PROF. MADYA DR. NUR HAFIZA BINTI ZAKARIA

PENSYARAH UNIVERSITI DS14

CONTACT

Phone: -

E-mail: mzhafiza@usim.edu.my

Faculty: Fakulti Sains Dan Teknologi

SUPERVISION

PhD - Completed: 1, O
4

Master - Completed: 0, Ongoing: 0

AREAS OF EXPERTISE

Cryptography

Other Computer Software And Services

Information, Computer And Comunication Technologies

ACADEMIC QUALIFICATION

PhD in Security In Computing (2016)

Master in Science (2012)

Bachelor in Computer Science (2009)

RESEARCH

1. OPTIMIZATION OF PARAMETERS TO IMPROVE COVER GENERATION ACCURACY FOR SECURE AUDIO STEGANOGRAPHY

2025 | GERAN PENYELIDIKAN USIM RACER | ON GOING | CO-RESEARCHER

2. ENHANCING CRYPTOGRAPHIC RESILIENCE THROUGH SYMMETRIC ENCRYPTION ALGORITHM UTILIZING VARIABLE LENGTH CHROMOSOMES GENETIC ALGORITHM

2024 | GERAN KPT | ON GOING | MAIN RESEARCHER

3. DEVELOPING CYBER SECURITY PROFESIONAL MODULES: TOWARDS DIGITAL RESILIENCE.

2024 | GERAN PENYELIDIKAN INDUSTRI | ON GOING | CO-RESEARCHER

4. HYBRID FUZZY LEAST SQUARES GENERATIVE ADVERSARIAL NETWORK (LS-GAN) BASED AUDIO STEGANOGRAPHY FOR BETTER IMPERCEPTIBILITY AND SECURITY REAL TIME PERFORMANCE.

2024 | GERAN KPT | ON GOING | CO-RESEARCHER

5. A NEW HYBRID DEEP NEURAL NETWORK MODEL FOR DETECTION OF MALWARE ATTACKS ON THE INTERNET OF MEDICAL THINGS ENVIRONMENT

2022 GERAN KPT ON GOING CO-RESEARCHER

RESEARCH

6. A NEW DNA-INSPIRED SYMMETRIC ENCRYPTION ALGORITHM FOR STRONG RANDOMNESS PROPERTIES.

2020 GERAN KPT COMPLETED MAIN RESEARCHER

7. BALANCED COVER AUDIO SUGGESTION FOR AUDIO STEGANOGRAPHY ALGORITHM BASED ON NSGA-II, SEGMENTATION AND CHAOTIC MAP

2020 GERAN KPT COMPLETED CO-RESEARCHER

8. LIGHTWEIGHT CRYPTOSYSTEM BY ADOPTING THE 3D FEATURE

2019 GERAN KPT COMPLETED CO-RESEARCHER

9. DYNAMIC S-BOX USING AFFINE TRANSFORMATION TO INCREASE THE SECURITY OF ENCRYPTION

2018 GERAN PENYELIDIKAN USIM COMPLETED MAIN RESEARCHER

PUBLICATION

1. ANALYSIS OF TRUST MODELS IN PUBLIC KEY INFRASTRUCTURE: A SYSTEMATIC LITERATURE REVIEW OF INTEROPERABILITY CHALLENGES

MALAYSIAN JOURNAL OF SCIENCE, HEALTH & TECHNOLOGY

2025 JOURNAL OTHER DATABASE CORRESPONDING AUTHOR

2. MALWARE DETECTION USING DEEP LEARNING (DL).

JOURNAL OF ADVANCED RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY

2024 JOURNAL OTHER DATABASE CORRESPONDING AUTHOR

3. SAKTI&#65533;: SECURED CHATTING TOOL THROUGH FORWARD SECRECY

JOURNAL OF ADVANCE RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY

2024 JOURNAL OTHER DATABASE MAIN AUTHOR

4. 3D LIGHTWEIGHT CRYPTOSYSTEM DESIGN FOR IOT APPLICATIONS BASED ON COMPOSITE S-BOX

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTATIONAL THINKING AND DATA SCIENCE (CTDS)

2024 JOURNAL OTHER DATABASE CO-AUTHOR

5. DESIGN AND IMPLEMENTATION OF A GENETIC ALGORITHM-BASED BLOCK CIPHER FOR ENHANCED CRYPTOGRAPHIC SECURITY

SEMINAR ANTARABANGSA ISLAM DAN SAINS (SAIS) 2024

2024 PROCEEDING NON-INDEX MAIN AUTHOR

6. A COMPARATIVE ANALYSIS OF KEY MANAGEMENT IN PKI INTEROPERABILITY USING SYSTEMATIC LITERATURE REVIEW

SCIENCE TECHNOLOGY GRADUATES COLLOQUIUM (KOSIST 2024)

