara FATOKUN[2], Chukwudi Anthony UDEMBA[1]

[1]Department of Computer Science, College of Computing and Information Sciences, Caleb University, KM 15, Ikorodu-Itoikin Road, Imota, P.M.B. 21238, Lagos State, Nigeria

[2]Department of Mathematics, College of Pure and Applied Sciences, Caleb University, KM 15, Ikorodu-Itoikin Road, Imota, P.M.B. 21238, Lagos State, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.51244/IJRSI.2026.1306000420

Received: 28 June 2026; Accepted: 03 July 2026; Published: 15 July 2026

ABSTRACT

This paper provides a detailed discussion on how cryptography techniques have been essential in changing the healthcare sector. Because of the emergence of various healthcare applications and the increase in the amount of data in the healthcare sector, there is a need for ensuring that the data are protected. In this paper, we will be looking at the capabilities of cryptography, which can help in solving problems and ensuring security in future healthcare systems. This paper focuses on cryptography in healthcare systems, which is made up of practices and methods that ensure that sensitive healthcare information is encrypted, authenticated, hashed and keys are managed securely. This paper provides an overview of cryptographic evolution and concepts. It also looks at some of the challenges that may affect the use of cryptography in practice. Overcoming such issues will require a pragmatic and structured strategy. The paper offers pragmatic suggestions that will help in utilizing cryptography in an efficient manner within real-world systems hence, the paper proposed an implementation framework integrating encryption, authentication, key management and auditing. These findings offer a way forward for policy-makers to increase the security and resilience of EHRs within the public health care system through empirical knowledge. The paper ends by making actionable suggestions for the health care organization and future research direction.

Keywords: Cryptography, Electronic Health Records (EHRs), Healthcare Security, Data Privacy, Encryption, Cybersecurity, Electronic Medical Records (EMRs)

INTRODUCTION

The transfer of health information in the modern healthcare system is based on the safety of its transmission when keeping confidentiality and integrity of the patients' information (Afzal et al., 2025). Healthcare industry at large has recently experienced a number of major transformations due to fast development of technology and growing need for quality care (Chukwurah et al., 2025). One such technology to make an entry into this sector is the Cryptography, having an ability to bring about a revolution in the delivery, management and security of the healthcare services. The digitization of the health system has brought about a revolutionary change in the healthcare sector, making clinical processes more efficient and improving the process through which patient data is recorded, stored and used to provide healthcare services. According to the Author, it can be stated that there has been a revolutionary change in the field of healthcare, from the traditional practice of maintaining paper records to maintaining Electronic Health Records (EHRs) (Chuma, 2026). (Chuma, 2026) says it should be noted that EHRs have become the backbone of modern healthcare due to fast access to patient's data that leads to accurate diagnosis, tailored treatment and better results overall. Nevertheless, this technological change has opened a new field for exploitation from cyber criminals through the abuse of patient's health data for personal gain. (Chuma, 2026) proves that increasing reliance on digital healthcare systems and networks has increased the susceptibility of sensitive medical records to advanced cybersecurity risks and attacks. Since the data stored in electronic health records is extremely sensitive in nature, the healthcare industry continues to be the most

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

vulnerable sector when it comes to cybersecurity incidents like phishing attacks, data breaches, ransomware, and other forms of cybercrimes.

The trend in the last decade has been the tendency to aggregate online medical records of patients via cloud computing and other technologies. There is a need to secure data of patients which might not be sufficiently protected during the coronavirus disease. In 2020, there was an unusual increase in the number of cyber-attacks against healthcare organizations worldwide, including hospitals and clinics. Cryptographic data protection could improve the security of medical records, because not only would it provide perimeter protection against external cyber-attacks but also constant protection against external and internal cyber-attacks. This could be accomplished by encrypting the medical records; hence, even if the perimeter is broken and the attacker enters the system, the data remains secured. With the application of modern cryptographic technology, such a protection could not only be applied to the data at rest but also to the data in use (Lewis et al., 2022).

Cryptography acts as the fundamental pillar in computer science and information security since it plays a key role in ensuring the security of vital data against any malicious use. From the 1920s to date, cryptography has remained the most efficient means of communicating secretly, because of the ability to transform readable human data, referred to as plaintext, into an unreadable form known as ciphertext (Muhenga et al., 2025).

Cryptographic systems, as a discipline, solve the problems of confidentiality, integrity, and authentication in information transmission. Cryptography can be categorized into two broad categories; symmetric key cryptosystems and asymmetric or public-key cryptosystems. Symmetric cryptosystems use keys that have been shared between users. The major strengths of symmetric cryptosystems include security against any cryptographic attack, securing information privacy, and offering non-repudiation services such that one can trace a certain message to its rightful sender (Gilbert & Gilbert, 2024).

In light of all these facts, the Nigeria healthcare system as other African nations has been making good progress in using electronic health records to achieve greater efficiency and quality in their operations. But unfortunately, these systems are based mostly on very basic cryptography or lack thereof, together with archaic authentication techniques and software, which makes them vulnerable to any potential future attack aimed at jeopardizing a vast amount of health information stored or transmitted through these systems. These systems lack proper solutions to tackle emerging computer-based attacks and threats, thus creating an important gap in terms of national security preparedness. This means that the lack of a strategy for cryptography migration creates an important gap in the Nigeria healthcare system.

Another limitation is that although there is an abundance of research on the use of cryptography in securing EHRs, most of them are conceptual and have been carried out in developing countries such as the United States of America and Canada. Thus, there is no empirical research in relation to the readiness for cryptographic implementation in the Nigerian context. This study sought to fill the gaps through empirical examination of the use of cryptography in securing EHRs in Nigeria, with a view to recommending measures to enhance readiness.

Moreover, the rate of occurrence of information security problems in relation to the Electronic Health Record system (EHR) is progressively becoming a source of worry, hence necessitating measures aimed at addressing these problems in order to prevent the unauthorized manipulation and access to the information contained in these records, hence ensuring that confidentiality, availability and integrity are upheld. Failure to do so will lead to complications such as incorrect diagnosis and treatment, and in the worst-case scenario, death (Ganiyu et al., 2019). Therefore, in this paper we present some of the cryptographic practices that can be considered to secure EHRs.

Statement of the Problem

With the increasing adoption of digitized solutions in healthcare systems across the world, there has never been a more critical need to develop strong cybersecurity measures. As Nigeria continues to embrace Electronic Medical Records and Electronic Health Records, the management of health information becomes a concern that needs to be addressed. Unfortunately, this has come with numerous cyber security threats, thereby making it necessary to understand the basics of cybersecurity (Opele & Nafada, 2025).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

The use of digital technology for handling the information of patients by hospitals and other medical facilities has raised serious issues about the safety and privacy of data. Despite the fact that there are many limitations associated with the use of old techniques for ensuring the security of healthcare information; such methods are much more susceptible to attacks from hackers, and do not have much capacity to withstand attacks on the integrity and privacy of health information. These methods do not take into account the different threats of the cyber world (Venkataradhakrishnamurty & Malathi, 2025). In recent times, there has been a speedy digitalization of the healthcare sector within the last decade, which has led to an increase in attacks on patient information. The present encryption technology includes DES and AES, which face certain problems regarding speed and power. This means that there is need for alternative approaches to overcome these limitations (Venkataradhakrishnamurty & Malathi, 2025).

The security of health care data has become extremely essential due to the highly personal nature of the patient information involved and also because of the increasing trend of cyber attacks against medical data. The current techniques of security enhancement have been discussed to highlight the limitations and also the necessity of developing new cryptographical solutions to this problem. Another limitation lies in the integration problems between the various health care systems as well as the lack of any standard cryptographic solution for health care system. In this research paper, we would attempt to develop various cryptography techniques to protect against cyber attacks.

Objectives of the Study

1. To investigate the theory behind cryptography and its evolution and importance in the protection of digital health care systems.

2. To find out and study various existing cryptographic mechanisms used for securing Electronic Health Record (EHR) systems, Electronic Medical Record (EMR) systems, and other healthcare systems.

3. To study the efficiency of cryptographic measures in providing security aspects like confidentiality, integrity, authentication, access control, and non-repudiation to healthcare data.To investigate the necessity of cryptography in healthcare environments, particularly for securing data at rest, data in use, and data in transit.

4. To determine the problems and obstacles involved in the implementation of cryptographic methods in the health sector, particularly in developing countries like Nigeria.

5. To come up with recommendations on how to enhance cybersecurity in the health sector by adopting cryptographic methods and other emerging security technologies.

LITERATURE REVIEW

In this segment, relevant literature related to cryptology in healthcare is examined. This discussion focuses on the approaches used, the applications involved, the advantages and disadvantages of such approaches, and their contributions to healthcare security. It is intended to offer a broad overview of the existing state of affairs in health care cryptology.

The selected articles were analyzed and organized thematically according to their contributions in the application of cryptography and authentication technologies to secure electronic health records. Instead of analyzing each paper separately, the relevant literature was organized using common themes identified in the various papers.

Theme 1: Cryptography Techniques for Information Privacy Protection

One main theme from the selected literature is the use of cryptographic algorithms to maintain the confidentiality and privacy of healthcare information. Pandhare and Nikam (2021) indicated that the security of IoMT health data could be improved by using cryptographic techniques in which the AES algorithm guarantees data confidentiality, whereas access control is attained by key generation for the healthcare provider and patients. Likewise, Rajarathna (2021) maintained that the transfer of healthcare information in the cloud environment

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

needed cryptographic algorithms to protect the medical information that is being transferred using communication channels such as email and web application.

A number of research work applied AES alone or alongside other forms of encryption algorithms. Wahyudi and Romli (2023) applied AES for encryption of electronic medical records of patients, while RSA algorithm was used for encrypting the keys to ensure security of Electronic Medical Records (EMR). Similar to this, Srinivasan et al. (2023) used AES encryption algorithm to protect communication between doctors and patients on a healthcare website so that their information remains safe from any unauthorized usage or access.

