BABCOCK UNIVERSITY
ILISHAN-REMO, OGUN STATE, NIGERIA

COLLEGE OF POSTGRADUATE STUDIES
2022/2023 PhD Thesis Abstract

Department of Computer Science

RFN: **Oladapo Olalekan ADEDURO**
RD: **Computer Science**
RS: **Computing and Engineering Sciences**
RE: **oladapo.adeduro@gmail.com**
RAE: **oladapo.adeduro@pg.babcock.edu.ng**
RP: **08032303599**

RT: **Hybrid-Based Cryptographic Algorithm for Cloud Data Security**

MS: **Prof. Monday EZE**
ME: **ezem@babcock.edu.ng**
SP: **08028669172**
CS: **Dr. Folashade AYANKOYA**
CE: **ayankoyaf@babcock.edu.ng**
CP: **08033673152**

AB: The issue of cloud data security is a significant concern for organizations and individuals due to the prevalence of cloud computing for storing and accessing data. Cloud data security is vulnerable to various threats, such as unauthorized access, data breaches, and data tampering, resulting in a breach of sensitive data's confidentiality, integrity, and authentication. The consequences of such violations can be severe, including financial loss, reputational damage, and legal consequences to individuals and organizations. Traditional cryptographic techniques, such as symmetric encryption, asymmetric encryption, and hash functions, have been widely used for protecting cloud-based data by previous studies. However, using a single encryption technique is insufficient for protecting data in the cloud. Hence, the development of a Hybrid-Based Cryptographic Algorithm (HBCA) for cloud-based data security.

The HBCA was developed using a combination of three cryptographic techniques, which are Advanced Encryption Standard (AES) with a 256-bit key size, Rivest-Shamir-Adleman (RSA) algorithm with a 2048-bit key size and Secure Hash Algorithm (SHA) with a 256-bit key size. The HBCA was implemented using Python programming language and Firebase cloud storage infrastructure. Encryption time, decryption time, key size, CPU utilization, and memory usage were used for evaluation and performance analysis of the developed HBCA. The developed HBCA was compared with existing cryptographic techniques: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), AES, Blowfish and RSA.

The results showed that the encryption times for DES, 3DES, AES, Blowfish, RSA, and HBCA were 2.9477 seconds, 2.9477 seconds, 3.8402 seconds, 3.9389 seconds, 3.0958 seconds, and 42.0885 seconds respectively, while the decryption times were 2.9477 seconds, 2.9477 seconds, 3.84024 seconds, 3.93891 seconds, 3.0958 seconds, and 42.0885 seconds respectively. Their key sizes were 132 bits, 147 bits, 142 bits, 448 bits, 512 bits, and 448 bits, while CPU utilization were 96.49 seconds, 85.09 seconds, 94.85 seconds, 120.23 seconds, 100.00 seconds, and 44.00 seconds respectively. Also, their memory usages were 15 bytes, 16 bytes, 25 bytes, 30 bytes, 20 bytes, and 13 bytes respectively. The HBCA algorithm performed better than the previous security algorithms in terms of key size, CPU utilization, and memory usage, making it more effective and appropriate for devices with limited resources. The study discovered that the overall security posture of the HBCA system was stronger, as it was able to stand against various attacks.

The study concluded that the HBCA implemented was effective and less susceptible to known threats. It offered improved key size, CPU, and memory utilization, making it more robust and efficient for securing cloud data. It was therefore recommended that HBCA should be adopted by organizations using cloud storage to store sensitive data.

Keywords: Cloud storage, Confidentiality of information, Data security, HBC algorithm, Integrity of information

Word Count: 430

Abbreviations: RFN: Researcher's Full Name, RD: Researcher's Department, RS: Researcher's School, RE: Researcher's Email, RAE: Researcher's Alternate Email, RP: Researcher's Phone Contact, RT: Registered Title, MS: Main Supervisor, ME: Main Supervisor's E-mail Address, SP: Main Supervisor's Phone Contact, CS: Co-Supervisor, CE: Co-Supervisor's E-mail Address, CP: Co-Supervisor's Phone Contact, AB: Abstract

Suggested Citation: Adeduro, O.O., Eze, M. and Ayankoya, F.Y. 2023. Hybrid-Based Cryptographic Algorithm for Cloud Data Security. PhD Thesis Abstract, College of Postgraduate Studies, Babcock University. **https://doi.org/10.61867/pcub.1(5).112**