2024 PROCEEDING NON-INDEX CORRESPONDING AUTHOR

7. IMPROVING DYNAMIC SECURITY OF THE LEAST SIGNIFICANT BIT USING BLOCK-BASED CHAOTIC MULTI-LEVEL LSB (BCM-LSB)

THE 9TH INTERNATIONAL CONFERENCE ON CYBER SECURITY, PRIVACY IN COMMUNICATION NETWORKS (ICCS 2023)

2024 PROCEEDING SCOPUS CORRESPONDING AUTHOR

8. SYSTEMATIC LITERATURE REVIEW: TREND ANALYSIS ON THE DESIGN OF SECURE LIGHTWEIGHT BLOCK CIPHER

JOURNAL OF KING SAUD UNIVERSITY - COMPUTER AND INFORMATION SCIENCES

2023 JOURNAL SCOPUS CO-AUTHOR

9. REPORT ON THE PHASE 1 EVALUATION OF EXISTING CRYPTOGRAPHIC ALGORITHMS (AKSA) CONSIDERED FOR MYSEAL 2.0 (VERSION 1.2)

2023 POLICY

10. LAO-3D: A SYMMETRIC LIGHTWEIGHT BLOCK CIPHER BASED ON 3D PERMUTATION FOR MOBILE ENCRYPTION APPLICATION

SYMMETRY

2022 JOURNAL SCOPUS CO-AUTHOR

11. A THEORETICAL COMPARATIVE ANALYSIS OF DNA TECHNIQUES USED IN DNA BASED CRYPTOGRAPHY

JOURNAL OF SUSTAINABILITY SCIENCE AND MANAGEMENT

2022 JOURNAL OTHER DATABASE CORRESPONDING AUTHOR

12. STATISTICAL ANALYSIS OF 3D RECTANGLE ENCRYPTION ALGORITHM

RESEARCH WORLD INTERNATIONAL CONFERENCE

2022 PROCEEDING NON-INDEX CORRESPONDING AUTHOR

13. 3D DESIGN FOR LIGHTWEIGHT S-BOX

2022 INTERNATIONAL CONFERENCE ON INNOVATIONS IN SCIENCE, ENGINEERING AND TECHNOLOGY (ICISET)

2022 PROCEEDING SCOPUS CORRESPONDING AUTHOR

PUBLICATION

14. ANALYSIS OF PERMUTATION FUNCTIONS FOR LIGHTWEIGHT BLOCK CIPHER DESIGN

8TH INTERNATIONAL CRYPTOLOGY AND INFORMATION SECURITY CONFERENCE 2022 (CRYPTOLOGY2022)

2022 PROCEEDING SCOPUS CORRESPONDING AUTHOR

15. SECURITY ANALYSIS BETWEEN STATIC AND DYNAMIC SBOXES IN BLOCK CIPHERS

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)

2021 JOURNAL MYCITE MAIN AUTHOR / CONTACT PERSON IN USIM

16. A SYSTEMATIC LITERATURE REVIEW ON LIGHTWEIGHT SECURED S-BOX DESIGN FOR MHEALTH APPLICATIONS

SELANGOR SCIENCE & TECHNOLOGY REVIEW (SESTER)

2021 JOURNAL OTHER DATABASE CO-AUTHOR

17. COMPUTING II

2021 BOOK CO-AUTHOR

18. RANDOMNESS TESTS ON NINE DATA CATEGORIES OF RECTANGLE USING NIST STATISTICAL TEST SUITE

INTERNATIONAL JOURNAL OF CRYPTOLOGY RESEARCH

2020 JOURNAL OTHER DATABASE CO-AUTHOR

19. EXTENDED RECTANGLE ALGORITHM USING 3D BIT ROTATION TO PROPOSE A NEW LIGHTWEIGHT BLOCK CIPHER FOR IOT

IEEE ACCESS

2020 JOURNAL ISI CO-AUTHOR

20. RANDOMNESS ANALYSIS ON RECTANGLE BLOCK CIPHER

CRYPTOLOGY2020

2020 JOURNAL SCOPUS CO-AUTHOR

21. RANDOMNESS ANALYSIS ON RECTANGLE BLOCK CIPHER

PROCEEDINGS OF THE 7TH INTERNATIONAL CRYPTOLOGY AND INFORMATION SECURITY CONFERENCE 2020 (CRYPTOLOGY2020)

