UNIVERSITY TEKNOLOGI MARA

DIGITAL SIGNATURE IN E-CERTIFICATE

MUHAMMAD IQHUAN HARIIRIE BIN SUHAIMI

BACHELOR OF COMPUTER SCIENCE (Hons.)

JANUARY 2025

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, my special thanks go to my supervisor, Muhammad Atif Bin Ramlan, for his invaluable guidance, support, and patience throughout this project. Your insights and expertise were instrumental in the completion of this research.

Special appreciation also goes to my beloved parents for their unwavering support, encouragement, and prayers, which have been a constant source of strength for me.

Lastly, I'd like to express my heartfelt gratitude to my friends for their unwavering support, understanding, and encouragement. Their kindness and belief in me played a huge role in helping me complete this research.

ABSTRACT

The project implements RSA digital signatures to tackle authenticity and integrity issues with e-certificates at Universiti Teknologi MARA Kuala Terengganu's activity clubs. Users generate and sign e-certificates securely through a Next.js and Firebase-built web-based platform that provides verification capabilities. The system uses RSA digital signatures to ensure e-certificate integrity and authenticity. The system enables automatic e-certificate generation and batch signing and provides secure email distribution through the Resend API in addition to online and PDF-native verification options. Nine participants from the activity club committee with students took part in the evaluation by completing System Usability Scale (SUS) tests which yielded a score of 70.3 showing good usability. Test results from comprehensive functionality evaluation showed that essential system features operated successfully for e-certificate generation and digital signing followed by verification and distribution. Self-signed certificates used for internal university purposes successfully prevent unauthorized changes which protects e-certificates from alteration and confirms their integrity and authenticity. The practical implementation offers a usable approach toward digital credential management in educational institutions while new features can be developed in the future.

TABLE OF CONTENTS

CHAPTER 3 METHODOLOGY

CHAPTER 4 RESULT AND DISCUSSION

CHAPTER 5 CONCLUSION