RSA and Elliptic Curve Encryption System:
A Systematic Literature Review

Musa Ugbedeojo, Landmark University, Nigeria

Marion O. Adebiyi, Landmark University, Nigeria
🆔 https://orcid.org/0000-0001-7713-956X

Oluwasegun Julius Aroba, Durban University of Technology, South Africa*
🆔 https://orcid.org/0000-0002-3693-7255

Ayodele Ariyo Adebiyi, Landmark University, Nigeria

ABSTRACT

Almost every living species has a motive to communicate electronically with one another and preserve data for immediate or future use. These data are becoming too large to be maintained on personal storage devices. Technological innovation has cleared the path for vast, remote storage known as the cloud. This innovation is being provided as a service to people and organizations due to the high cost of investment and the high-tech skills needed for its maintenance. Despite the many benefits of cloud computing, data privacy, integrity, and access control are issues that require immediate attention. Many studies have been conducted in order to find solutions to these challenges. In this review, the authors look at the numerous methods that have been proposed to address these security challenges. The research revealed that elliptic curve cryptography and the advance encryption system (AES) were the techniques that were most frequently used to address security issues in the digital world.

KEYWORDS

Cloud Computing, Cryptography, Cryptosystem, Elliptic, Encryption Algorithm

INTRODUCTION

Technology advancements have increased the volume of data stored by individuals and businesses. Due to the bulk, this data type could no longer be stored on microcomputers. Organizations and individuals have kept their high-volume data on a third-party cloud with ample storage capacity. While this problem has been solved for organizations and individuals, there is still the issue of data security, integrity, and access restrictions. Sebastian (2022) reported that data breaches costs the United States between $3.86 Million and $4.24 Million. The majority of these treats came from remote work. Researchers have devised several cryptographic algorithms for data security, integrity verification, and access control concerns. As technology improves daily, early cryptographic techniques appear unsuitable for modern-day advances, as various attacks (Alqahtan & Sheldon, 2022) on

critical cryptographic systems have been reported. Cloud security challenges have been identified and categorized into security standards, network category, access control, cloud infrastructure, and data category (Khalil et al., 2014).

The rest of this review paper is organized as follows: We first review relevant cryptographic approaches. We then present our review methodology, outline our results and discussions, and conclude with crucial areas for additional work.

Cryptography

Cryptographic techniques have shown to be a lifesaver regarding data integrity and security. Shruthy and Maheswar (2022) defined cryptography as "the art of writing or solving codes." Cryptography conceals or changes original material into a form only the intended recipient can comprehend. Securing digital communication has proven complex, as eavesdroppers frequently hijack network traffic for nefarious purposes or as part of research. When two parties communicate via the network, a secure communication technique ensures that the conversation is secure. Cryptographic techniques safeguard the process by converting data into an unreadable form by eavesdroppers, making communication secure. Imam et al. (2021) defined encryption as "the process of transforming data into an unreadable format, and decryption is the act of converting the unreadable form back to a readable form." Many cryptographic techniques have been developed to ensure that communication between parties is secured. According to Imam et al., 2021, for any encryption technique to be secured, it must possess three important security features: confidentiality, authentication, and data integrity.

Tuteja and Shrivastava (2014) stated that based on the encryption key, two types of encryption techniques are distinguished: asymmetric (public) and symmetric (private). Symmetric encryption approaches encrypt data with a single encryption key before delivering it over the network to the intended recipient. The receiver uses the same key to decrypt the message. Although this type of encryption approach is fast, its security cannot be guaranteed because there is no secure way of sending the encryption key. The first of this type of encryption is called Data Encryption Standard (Hatzivasilis et al., 2018). Over the years, other data encryption techniques, such as 3DES, AES, RC6, RC4, Blowfish, and IDEA have been developed (Abd-Elminaam et al., 2010) to modify the flaws observed in those techniques.

The issue of exchanging keys for encryption and decryption was addressed by public key (asymmetric key) encryption. The challenge of secret key exchange without being stolen before it reaches the parties involved in communication was alleviated using an asymmetric encryption technique. Asymmetric encryption has separate encryption and decryption keys in contrast to symmetric encryption. Both the encryption and decryption systems use a set of keys. The public key is the first, while the private key is the second. When a communication is encrypted with one of the pair's keys, it can only be deciphered with the other key (Rountree, 2011). Asymmetric key algorithms are, in a strict sense, slower than symmetric key algorithms. This slow speed is partly evident because symmetric algorithms are inherently more complex, requiring more advanced techniques. Popular public key encryption algorithm examples include RSA, Diffie–Hellman key exchange, ElGamal, Digital Signature Algorithm, and Elliptic-curve.

RSA Encryption Algorithm

The Diffie-Hellman public key was the first publicly released public key algorithm, and it only enabled key exchange protocol between known participants (at least at first). ElGamal expanded it to include a full encryption and signature public key technique for ECC cryptography (Braga & de Morais, 2014). Soon after Diffie-Hellman was released, the RSA cryptosystem (Rivest Shamir Adleman) was introduced to the public (Abdullah et al., 2018). RSA algorithm provides two keys for cryptographic purposes: one for encryption called public key, published for interested parties in secure communication, and the second for decryption. Unlike the public key, the private key is kept private and used for decryption. The RSA algorithm security is founded on two separate mathematical

Related Content

Assessing the Security of Software Configurations
Afonso Araújo Netoand Marco Vieira (2012). *Threats, Countermeasures, and Advances in Applied Information Security (pp. 129-157).*
www.irma-international.org/chapter/assessing-security-software-configurations/65766

Security in Health Information Systems
Christina Ilioudiand Athina A. Lazakidou (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 1759-1765).*
www.irma-international.org/chapter/security-health-information-systems/23191

Combination of Access Control and De-Identification for Privacy Preserving in Big Data
Amine Rahmani, Abdelmalek Amineand Reda Mohamed Hamou (2016). *International Journal of Information Security and Privacy (pp. 1-27).*
www.irma-international.org/article/combination-of-access-control-and-de-identification-for-privacy-preserving-in-big-data/155102

A Dynamic Privacy Manager for Compliance in Pervasive Computing
Riccardo Bonazzi, Zhan Liu, Simon Ganièreand Yves Pigneur (2012). *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards (pp. 285-307).*
www.irma-international.org/chapter/dynamic-privacy-manager-compliance-pervasive/61505

Self-Embedding Watermarking with Content Restoration Capabilities
Rong Huangand Kyung-Hyne Rhee (2013). *Multimedia Information Hiding Technologies and Methodologies for Controlling Data (pp. 305-334).*
www.irma-international.org/chapter/self-embedding-watermarking-content-restoration/70294