Documents

Abdullah, H.S., Khalifa, O.O., Hashim, A.H.A.

Enhanced Mobile App Security for Healthcare Applications

(2024) *Proceedings of the 9th International Conference on Mechatronics Engineering, ICOM 2024*, pp. 177-182.

DOI: 10.1109/ICOM61675.2024.10652340

Kuliyyah of Engineering, IIUM, Department of Electrical and Computer Engineering, Kuala Lumpur, Malaysia

Abstract
As the number of mobile device usage continues to rise, the security of mobile apps is becoming an increasingly pressing concern as they have become an integral part of our daily lives. Mobile application, particularly those handling sensitive data like healthcare information, face increasing threats from malicious actors seeking unauthorized access. This paper explores the integration of Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key encryption in a healthcare application. The paper demonstrates how AES-ECC encryption can be integrated into the core of the application, creating a fortress of confidentiality and integrity. AES encryption safeguards healthcare data from unauthorized access, ensuring its confidentiality and compliance with regulations like HIPAA while ECC's efficient key management allows for shorter encryption keys, enhancing app performance in mobile app environments with limited storage and computational power. The performance of the AES-ECC setup is also tested, comparing power consumption and CPU time against scenarios where only AES encryption is used. The findings contribute to the advancement of mobile app security practices and offer insights and guidelines for developers to safeguard sensitive data against evolving cyber threats. © 2024 IEEE.

Author Keywords
AES; ECC; healthcare; mobile apps; Security

Index Keywords
Data integrity; Advanced Encryption Standard, Curve cryptography, Elliptic curve, Elliptic curve cryptography, Health care application, Healthcare, Mobile app, Performance, Security, Unauthorized access; Electronic health record

References

- Elsantil, Y.
  User Perceptions of the Security of Mobile Applications
  (2020) *International Journal of E-Services and Mobile Applications*, 12 (4), pp. 24-41.
  Oct

- *Malaysian (KLSE) Healthcare Sector Analysis*,
  Simply Wall Street Pty Ltd, Simply Wall St

- Montoya, A.O., Muñoz, M.A., Kofuji, S.T.
  Performance analysis of encryption algorithms on mobile devices
  (2013) *Proceedings-International Carnahan Conference on Security Technology*,

- Maqsood, F., Ahmed, M., Mumtaz, M., Ali, M.
  Cryptography: A Comparative Analysis for Modern Techniques
  (2017) *International Journal of Advanced Computer Science and Applications*, 8 (6).

- Ching, G.H., Zolkipli, M.F.
  Review on Cryptography Techniques in Network Security
  (2021) *Journal of ICT in Education*, 8 (2), pp. 125-135.

- Abood, O.G., Guirguis, S.K.
  A Survey on Cryptography Algorithms
  (2018) *International Journal of Scientific and Research Publications (IJSRP)*, 8 (7).

- Patel, P., Patel, R., Patel, N.
  Integrated ECC and Blowfish for Smartphone Security
  (2016) *Phys Procedia*, 78, pp. 210-216.
  no. December 2015

- Arif, A., Bin, N., Azli, S.
  (2023) *CYBERSECURITY FOR DATA TRA N SMISSIO N I N IOT*,

no. June

- Zarpelão, B.B., Miani, R.S., Kawakani, C.T., De Alvarenga, S.C.
A survey of intrusion detection in Internet of Things
(2017) *Journal of Network and Computer Applications*, 84, pp. 25-37.

- Rajaprakash, S., Karthik, K., Mohan, A., Sarkar, S., Mathew, J.
Design of new security system using RB21 algorithm
(2020) *Advances in Mathematics: Scientific Journal*, 9 (3), pp. 1149-1155.

- Cinar, A.C., Kara, T.B.
The current state and future of mobile security in the light of the recent mobile security threat reports
(2023) *Multimed Tools Appl*, 82 (13), pp. 20269-20281.

- Hasan, M.K.
A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things
(2022) *IET Communications*, 16 (5), pp. 421-432.

- Almalawi, A., Khan, A.I., Alsolami, F., Abushark, Y.B., Alfakeeh, A.S.
Managing Security of Healthcare Data for a Modern Healthcare System
(2023) *Sensors*, 23 (7), pp. 1-18.

- De Santis, F., Schauer, A., Sigl, G.
ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications
(2017) *Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017*, pp. 692-697.

- Prabu, M., Shanmugalakshmi, R.
An Overview of Side Channel Attacks and Its Countermeasures using Elliptic Curve Cryptography
(2010) *IJCSE International Journal on Computer Science and Engineering*, 2 (4), pp. 1492-1495.

- Fayyaz, U., Niazi, S.A., Aziz, A., Amin, A.
A Secured Care Service System Using AES for Internet of Medical Things
(2023) *Proceedings-2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology, ICES and T 2023*, pp. 1-4.
no. January

- Kodzo, D., Hodowu, M., Korda, D.R., Danso Ansong, E.
An Enhancement of Data Security in Cloud Computing with an Implementation of a Two-Level Cryptographic Technique, using AES and ECC Algorithm
(2020) *International Journal of Engineering Research & Technology (IJERT)*, 9, p. 2278.
no. September, [Online]

- Abarzúa, R., Valencia, C., Lòpez, J.
Survey on performance and security problems of countermeasures for passive side-channel attacks on ECC
(2021) *J Cryptogr Eng*, 11 (1), pp. 71-102.

Sponsors: IEEE
Publisher: Institute of Electrical and Electronics Engineers Inc.

Conference name: 9th International Conference on Mechatronics Engineering, ICOM 2024
Conference date: 13 August 2024 through 14 August 2024
Conference code: 202303

ISBN: 9798350349788
Language of Original Document: English
Abbreviated Source Title: Proc. Int. Conf. Mechatronics Eng., ICOM
2-s2.0-85204296051
Document Type: Conference Paper
Publication Stage: Final

Source: Scopus