


Chapter 19

A Review on Different Encryption and Decryption Approaches for Securing Data

Udochukwu Iheanacho Erundu

Landmark University, Omu-aran, Nigeria

Nehemiah Adebayo

 <https://orcid.org/0000-0001-5838-8843>

Landmark University, Omu-aran, Nigeria

Micheal Olaolu Arowolo

Landmark University, Omu-aran, Nigeria

Moses Kazeem Abiodun

 <https://orcid.org/0000-0002-3049-1184>

Landmark University, Omu-aran, Nigeria

ABSTRACT

With the advancement of network and multimedia technologies in recent years, multimedia data, particularly picture, audio, and video data, has become increasingly frequently used in human civilization. Some multimedia data, such as entertainment, politics, economics, militaries, industries, and education, requires secrecy, integrity, and ownership or identity protection. Cryptology, which looks to be a viable method for information security, has been used in many practical applications to safeguard multimedia data in this regard. Traditional ciphers based on number theory or algebraic ideas, such as data encryption standard (DES), advanced encryption standard (AES), and other similar algorithms, which are most commonly employed for text or binary data, do not appear to be appropriate for multimedia applications. As a result, this research examines effective algorithms for data security.

DOI: 10.4018/978-1-6684-5250-9.ch019

INTRODUCTION

Cloud computing paradigms are becoming increasingly popular in the ever-changing technological landscape. In order to keep up with the ever-expanding possibilities of modern communications, special security measures are needed, particularly for computer networks. As the amount of data being exchanged on the Internet grows, so does the importance of network security. Protecting data from misuse and unauthorized access necessitates maintaining its confidentiality and integrity. Information hiding has grown exponentially as a result. In today's world, security measures can be broken down into a variety of subcategories, such as information concealment (Steganography), data encryption (Cryptography), or any combination thereof (Sethi & Sarangi, 2017).

People's lives have been impacted by digital technologies. Most modern electronic gadgets store their data with an external cloud service. In the cloud, people are storing a plethora of media items. A large number of individuals all over the world use these media every single second. It is imperative that these media are not accessed illegally. The user-end encryption is one of the most vulnerable points for data leaks (van Steen & Tanenbaum, 2016).

In the new computing paradigm of cloud computing, various services can be provided on demand and at a low cost. Cloud computing's primary goal is to provide fast, easy-to-use computing and data storage services to the masses. Today's computing model, called "cloud computing," makes use of a decentralized network to deliver a wide range of resources at a low cost and on demand. In addition, cloud computing's primary goal is to provide fast, easy-to-use computing and data storage services in a cloud environment (Wu & Buyya, 2015). Although the computing community has mastered the use of cloud computing services, some threats and risks do exist in this setting. Numerous techniques, such as cryptography, exist to improve the security of cloud computing and data in the cloud. Data or messages can be transferred securely while maintaining their privacy, and the cypher text used to encrypt them is only visible to the intended recipient. Data encryption, data quality assurance, and data authentication are all examples of cryptology. Cryptography provides a wide range of more secure methods that can be used to provide these services. Data that must remain private is encrypted and decrypted with the help of well-known cryptographic algorithms, such as those found in encryption protocols, digital signatures, and hash functions (Symmetric Algorithms, Asymmetric Algorithms, and Hybrid Algorithms). Protection is a problem for all of the current schemes. Cryptographic key generation, retrieval, data encoding, and decryption all take a lot of time in these schemes (Hashizume et al., 2013).

Furthermore, one of the most difficult tasks in cloud computing is safeguarding sensitive and confidential data while it is being transported and stored due to the possibility of various attacks. Using a large number of and more complex encryption keys makes the process more difficult (Al-Issa et al., 2019).

To address data security concerns, a wide range of encryption methods have been proposed for making better decisions about which encryption method to use for smart systems data security by studying a variety of techniques. Execution time, complexity, and maintainability all depend on having a thorough understanding of each technique. Some existing cloud computing security models, which use encryption algorithms to store and transmit data, have security flaws and privacy violations, which are the focus of this paper. Data security and privacy in the cloud computing environment can only be ensured by encrypting data in storage and transmission. Security policies are specified and enforced through a model used in computer science. Structured access privileges, computation models, distributed computing models, or no theoretical grounding at all can be used to build a security system (Qureshi et al., 2022).

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/a-review-on-different-encryption-and-decryption-approaches-for-securing-data/312431

Related Content

Distributed Ledger Technology in 6G Management Strategies for Threat Mitigation

Chetan Thakar, Rashi Saxena, Modi Himabindu, Rakesh C., Amit Duttand Joshuva Arockia Dhanraj (2024). *Security Issues and Solutions in 6G Communications and Beyond* (pp. 160-176).

www.irma-international.org/chapter/distributed-ledger-technology-in-6g-management-strategies-for-threat-mitigation/351772

Encryption of Analog and Digital signals through Synchronized Chaotic Systems

Kehui Sun (2011). *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption* (pp. 415-438).

www.irma-international.org/chapter/encryption-analog-digital-signals-through/43310

Demystifying Global Cybersecurity Threats in Financial Services

Deepika Dhingra, Shruti Ashokand Utkarsh Kumar (2021). *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 181-202).

www.irma-international.org/chapter/demystifying-global-cybersecurity-threats-in-financial-services/284152

An Improved Intrusion Detection System to Preserve Security in Cloud Environment

Partha Ghosh, Sumit Biswas, Shivam Shaktiand Santanu Phadikar (2020). *International Journal of Information Security and Privacy* (pp. 67-80).

www.irma-international.org/article/an-improved-intrusion-detection-system-to-preserve-security-in-cloud-environment/241286

Synthesis of Evidence on Existing and Emerging Social Engineering Ransomware Attack Vectors

Abubakar Belloand Alana Maurushat (2023). *Cybersecurity Issues, Challenges, and Solutions in the Business World* (pp. 234-254).

www.irma-international.org/chapter/synthesis-of-evidence-on-existing-and-emerging-social-engineering-ransomware-attack-vectors/313869