Hybrid encryption schemes have also been proposed for securing health-related information. For instance, Kizhuvettil et al. (2025) developed Medi Messenger app using AES-RSA hybrid encryption algorithm to securely store patient information as well as offer services including appointment scheduling, telemedicine consultation, disease management, and storage of medical images. Li and Huang (2024) suggested a scheme of privacy protection in hospitals based on hospital big data which uses hybrid encryption scheme involving AES, Elliptic Curve Cryptography (ECC), and SHA-1 digital signatures to provide secure storing, transferring, and authentication of hospital data. Experimental results revealed better encryption efficiency and enhanced security in comparison to conventional RSA-AES hybrid encryption.

Further advancements in cryptography security were made by Sabonchi (2025) who combined Lion Optimization Algorithm (LOA), SHA-256 hash function, and Elliptic Curve Cryptography to increase EHR security. The method decreased the time required for encryption and decryption while providing enhanced security performance compared to other cryptographic methods. In addition, Ganiyu et al. (2019) used asymmetric and visual cryptography in web-based EHR system to ensure that no unauthorized access is made on patients' information. Finally, Silva et al. (2013) showed that privacy and confidentiality features considerably increased users' trust in mobile health care applications.

Theme 2: Authentication and Access Control for Healthcare Systems

An additional prominent theme that emerges from the literature is the improvement of the methods for authentication and access control for protecting health care information systems. Bahache et al. (2024) tackle the issue of authentication in cloud-based health care systems by developing a safe post-quantum authentication method using Kyber cryptography.

Yaseen et al. (2023) came up with a secure EHR authentication model by employing robust authentication mechanisms and RSA signatures. Their model successfully protected against impersonation, replay attacks, denial of service, man-in-the-middle attack, and insider attacks and had minimal communication overhead. To enhance the security of prescriptions, they employed QR codes along with RSA signatures of physicians.

The significance of authentication security was reiterated by Chuman and Msomi (2024) who explored password authentication flaws in public hospitals. Their qualitative research findings indicated various loopholes like user enumeration, poor credentials, faulty authentication, credential stuffing, phishing, ransomware, cryptojacking, and password re-use by healthcare workers in hospitals.

In the same way, Iherinwa et al. (2026) suggested enhancing the Electronic Health Records system by use of hybrid two-layer authentication strategy that utilizes Personal Identification Numbers (PINs) and barcodes for authentication. As per the authors, such an approach would adequately solve the numerous security issues involved with normal EHR systems.

Theme 3: Secure Data Sharing

Secure sharing of information is another aspect which has been repeatedly emphasized in the literature. In this regard, Liu et al. (2024) introduced a consortium blockchain architecture for sharing Electronic Medical Records which utilized encryption technique with the help of InterPlanetary File System (IPFS) and proxy re-encryption techniques. This strategy makes it possible for patients to give authorization to other healthcare providers to decrypt and access Electronic Medical Records without disclosing their encrypted forms.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Moreover, Rajarathna (2021) emphasized the significance of securing information exchange using cloud technology with the help of cryptographic algorithms to ensure protection of healthcare information conveyed via emails and web applications. Likewise, Kizhuvettil et al. (2025) showed an example of secured communication in telemedicine services incorporated into their encryption mechanism for e-health platform. Thus, it became possible to have a private communication between patients and healthcare professionals.

Finally, Srinivasan et al. (2023) also ensured secured doctor-patient communication via encryption of medical information conveyed through web-based healthcare platform.

Theme 4: Evaluation of Existing Cryptographic Techniques

Other studies were concerned with the assessment of the current cryptographic practices rather than suggesting an entirely new security framework. Schmeelk and Tao (2022) investigated 203 mobile applications for health care developed with the help of open-source software and available at GitHub in order to evaluate their compliance with cryptographic security principles. It was found that none of the applications uses cryptography in a complete way throughout all their components; therefore, the authors suggested additional developer training before deploying such apps.

In the same way, Thabit (2019) discussed the development of cryptography-based security methods used for protecting medical data in eHealth care systems during the past decade.

In addition, Chuman and Msomi (2024) have reiterated the importance of the above results by illustrating how human-related aspects like poor password practices and out-of-date technology continue to pose security threats despite the existence of sophisticated cryptographic techniques.

From the thematic synthesis, it is evident that the existing literature has widely investigated different forms of cryptographic techniques, such as AES, RSA, ECC, SHA-256, hybrid cryptography, blockchain, proxy re-encryption, and post-quantum cryptography, in a bid to enhance the privacy, integrity, and accessibility of healthcare data. Other studies have mainly focused on authentication procedures like RSA digital signatures, passwords, personal identification numbers (PIN), QR code authentication, and post-quantum cryptography.

Table 1: Summary of Reviewed Literature

Author & Year	**Objectives**	**Methodology**	**Results**	**Limitation**	**Future work**
Pandhare & Nikam (2021)	To secure IoMT healthcare data using cryptographic methods.	Employed AES encryption and key generation for access control.	AES ensured confidentiality while generated keys provided secure access to private healthcare records.	Focused mainly on encryption without adaptive authentication mechanisms.	Integrate intelligent authentication and scalable IoMT security frameworks.
Bahache et al. (2024)	To develop a secure post-quantum authentication scheme for cloud healthcare applications.	Employed Kyber-based post-quantum authentication protocol.	Resistant to quantum attacks	Did not evaluate usability	Validate the scheme in real healthcare cloud environments.
Rajarathna (2021)	To review cryptographic mechanisms for cloud-based healthcare	Literature review	Highlighted the necessity of cryptographic algorithms for protecting cloud communications.	No implementation	Develop practical cloud-based cryptographic healthcare systems.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	information exchange.				
Schmeelk & Tao (2022)	To evaluate cryptography implementation in healthcare mobile applications.	Source code analysis of 203 open-source healthcare applications on GitHub.	None of the applications fully implemented cryptography across all components.	Limited to open-source applications only.	Improve developer training and secure software development practices.
Thabit (2019)	To review recent cryptography-based security approaches in eHealth systems.	Systematic review	Summarized major cryptographic methods and their security requirements.	No empirical validation	Investigate emerging cryptographic technologies for modern eHealth systems.
Silva et al. (2013)	To evaluate privacy and confidentiality in a mobile health application	Experimental performance testing using 35 users across seven mobile devices.	Users experienced acceptable confidentiality and privacy	Small sample size and limited application scope.	Evaluate larger populations and diverse mobile platforms.
Kizhuvettil et al. (2025)	To develop a secure e-health application using hybrid encryption.	Employed AES-RSA hybrid encryption with Firebase	Successfully secured patient data while providing telemedicine, appointments	Focused primarily on Android implementation	Extend to cross-platform healthcare systems
Sabonchi (2025)	To improve EHR security using optimized cryptographic techniques.	Combined Lion Optimization Algorithm, SHA-256, and ECC encryption	Faster encryption/decryption with over 18.89% improvement in performance.	Limited evaluation against emerging cyber threats.	Explore AI-driven optimization
Wahyudi & Romli (2023)	To secure Electronic Medical Records	Employed AES encryption and RSA key protection.	Improved confidentiality and integrity of patient medical records	Limited to Android-based healthcare systems.	Extend implementation to web and cloud healthcare platforms
Li & Huang (2024)	To develop a hybrid encryption scheme for hospital big data privacy protection.	Hybrid AES, ECC, SHA-1, and data compression techniques.	Achieved stronger security and faster encryption/decryption than conventional approaches.	Focused mainly on hospital big data	Investigate scalability in distributed healthcare environments.
Srinivasan et al. (2023)	To secure doctor-patient communication through encrypted databases.	Web application using AES	Protected patient information against hacking and unauthorized access	Authentication mechanisms were minimally discussed.	Integrate stronger authentication techniques alongside encryption.
Liu et al. (2024)	To provide secure	Employed blockchain, IPFS	Enabled secure encrypted EMR	Blockchain implementation	Optimize blockchain

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	Electronic Medical Record sharing.	storage, and proxy re-encryption	sharing with controlled access authorization	complexity may limit adoption	efficiency and interoperability.
Chuman & Msomi (2024)	To investigate authentication vulnerabilities in public hospitals.	Interviews with IT professionals in public hospitals.	Identified weak passwords, phishing, ransomware, credential leakage, and legacy system vulnerabilities	Limited to selected public hospitals.	Develop and evaluate stronger authentication frameworks in healthcare institutions.
Yaseen et al. (2023)	To develop a secure EHR authentication system.	RSA digital signatures, strong authentication, Scyther analysis, and CK protocol verification	Resistant to impersonation, replay, DoS, MITM, and insider attacks with low communication cost	Did not incorporate adaptive authentication factors.	Integrate adaptive multi-factor authentication.
Ganiyu et al. (2019)	To design a secure web-based electronic health record system.	Employed asymmetric and visual cryptography	Prevented unauthorized access while maintaining essential EHR functionality.	Limited discussion of usability and scalability.	Integrate advanced authentication and cloud deployment
Iherinwa et al. (2026)	To improve EHR security using two-layer authentication.	employed PIN and barcode-based hybrid authentication model.	Expected to strengthen authentication security for Electronic Health Records.	Proposal lacks implementation and performance evaluation.	Implement and validate the hybrid authentication model in healthcare institutions

Proposed framework for Cryptography Practices in Healthcare System

The following framework incorporates four main security elements obtained from the literature reviewed in order to give complete security to the health care systems as illustrated in the Figure below.

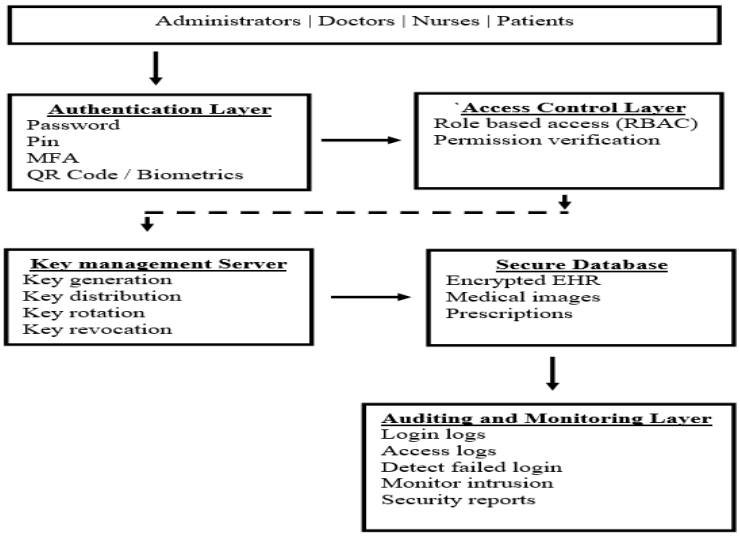


Figure 1: Proposed Diagram of the Integrated Framework for Healthcare systems using Cryptographic Practices

Authentication Layer: Authenticated users alone are supposed to move to the next security layer. The first security layer ensures that the identity of the health care users is authenticated before accessing the system. From the analyzed literature, authentication can be done in the following ways; Username and password, PIN, Multifactor authentication, QR code authentication, and biometric authentication.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Access Control Layer: Users are allocated access privileges that allow them to undertake their responsibilities, hence avoiding any unnecessary access. After the authentication process, RBAC ensures the privilege levels of the users. Some of the common roles are: Doctors, Nurses, Lab Technicians, Pharmacists, Admins and Patients.

Key Management Layer: This will ensure that the encryption keys are not exposed and enhance the security of the entire system. According to the literature review, encryption alone cannot be effective unless there is a proper handling of the cryptographic keys. This is why the proposed framework includes a Key Management Server that will undertake: Key generation; Key distribution; Key storage; Key rotation; Key revocation; Key backup/recovery.

Encryption Layer: This combined approach will guarantee that the healthcare information is confidential, accurate, and safe during transmission. Following authentication and authorization, all sensitive health care information will be encrypted before being either stored or transmitted. This framework incorporates various cryptographic algorithms from the literature review including AES encryption of the Electronic Health Records, RSA/ECC for secure key exchange and SHA-256 for password hashing.

Secure Database: Since the data is still encrypted, data privacy will be assured despite any vulnerabilities on the storage system. The encrypted patients' records will be stored in a secure database or cloud computing environment which will include: Electronic Health Records; Medical images; Prescriptions; Laboratory reports and Appointment details.

Auditing and Monitoring Layer: Auditing logs are also used to help health care institutions adhere to regulations. The last layer keeps monitoring system events to identify any suspicious activity. Some important tasks carried out by the auditing process include: Login attempts logging User activities logging Data access logging Failed login attempts logging Anomalous data access logging Audit report generation and Forensic investigation support.

Table 2: How the Framework was derived from the Literature

Framework component	**Supporting studies**
Authentication	Bahache et al. (2024); Yaseen et al. (2023); Chuman & Msomi (2024); Iherinwa et al. (2026)
Encryption	Pandhare & Nikam (2021); Wahyudi & Romli (2023); Li & Huang (2024); Sabonchi (2025); Kizhuvettil et al. (2025); Srinivasan et al. (2023)
Key Management	Pandhare & Nikam (2021); Li & Huang (2024); Yaseen et al. (2023); Kizhuvettil et al. (2025)
Auditing & Monitoring	Chuman & Msomi (2024); Schmeelk & Tao (2022); Liu et al. (2024)

Cryptography Evolution, Concept and Techniques

This section introduces a brief evolution of cryptography, while subsequent paragraph gives an overview on cryptograph concept and techniques.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

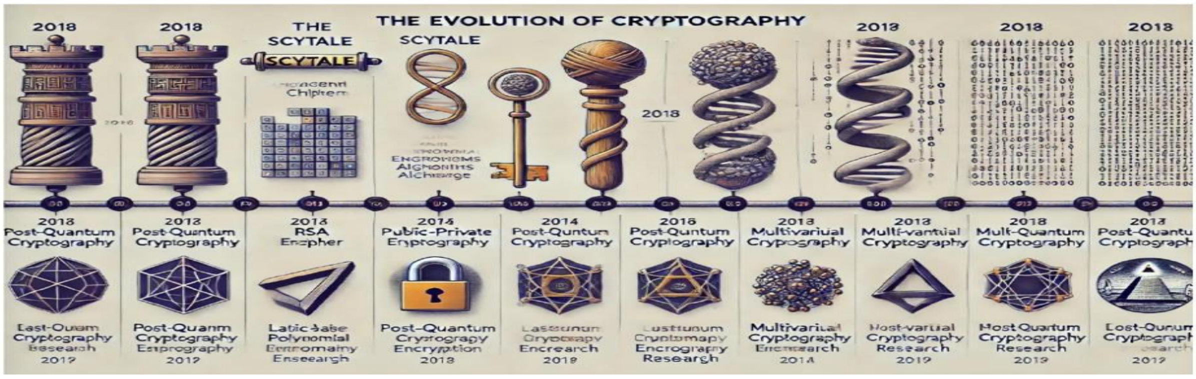


Figure 2: Evolution of cryptography (Gilbert & Gilbert, 2024)

This image conveys the story of cryptography evolution from ancient methods, such as the Scytale cipher that used parchment wrapped around rods to encode messages, to the latest methods known as post-quantum cryptography (Gilbert & Gilbert, 2024)

The timeline highlights key milestones:

1. Ancient Tools: The Scytale is representative of the earliest methods of secure communication, basic but efficient for its time.

2. Classical Progressions: The use of algorithms such as RSA added a new level of sophistication to encryption.

3. Contemporary Encryption: The development of public-private keys systems ushered in an era of online encryption.

4. Quantum Encryption: The advent of quantum computing is prompting the development of more robust methods of cryptography.

The icons and diagrams help make the timeline come alive, illustrating how cryptography has gone from primitive physical devices to abstract mathematics and even quantum-proof cryptographic methods. It is a captivating visual representation of how humans are able to adapt to their security environment.

Cryptography Overview

Cryptography hides or modifies the original information to ensure that it becomes something that only the recipient can understand. It has been difficult to secure digital communication since eavesdroppers often interfere with the network to carry out malicious activities or even conduct their experiments. If two people use the network to communicate, then there should be a way of securing the communication. Cryptography ensures security in communication through modifying data into something unintelligible by the eavesdroppers (Ugbedeojo et al., 2024). In (Mohammed & Hussein, 2023) Cryptography is referred to as a process that can be used to protect information. Protection is ensured through converting the message or the information into an unreadable form. Cryptography ensures that no unauthorized individual understands or sends any message. Cryptography is a process that creates a secured communication channel between two parties to ensure that information is kept secure when there are unauthorized individuals around. This was invented by Institute of Electrical and Electronics Engineers (IEEE). The two processes that take place in cryptography include encryption and decryption (Surla & Lakshmi, 2023). In (Mushtaq et al., 2017) Security becomes the necessary part to store information and transfer through the networks in a secure manner. Thus, the secure communication becomes the basic need in every transaction through networks. Cryptography becomes an important part of secure communication and transmission of information through security services. This helps in protecting sensitive information by encoding it in such a way that only the intended receiver becomes able to decode the data back into the readable form of text. The conversion of plaintext into ciphertext through the use of a key becomes known as the encryption process while decryption becomes the reverse of the encryption process. The cryptography algorithms become the secure and efficient, having low cost, small memory footprint and easy to

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

implement along with its multiple platform implementation. Many applications have been developed for securing cryptographic algorithms using various mathematical processes. It becomes really tough to develop a fully secured encryption algorithm because of the challenges posed by the cryptanalysts who continuously try to gain access to the available cryptographic system. The proper selection of algorithms becomes necessary for achieving high security requirements to protect the cryptographic elements from cryptanalysis (Mushtaq et al., 2017).

In (Rahman, 2026) Modern computerized systems require cryptography to safeguard their data, communications, and identities. With the expansion of digital services on networks and cloud platforms, it has become inevitable to have some cryptographic methods to protect them. In fact, huge amounts of sensitive data such as financial, medical, and military information is transmitted via the global network infrastructure in every single moment.

Typically, the principal objective towards which cryptography strives to strive for is information security and its efficient management and utilization. The objective may further be subdivided into a number of concerns related to confidentiality, authentication, data integrity, non-repudiation, access control, and availability (Al-Shabi, 2019). The following paragraph details the descriptions of each one of them;

Authentication: This involves proving the identity of a party to someone else who is unaware of the said party's identity

Confidentiality: This ensures that a message's meaning is encrypted to secure it from any unauthorized usage. It assures that the information is accessible only by those who have the authority to access it.

Data Integrity: This assures that the information that is received is exactly the same as the information sent. This is the assurance of the correctness and accuracy of the data.

Access Controls: This involves assigning special access privileges to different users in order to access different features.

Non-Repudiation: Assurance that a person/entity cannot disavow or deny their actions.

Availability: Ease of accessing the data.

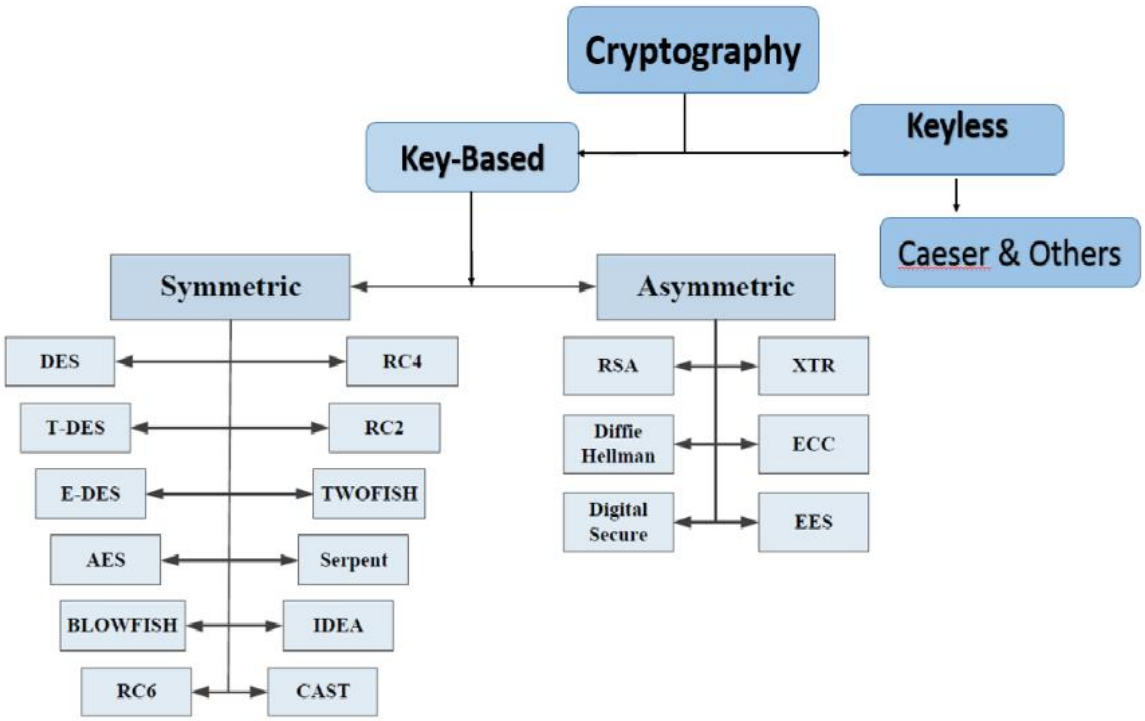


Figure 3: Classification of cryptography (Al-Shabi, 2019)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

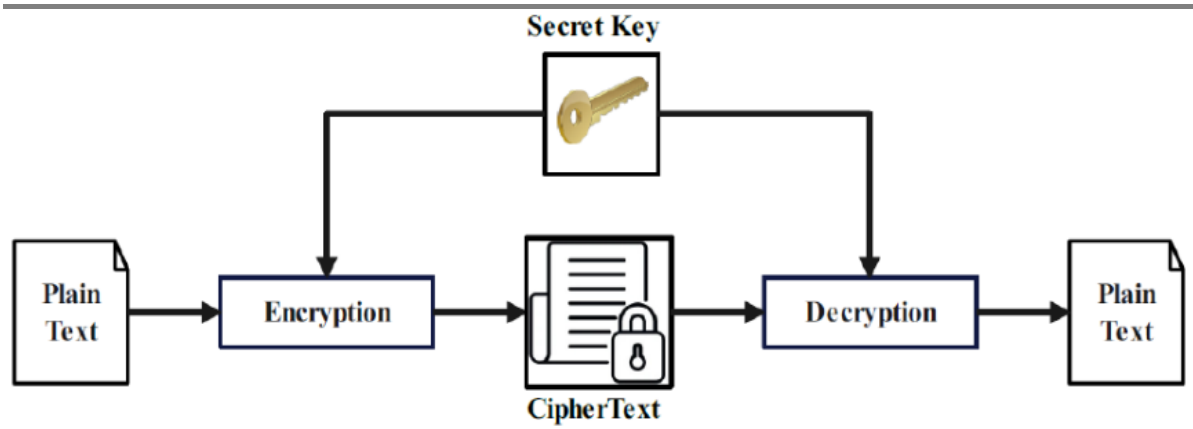


Figure 4: Symmetric process (Surla & Lakshmi, 2023)

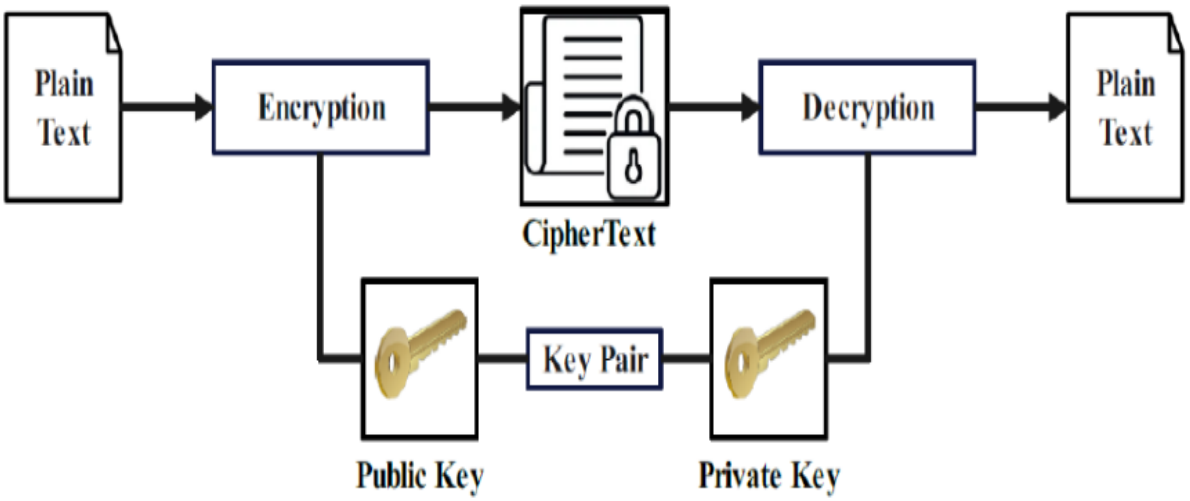


Figure 5: Asymmetric process (Surla & Lakshmi, 2023)

From the above diagram, Symmetric key cryptography encryption is performed using the same key used during decryption. This encryption scheme handles large volumes of data in high speeds and it can be implemented provided there are secure ways of distributing the key. Examples of such include the Caesar cipher, Stream ciphers, and Block ciphers. This encryption scheme is more preferred when there is need for communication within the network whereby there exists some level of trust and therefore sharing of the key between the users is possible. Asymmetric/public-key encryption as its name suggests, differs from symmetric key encryption by use of two keys instead of using one. More formally, this scheme removes the necessity of secure key distribution since along with the public keys it is possible to distribute them freely and ensure security through the private keys. The RSA algorithm is an example of the asymmetric algorithm that provides the hash functions (Muhenga et al., 2025).

In symmetric-key encryption, both the sender and the receiver use the same exact key to encrypt and decrypt the information. If a key K is used to encrypt the plain text, then the same key K is used to retrieve the original message from the cipher text (Gill, 2014). Symmetric key encryption systems are quite efficient and user-friendly too. But key management is a hard issue in symmetric encryption. Before starting a dialogue, the two entities have to share the key among themselves. The most commonly used attacks against symmetric ciphers are chosen plaintext attack, known plaintext attack, linear cryptanalysis, and differential cryptanalysis. In the case of asymmetric key encryption system, the data is encrypted using a public key by the sender, and decrypted using a private key by the recipient (Surla & Lakshmi, 2023).

Cryptography Techniques

The paragraph below detailed some cryptography techniques

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

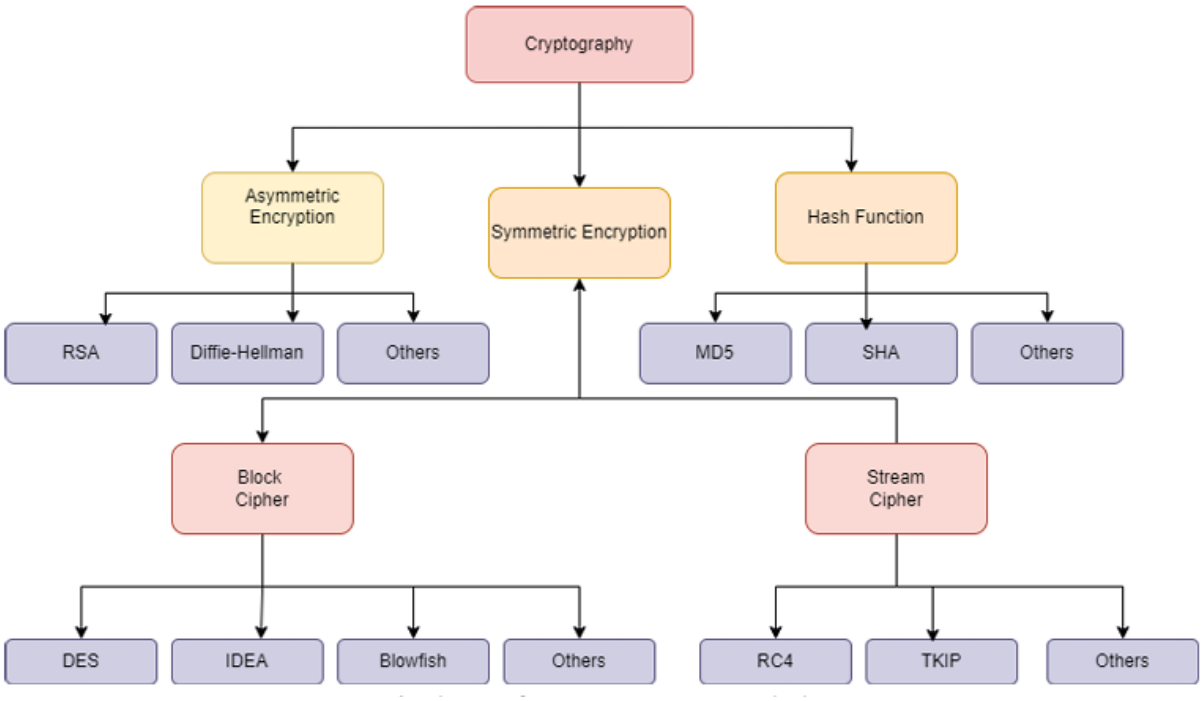
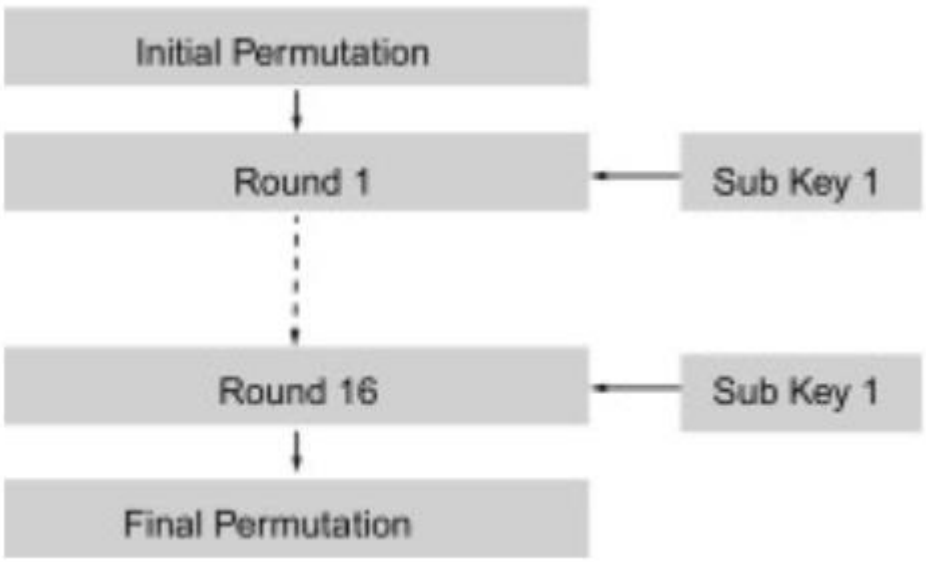


Figure 6: General idea of Cryptography Algorithms (Baig et al., 2024)

Data Encryption Standard (DES) Technique

Data Encryption Standard (DES) is a block cipher which was developed by NIST in 1974. This cipher has a 56 bit key which makes DES cipher vulnerable to brute force attacks in the present age computing environment; so although DES cipher is still being used and is a part of the TLS cipher suite, DES cipher is not recommended for use in new systems. However, although DES should be considered as deprecated cipher, it is still widely used (Martin, 2022). DES became the base of early data encryption systems and was widely implemented in commercial and governmental organizations (Ravi, 2025). Thus, we can consider DES cipher as an example of how a modern cipher is built as shown in the Figure



below.

Figure 7: DES (Martin, 2022)

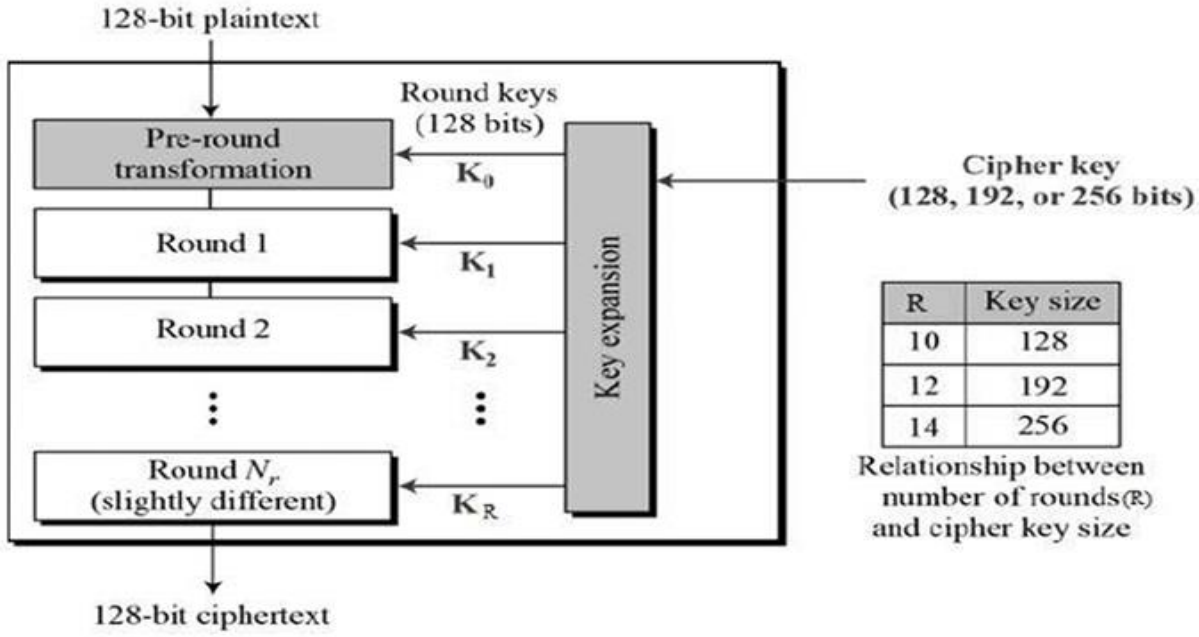
Block ciphers involve the execution of the encryption algorithm on a block of data. This is referred to as an "encryption round". The encryption process of the resulting encrypted block of data will be executed on more encryption rounds. In the case of the DES algorithm, this is done in up to 16 rounds. The individual encryption

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

round has a unique encryption key referred to as a subkey. The subkeys are generated from the original encryption key that consists of 56 bits plus another 8 bits for parity (Martin, 2022).

Advanced Encryption Standard (AES) Technique

AES algorithm is symmetric block cryptography and is an international standard of digital data protection. This algorithm has been selected due to its stability, effectiveness and very high level of security. AES is a successor to the previous widely used Data Encryption Standard (DES), which was considered insufficiently protected as its key was too short. AES can be used in three variations: 128-bit, 192-bit, and 256-bit keys. In regard to the web applications AES-128 is a main variant as it has high speed of work with low resource consumption. This algorithm works with 128-bit data blocks and performs 10 key operations with AES-128 algorithm, thus providing good level of protection while maintaining the effectiveness of encryption process. AES-128 is suitable for the usage in the security systems prototypes on client side due to limited resources of user's browsers. AES has been implemented in many systems for protection of text messages, documents and communications (Sukiman et al., 2026). In (Akwukwuma et al., 2024) With the growing significance of data security in the modern times, the necessity to have strong encryption methods has increased immensely. The Advanced Encryption Standard (AES) is considered to be one of the most secure encryption methods in practice today. The AES encryption method is a symmetric block encryption method which has a block/chunk size of 128 bits. These unique blocks are encrypted using keys which are of 128, 192, and 256 bits respectively. The ciphertext is then produced by combining these encrypted blocks .



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 8: Diagram of AES (Dalave et al., 2022)

The three varieties of AES algorithms are AES-128bit, AES-192bit, and AES-256bit in each iteration the data blocks will be encrypted and decrypted using 128 bit or 192 bits or 256 bits keys respectively. The Rijndael algorithm was modified to include block size and additional key lengths, but these were not passed on to AES (Dalave et al., 2022).

Rivest-Shamir-Adlema (RSA) Technique

The RSA algorithm uses an asymmetric approach. The RSA algorithm generates two keys that are used in cryptography: one key for encryption known as the public key and another key used for decryption. While the public key is made available to all interested parties who wish to communicate securely, the private key is not made public and used only for decryption purposes. RSA security is based on two separate computational difficulties: the first is known as the RSA problem where it is computationally impossible to find the private key from the public key within polynomial time, and the second is known as factorization of large numbers (Ugbedeojo et al., 2024). Following the original appearance, there have been several changes to the original

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

algorithm due to different public keys. Thanks to this improvement, the security for this research became better, with just a minor improvement in encryption time and without any modification of decryption time. In order to improve encryption, researchers used the similar idea as padding and optimized key generation by using continuous fractions. Moreover, they proved that the proposed algorithm is protected from meet-in-the-middle attack compared to the conventional RSA algorithm (Ugbedeojo et al., 2024).

Necessity of Cryptography in Healthcare

Protection against attacks on the data forms the issue and lowers the fraud rate for both providers and financiers by making payments via an automatic process, and hence increases the patient's satisfaction. The study of protecting the confidentiality of data by ensuring the integrity of the data and the authentication of the information is called cryptography. Hashing makes it more necessary to ensure the integrity of the transmitted messages (Gandam & Muralikrishna, 2020).

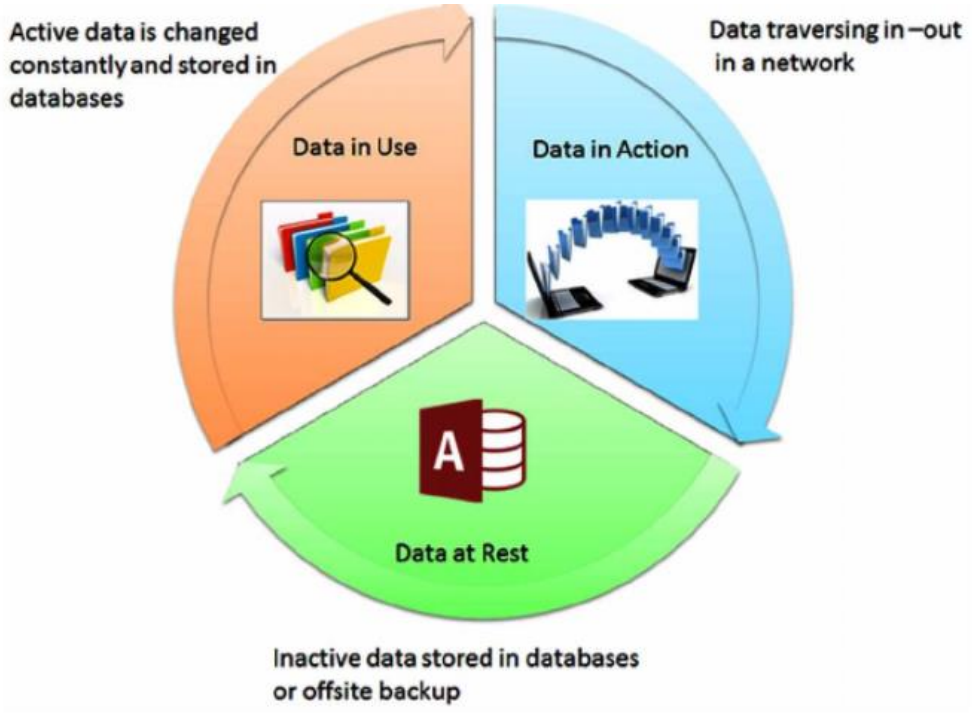


Figure 9: Data in three phases (Gandam & Muralikrishna, 2020)

Data protection is necessary during every step, and there are three stages of data that have been mentioned above in Figure, which are as follows: 1. Data in action; 2. Data in use; and 3. Data at rest. Data in action is that data which travels through various networks. It travels through systems located at different locations. Data in use is updated and changed during its usage (Gandam & Muralikrishna, 2020).

For any database that houses digital information, it becomes imperative that data security is of utmost importance for securing data from any unauthorized access. When data is stored on disk for long duration of time, it should be secured using encryption process which is popularly known as On-The-Fly encryption. Security using hardware devices for storing data for longer time span helps in protecting data against any malicious user and/or any data breach. Hardware security through biometrics which prevents any malicious user to log into, log out of and/or tamper with the privileges is one such example that is used in this chapter. Authentication means verification of the user's identity. There are two parts to authentication – Identification and actual authentication. In the first part of identification, any particular person's identity is presented to the security system in terms of user ID. The security system looks at all the abstracted objects and authenticates the actual user thereby granting access. This is done when the user gives some indication to the system to verify his/her identity (Gandam & Muralikrishna, 2020).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Encryption is the method where the information/message is encoded such that only authorized individuals are able to access it. Encryption algorithm produces a pseudorandom encryption key. The two types of encryption include symmetric and asymmetric encryption. In symmetric encryption, both encryption key and decryption key are identical. The communicating individuals use the same key for secured communication. Asymmetric uses an encryption key that is openly published to everyone and the decrypting group possesses access to the key for reading the message known as a decryption key. Data at rest is encrypted using either AES or RSA encryption methods. This will involve implementation of cryptography on the database storing the data physically. In this case study, we have encryption implemented on Electronic Health Record database (Gandam & Muralikrishna, 2020).

Challenges in Adopting Cryptographic Techniques for Electronic Patient Healthcare Records

This section presents the challenges associated with adopting cryptographic techniques for patient records.

Barriers Associated with Regulators

According to the research conducted by (Lewis et al., 2022), many participants indicated that the regulatory standards for data security that they had to adhere to did not reflect the reality of data security in health care. It was highlighted by the participants that the regulatory standards were not clear, were often impractical and were unable to provide directions on how to implement them. Due to the lack of clearly stated regulatory standards, the respondents were hesitant to request for more funding for their infrastructure upgrade.

1. Unclear standards: "Drafts are developed and after that remain at the draft stage for two or three years, since there are many questions that remain open. But, on the other hand, even if it eventually gets to be published as regulation, its enforcement is not even at the minimum level – which leads to people just doing what they want."

2. Absence of regulations: "Our absence of regulation is an old story… The problems that information security has in the health-care sector is endless, due to insufficient resources... due to the fact that there is nobody who can force our management or Ministry of Health to allocate these resources. Now, imagine I come up to my management and say, 'Hey, we need a new system worth a million dollars.' They would look at me with a puzzled face and say, 'Why do you need it? What does it state somewhere that you need this?'"

3. Unrealistic Regulations: "It's not smart to put regulations without giving the necessary resources because it is not smart to ask someone to do something he/she is unable to do. For instance, the regulators say that all computers should have Windows 10. Alright, but we have OCT machine for photographing the eyes with XP. How can you implement this regulation? It will take millions of dollars to replace all our machines as per this regulation and it does not work that way."

Barriers Associated with Healthcare Providers

It was evident from the participant responses that the health care environment was perceived as a dynamic and complex environment where there were several restrictions that necessitated finding a balance between the need to safeguard the patients' data and ensuring efficient patient care through continued availability of their data to the professionals (Lewis et al., 2022).

1. Limited capacity: It was noted by the participants how challenging it can be to deal with the constantly increasing cost of cybersecurity when their budget and workforce are extremely limited. This was highlighted as one of the reasons why they have not upgraded their security system yet.

2. Business focus: There were some participants who concluded that information security was not one of the top priorities for their organization. Their organization focuses on allocating more resources on core health care operations than on security of their information.

Policy and Regulatory Challenges

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

The Electronic Health Record (EHR) is defined as the digital record of patient data that makes the healthcare service provision better and safer through increased efficiency and effectiveness. The EHR system is a critical tool to both the healthcare professionals and the patients; they include activities such as recording and accessing the patient's medical history, prescribing drugs, organizing complicated healthcare management plans among others. EHR systems have been implemented since the 1960s in the USA and are used by over 87% of office-based healthcare practitioners in the USA. In detail, the use of basic EHR systems has changed from 6.6% to 81.2%, while that of the advanced one changed from 3.6% to 63.2% from 2009 to 2019. On the other hand, the adoption rate is as low as 18% in a developing nation such as Nigeria (Bolatito & Togunwa, 2025).

The lack of proper national EHR policies or guidelines in Nigeria and other sub-Saharan Africa countries is another major challenge to the deployment of EMR. Lack of adequate financial inducements and poor implementation strategies coupled with lack of political commitment have made even available EHR systems dependent on unsustainable funding from foreign partners. Furthermore, the process of implementing policies is not uniform; some state governments have embarked on independent implementations of EHR pilots in tertiary institutions while others do not even have any digital health policy. This makes the implementation and use of EHR difficult. Another major problem is that of privacy and data protection. Lack of stringent legal frameworks to guard against the security of patients' information generates lack of trust among patients and health practitioners making them reluctant to use EHR systems (Bolatito & Togunwa, 2025).

Not only do these constraints have their own separate effects but rather, these factors are deeply intertwined and support each other. For instance, the absence of proper policies and poor governance arrangements lead to inadequate investment in ICT infrastructure whereas lack of proper infrastructure discourages policy planning and investments. Institutional inertia, which involves poor stakeholder coordination and poor financial mechanisms, is another important factor which aggravates these problems (Bolatito & Togunwa, 2025).

Methodology of the Study

The current study is based on a compilation of literature and publicly available information with respect to the use of cryptography within healthcare in Nigeria. The methodology adopted by us was that of a focused search of literature in various academic databases including Google Scholar, Research Gate, Citeseerx, Arxiv, Sciencedirect (monetized sometimes), IEEExplore (monetized sometimes) using terms like 'healthcare and cryptography', 'emerging cryptographic methods', 'Cryptography for securing Electronic Health Records' and 'Healthcare data, Healthcare institution and cryptography in Nigeria'.

Database Search

A research approach was formulated and applied in order to identify various databases that contained up-to-date and relevant research articles on the topic of Cryptography Practices in Healthcare System like Google scholar etc. The time span of this study is an Eight years period, from 2019 to 2026.

Review Strategy

In the present review, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) was used to provide transparency, reproducibility, and rigor in the selection of relevant literature. PRISMA offers a structured approach to the identification, screening, eligibility assessment, and inclusion of sources in the systematic review. Published date: 2019-2026; Language: English; Type of publication: Peer-reviewed journal articles and conference papers; Domain: Healthcare cybersecurity; Topic: Cryptographic practices in healthcare; Availability: Full text. Figure 9 presents an analysis of the comments regarding the PRISMA.

Search Stage

Search Stage 1 (Extraction)

A comprehensive search was performed from six (6) electronic databases. The result was 328 articles, which underwent an elaborate screening process.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Search Stage 2 (Screening)

By removing duplicate articles and irrelevant literature, there remained a certain number of articles for analysis.

Search Stage 3 (Eligibility)

72 articles were selected as relevant to the study while acquiring relevant literature. Following that, some articles were excluded due to the absence of a well-defined methodology and sole reliance on abstracts due to the restriction of paywalls.

Search Stage 4 (Inclusion)

Out of 328, 72 articles were selected as relevant to the research during the acquisition of the literature. Some articles were then removed because of the lack of proper methodology and solely based on abstracts because of the limitation of monetization.

Table 3: Summary of PRISMA Analysis

Stage	Number
Identified records	328
Duplicates removed	42
screened	286
Full Articles accessed	72
included	39

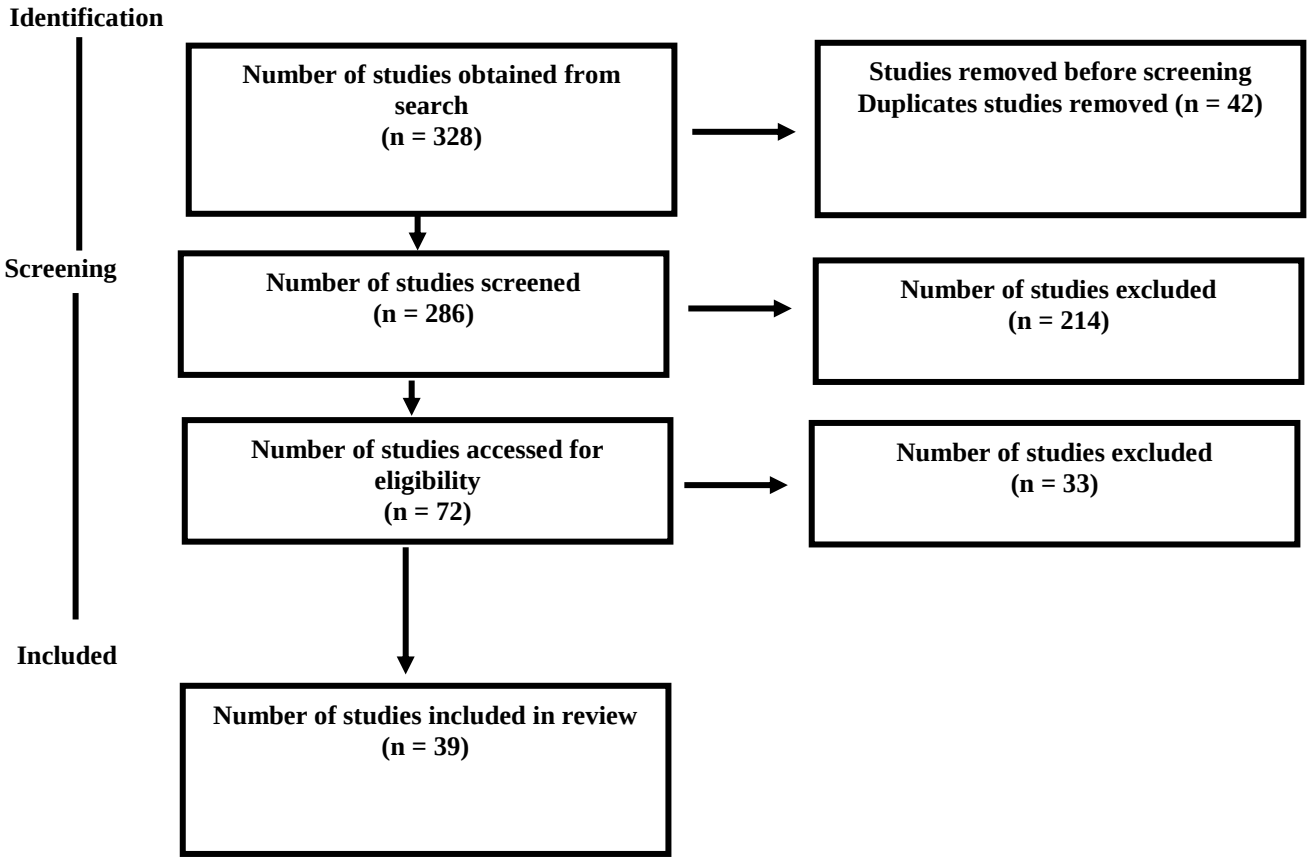


Figure 10: Feedback of the PRISMA Analysis

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

RESULT AND DISCUSSION

Result

Based on the literature review conducted from 2019 to 2026, it has been established that cryptography is one of the most effective ways of securing EHRs, EMRs, IoMT, cloud-based healthcare systems, mHealth apps, and telemedicine applications. The results show that there has been an increase in the usage of sophisticated cryptographic schemes used to meet confidentiality, integrity, authentication, access control, and non-repudiation requirements.

According to the distribution of cryptographic methods used in healthcare, it has been found that the most popular cryptographic techniques being implemented are the following: Advanced Encryption Standard (AES); Rivest-Shamir-Adleman (RSA); Elliptic Curve Cryptography (ECC); Hybrid AES-RSA Encryption; Hash Functions (SHA-256 and SHA-1); Visual Cryptography; Proxy Re-Encryption; Blockchain-based Encryption; and Post-Quantum Cryptography (Kyber).AES emerged as the most frequently utilized encryption algorithm due to its high speed, efficiency, and strong security characteristics. RSA was predominantly used for secure key management, authentication, and digital signatures, while ECC was preferred for environments requiring stronger security with lower computational overhead.

In the findings of the reviewed studies, the following results have been identified in the review: (1) Better Confidentiality and Data Protection: AES-based mechanisms effectively ensured the protection of healthcare databases, EMR, and patient-provider interactions. The studies have recorded a reduction in the cases of data leakages and unauthorized access to the data. (2) Better Authentication and Access Control: RSA signatures, barcode-based authentication, PIN-based authentication, and hybrid authentication methods helped improve the users' authentication process and avoid impersonation attacks. (3) Enhanced Security of Cloud-based Healthcare Systems: Hybrid cryptology approach using AES, RSA, and ECC made sure that the data being stored and transmitted via cloud-based environments are safe. (4) Usage of Emerging Technologies: Technologies such as blockchain, proxy re-encryption, and post-quantum cryptography were used to improve security against emerging security risks. (5) Faster Encryption and Decryption Times: Advanced cryptology mechanisms ensured fast encryption/decryption times. The ECC-LOA-SHA256 cryptology mechanism proposed by Sabonchi (2025) offered better processing times than traditional encryption mechanisms. (6) Protection against Cyber Attacks: Cryptography ensured better protection against the following cyberattack threats in healthcare systems: Phishing attacks, Replay attacks, Man-in-the-Middle (MITM) attacks, Denial of Service (DoS) attacks, Insider threats, Credential theft.

As for the challenges that were identified, despite all these improvements, some challenges have been identified by the review that impact the deployment of cryptologic technology in healthcare, including the following: The lack of standardized cryptologic frameworks, Weak cybersecurity policies and enforcement, The dependence on old healthcare systems, Limited funding, The poor cybersecurity awareness among healthcare workers, The low adoption rate of EHR systems in developing nations such as Nigeria, and Heterogeneity problems in healthcare systems.

Discussion

These results show that cryptography is an essential element in the protection of healthcare information systems. With the fast-growing digitalization of the sector, especially through the introduction of electronic health records and telemedicine systems, there has been a rise in the amount of confidential patient information stored and communicated digitally.

The review highlights that AES continues to be the leading encryption technique in the sector due to its efficiency and effectiveness. The efficacy of AES has been proven by several researchers, including Pandhare and Nikam (2021), Srinivasan et al. (2023), Wahyudi and Romli (2023), and Kizhuvettil et al. (2025). The high popularity of AES is due to the trust in this encryption system that is used in healthcare sector.

Moreover, the results also indicate that hybrid encryption through the use of both symmetric and asymmetric cryptographies is better in providing security compared to the use of either of these two techniques. Hybrid models including AES-RSA and AES-ECC take advantage of the speed of symmetric cryptosystems and the key management of the asymmetric encryption systems. According to researches done by Li and Huang (2024) and Kizhuvettil et al. (2025), there is improved efficiency and security when hybrid cryptography systems are employed.

Another important trend that can be observed in healthcare cybersecurity is the increasing interest in new technologies like blockchain and post-quantum cryptography. The blockchain approach increases the transparency, integrity, and traceability of medical records. On the other hand, post-quantum algorithms like Kyber solve security challenges associated with the future developments in quantum computing.

The review also suggests that cryptography is not enough for providing full healthcare security since there are many human-based vulnerabilities. Chuman and Msomi (2024) noted that such human-based issues as weak passwords, credentials reuse, lack of updates of the system, and poor cybersecurity awareness are among the major factors that cause security breaches within healthcare institutions.

From a Nigerian point of view, the results suggest a considerable gap between technological development and implementation. Despite the high effectiveness of the cryptographic solutions applied in the countries around the world, their use in Nigeria is restricted due to the low level of infrastructure development, lack of finances, absence of regulation, and fragmented EHR implementation approach. The low EHR adoption rate found by Bolatito and Togunwa (2025) is also a proof of this issue.

The review also shows that the problems with regulations and policies considerably affect cybersecurity within healthcare institutions. There are no clear national guidelines, enforcement, and financial resources to motivate healthcare organizations to invest in the new cryptography infrastructure.

The overall implications of the findings indicate that the future of cyber security in healthcare is to do with the incorporation of advanced cryptography techniques, multi-factor authentication, block chain technologies and post quantum security frameworks. In the case of Nigeria and other developing countries, it would be necessary to bolster policies, invest in ICT infrastructure of healthcare and cyber security awareness.

CONCLUSION AND RECOMMENDATIONS

The increasing digitalization of health care services has greatly facilitated the efficiency, accessibility, and quality of delivering health care services. Yet, the process of digitalization of healthcare has created various types of cyber threats in the form of data breaches, ransomware attacks, phishing, unauthorized access, and other cybercrimes. Due to the sensitivity of Electronic Health Records (EHRs) and Electronic Medical Records (EMRs), securing patients' information became one of the major requirements for the healthcare sector. This literature review has focused on analyzing the current approaches to cryptography used in the healthcare sector for securing the patients' information and delivering secure healthcare services. The research results show that the cryptography is still one of the most effective ways of ensuring confidentiality, integrity, authentication, access control, non-repudiation, and availability of healthcare information. As a result of the review, such cryptography technologies as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), hybrid encryption, blockchain-based security approaches, digital signatures, hashing, and post-quantum cryptography were identified as the main approaches used to ensure the security of the healthcare information. However, there are still some barriers preventing the effective use of cryptography solutions in the healthcare sector. Challenges facing healthcare cybersecurity include weak regulatory framework, limited financial capacity, reliance on old systems, poor cybersecurity skills among healthcare workers, lack of standardization of implementation processes, and poor interoperability among healthcare information systems. Challenges related to healthcare cybersecurity are especially common in developing countries like Nigeria since Electronic Health Record usage is still not high and cybersecurity is yet to be perfected. According to the findings of the paper, cryptography plays an essential role in securing healthcare information assets and fostering trust in digital healthcare systems. At the same time, technological means alone cannot secure healthcare information systems. The effectiveness of healthcare cybersecurity efforts depends on

proper utilization of cryptographic tools, development of sound regulation policies, constant training of employees, financial support, sound architecture of health care information systems, and implementation of good cybersecurity practices.

The following recommendations are suggested:

1. It is important that the healthcare organization trains their staff regularly through cybersecurity workshops and training to equip them with the knowledge to detect and deal with any threat that could arise.

2. It is necessary to devote enough effort towards ensuring that the organization adopts the best cryptography technology available.

3. The organization needs to build strategic alliances with other healthcare organizations and cybersecurity professionals in order to establish a network of information exchange on threats and possible measures.

4. The use of recognized cybersecurity frameworks is essential in guiding the cybersecurity approach taken by organizations. The framework could be Five Principles of Cybersecurity among others. Scholars and policymakers should work on encouraging the adoption of new security technologies such as blockchain technology, proxy re-encryption, and post-quantum cryptography in order to protect against future attacks.

5. The engagement of the government as well as the regulating bodies should be sought in the promotion of the policies in favor of cryptographic efforts in healthcare systems. This may involve financing of the cybersecurity infrastructure, setting of the policy and regulation and offering incentives for the enhancement of security measures. Government and healthcare regulating institutions should formulate cybersecurity policies and standards.

REFERENCES

1. Afzal, S., Bokhari, M.U., & Khan, I. (2025). A hybrid encryption model for medical image security in IoT healthcare. Discov Computing **28**, 321 (2025). https://doi.org/10.1007/s10791-025-09876-9
2. Akwukwuma, V.V.N., Chete F.O., Oshioluamhe, M.N. and Okpako A.E. (2024). Text Encryption Using Advanced Encryption Standard (AES) Algorithm. NIPES - Journal of Science and Technology Research. DOI: https://doi.org/10.5281/zenodo.12558923
3. Al-Shabi, M.A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. International Journal of Scientific and Research Publications 9(3):p8779; DOI:10.29322/IJSRP.9.03.2019.p8779
4. Bahache, A.N., Chikouche, N., & Akleylek, S. (2024) Securing Cloud-based Healthcare Applications with a Quantum-resistant Authentication and Key Agreement Framework. doi: https://doi.org/10.1016/j.iot.2024.101200
5. Baig, M.H., Ul-Haq, H.B., & Habib, W. (2024). A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance. Management Science Advances. https://doi.org/10.31181/msa1120244
6. Bolatito, B.A., & Togunwa, T.O. (2025). Barriers to the Adoption of Electronic Health Records in Nigerian Healthcare Systems: Analysing Infrastructure, Training and Policy Challenges. Perspective 4(2);34-41; doi: 10.25259/GJMS_1_2025
7. Chukwurah, A. I., Olannye, D. U., Edojarievwen, U. T., Onadje, F. O., Oghene, J. U., Uruh, K., Ogbogu, N. O., Etaghene, J. O. and Eborah, I. C. (2025). Emerging AI Applications in Healthcare: A Comprehensive Review. INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY; (A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA); DOI: https://doi.org/10.57233/ijsgs.v11i2.856
8. Chuma, K.G. (2026). Post-Quantum Cryptography for securing Electronic Health Records in the South African Public Healthcare System. Journal of Information Systems and Informatics; Vol. 8, No. 1, February 2026. DOI: 10.63158/journalisi.v8i1.1423
9. Chuman, K.G., & Msomi, M. (2024). Multi-Factor Authentication for Secured Access Control to Electronic Health Records in South African Public Hospitals (Preprint). DOI:10.2196/preprints.64918

10. Dalave, C.V., Lodh, A.A., & Dalave, T.V. (2022). Secure the File Storage on Cloud Computing Using Hybrid Cryptography Algorithm. International Journal for Research in Applied Science & Engineering Technology (IJRASET). Volume 10 Issue IV
11. Gandam, P.J., & Muralikrishna, I. (2020). Cryptography in the Healthcare Sector With Modernized Cyber Security. DOI:10.4018/978-1-7998-2253-0.ch008
12. Ganiyu, O.S., Olaniyi, O. M., Orooniyi T. (2019)," Securing Electronic Health Record System Using Cryptographic Techniques", Proceedings of Cyber Secure Nigeria 2019 Conference (CSNC 2019), Abuja, Nigeria, pp 48-53
13. Gilbert, C., & Gilbert, M.A. (2024). Investigating the Challenges and Solutions in Cybersecurity using Quantum Computing and Cryptography.
14. Gill, H. (2014). Selection of parameter 'r' in RC5 algorithm on the basis of prime number. Recent Advances in Engineering and Computational Sciences (RAECS); DOI:10.1109/RAECS.2014.6799519
15. Iherinwa, J.N., Olebara, C.C., & Ibebuogu, C.C. (2026). Design and Implementation of Secured Electronic Health System Using Pin and Barcode Technology. International Journal of Social Sciences and Management Research, Vol 12. No.2. DOI: 10.56201/ijssmr.vol.12no2.2026.pg189.193
16. Kizhuvettil, G., Zhang, T., Lu, J., Kethireddy S., & Fu, X., (2025). Medi Messenger: Secure E-Healthcare App Built with HybridEncryption Schema. ES Gen., 2025, 9, 1598. DOI: https://dx.doi.org/10.30919/esg1598
17. Lewis N, Connelly Y, Henkin G, Leibovich M, & Akavia A. (2022). Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records. Healthc Inform Res. 2022 Apr;28(2):132-142. doi: 10.4258/hir.2022.28.2.132. Epub 2022 Apr 30. PMID: 35576981; PMCID: PMC9117802.
18. Li, W., & Huang, Q. (2024). A hybrid encryption algorithm based approach for secure privacy protection of big data in hospitals. Egyptian Informatics Journal Volume 28. DOI: https://doi.org/10.1016/j.eij.2024.100569
19. Liu, G., Xie, H., & Wang, W. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. J Cloud Comp **13**, 44. https://doi.org/10.1186/s13677-024-00608-w
20. Martin, T. (2022). Cryptography—The basics. https://doi.org/10.1016/B978-0-12-821469-5.00012-0
21. Mohammed, Z.A., & Hussein, K.A. (2023). Lightweight Cryptography Concepts and Algorithms: A Survey. Conference: 2023 Second International Conference on Advanced Computer Applications (ACA). DOI:10.1109/ACA57612.2023.10346914
22. Muhenga, R., Sapundzhi, F., Popstoilov, M., Georgiev, S., & Todorov, V. (2025). Comprehensive Analysis of Cryptographic Algorithms: Implementation and Security Insights. Engineering Proceedings, 104(1), 43. https://doi.org/10.3390/engproc2025104043
23. Mushtaq, M.F., Jamel, S., Hassan, A., & Pindar, Z.A. (2017). A Survey on the Cryptographic Encryption Algorithms. International Journal of Advanced Computer Science and Applications 8(11):333-344. DOI:10.14569/IJACSA.2017.081141
24. Opele, J.K., & Nafada, B.G. (2025). UNDERSTANDING CYBERSECURITY IN THE IMPLEMENTATION OF HEALTH INFORMATION MANAGEMENT SERVICES. Unizik Journal of Educational Research and Policy Studies (UNIJERPS) VOL.19 (2)
25. Pandhare, R., & Nikam, S.S. (2021). Security of IoMT healthcare data using cryptographic techniques. International Journal of Advanced Trends in Computer Science and Engineering. https://doi.org/10.30534/IJATCSE/2021/531012021
26. Rahman, M.S. (2026). Cryptography in Digital Security: Foundations, Applications, and Emerging Challenges.
27. Rajarathna, N. (2021). A Study on Different Types of Cryptographic Algorithms in Securing Cloud Based HealthCare Services.
28. Ravi, R. (2025). What is data encryption standard algorithm? [Online]. Website: https://www.acte.in/data-encryption-standard-algorithm
29. Sabonchi, A.K.S. (2025). Securing Electronic Health Records with Cryptography and Lion Optimization. Journal of Cyber Security 7(1):21-43. DOI:10.32604/jcs.2025.059645

30. Schmeelk, S., & Tao, L. (2022). Case Study of Mobile Health Applications: The OWASP Risk of Insufficient Cryptography. Journal of Computer Science Research 4(1):22-31. DOI:10.30564/jcsr.v4i1.4271
31. Silva BM, Rodrigues JJ, Canelo F, Lopes IC, Zhou L. (2013). A data encryption solution for mobile health apps in cooperation environments. J Med Internet Res. 2013 Apr 25;15(4):e66. doi: 10.2196/jmir.2498. PMID: 23624056; PMCID: PMC3636327.
32. Srinivasan, T., Kumanan, T., Jain, S., & Geetha, S. (2023). Healthcare Management System using Cryptography Encryption (Web Security)
33. Sukiman, T.S.A., Sandy, C.L.M., Meiyanti, R., & Rizal, R.A. (2026). Implementation Of AES Algorithm For Text Message Encryption And Decryption Process. Gameology and Multimedia Expert 3(1):25-30; DOI:10.29103/game.v3i1.25923
34. Surla, G., & Lakshmi, R. (2023). A Collaborative Quantum Assisted Extended Elliptic Curve Cryptography Technique for Secure Data Transmission over Network. DOI:10.21203/rs.3.rs-3577699/v1
35. Thabit, R. (2019). Review of Cryptography Applications in eHealth Security Systems
36. Ugbedeojo, M., Adebiyi, M.O., Aroba, O.J., & Adebiyi, A.A. (2024). RSA and Elliptic Curve Encryption System. DOI: https://doi.org/10.4018/IJISP.340728
37. Venkataradhakrishnamurty, P., & Malathi, K. A (2025). holistic framework for strengthening security of healthcare data through encryption utilizing blockchain technology. Sci Rep **16**, 2008 (2026). https://doi.org/10.1038/s41598-025-31698-4
38. Wahyudi, R., & Romli, M.A. (2023). Android-based Patient Medical Record Data Security Application using AES and RSA Method Cryptography. International Journal of Computer Applications 185(40):34-39; DOI:10.5120/ijca2023923205
39. Yaseen, A.A., Patel, K., Yassin, A.A, Aldarwish, A.J., & Hussein H.A. (2023). Secure Electronic Healthcare Record Using Robust Authentication Scheme IAENG International Journal of Computer Science, 50:2, IJCS_50_2_16.