2020 PROCEEDING NON-INDEX CO-AUTHOR

22. ENERGY METER BASED WIRELESS MONITORING SYSTEM USING BLYNK APPLICATION VIA SMARTPHONE

2020 IEEE 2ND INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE IN ENGINEERING AND TECHNOLOGY (IICAIET)

2020 PROCEEDING NON-INDEX CO-AUTHOR

23. SECURITY ANALYSIS BETWEEN STATIC AND DYNAMIC S-BOXES IN BLOCK CIPHERS

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT

2019 JOURNAL MYCITE MAIN AUTHOR

24. SECURITY ANALYSIS BETWEEN STATIC AND DYNAMIC S-BOXES IN BLOCK CIPHERS

LANGKAWI INTERNATIONAL MULTIDISCIPLINARY CONFERENCE 2019 (LIMC 2019)

2019 PROCEEDING NON-INDEX MAIN AUTHOR

25. ISSUES IN LIGHTWEIGHT ENCRYPTION ALGORITHM FOR MHEALTH

MATERIALS SCIENCE FORUM JOURNAL (Q3)

2018 JOURNAL SCOPUS CO-AUTHOR

26. STATE OF THE ART INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING

INTERNATIONAL JOURNAL OF COMMUNICATION NETWORKS AND INFORMATION SECURITY (IJCNIS)

2018 JOURNAL WOS CO-AUTHOR

PUBLICATION

27. A REVIEW ON AN INTELLIGENT HUMAN SECURITY SYSTEM USING HIDDEN MARKOV MODEL (HMM)

SEMINAR ANTARABANGSA ISLAM DAN SAINS 2018

2018 PROCEEDING NON-INDEX CO-AUTHOR

28. A REVIEW ON AN INTELLIGENT HUMAN SECURITY SYSTEM USING HIDDEN MARKOV MODEL (HMM)

CONTEMPORARY ISSUES: ISLAM & SCIENCE

2018 CHAPTER IN BOOK CO-AUTHOR

29. AN IMPROVED AES S-BOX BASED ON FIBONACCI NUMBERS AND PRIME FACTOR

INTERNATIONAL JOURNAL OF NETWORK SECURITY

2017 JOURNAL SCOPUS CO-AUTHOR

30. AN IMPROVED AES S-BOX BASED ON FIBONACCI NUMBERS AND PRIME FACTOR

INTERNATIONAL JOURNAL OF NETWORK SECURITY

2017 PROCEEDING NON-INDEX CO-AUTHOR

31. A BLOCK CIPHER BASED ON GENETIC ALGORITHM

2017 BOOK MAIN AUTHOR

32. A BLOCK CIPHER BASED ON GENETIC ALGORITHM

2017 BOOK MAIN AUTHOR

33. DESIGNING NEW BLOCK CIPHER BASED ON GENETIC ALGORITHM APPROACH.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION SECURITY

2015 JOURNAL WOS MAIN AUTHOR

34. ENHANCING ADVANCED ENCRYPTION STANDARD (AES) S-BOX GENERATION USING AFFINE TRANSFORMATION

JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY

2015 JOURNAL SCOPUS MAIN AUTHOR

35. MODIFIED A5/1 BASED STREAM CIPHER FOR MODIFIED A5/1 BASED STREAM CIPHER FOR MODIFIED A5/1 BASED STREAM CIPHER FOR MODIFIED A5/1 BASED STREAM CIPHER FOR SECURED SECURED SECURED SECURED GSM GSM GSM GSM COMMUNICATION COMMUNICATION COMMUNICATION COMMUNICATION

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY

2011 JOURNAL OTHER DATABASE MAIN AUTHOR

36. THE SECURITY LEVEL OF TWO XORED-BASED A5 CRYPTO SYSTEM

INTERNATIONAL CONFERENCE ON RESEARCH AND EDUCATION IN MATHEMATICS (ICREM).

2011 JOURNAL OTHER DATABASE MAIN AUTHOR

37. THE SECURITY LEVEL OF TWO XORED-BASED A5 CRYPTO SYSTEMS

INTERNATIONAL CONFERENCE ON RESEARCH AND EDUCATION IN MATHEMATICS (ICREM).

2011 PROCEEDING NON-INDEX MAIN AUTHOR

CONSULTATION

1. PASUKAN PERUNDING SISTEM E-WALLET (USIMPAY) USIM

USIM

2023 UNIVERSITY

2. PANEL PAKAR PENILAI ALGORITMA KRIPTOGRAFI SEDIA ADA (AKSA)

CYBER SECURITY MALAYSIA

2023 NATIONAL

3. PROJEK PEMBANGUNAN SENARAI ALGORITMA KRIPTOGRAFI TERPERCAYA NEGARA (MYSEAL)

CYBER SECURITY MALAYSIA

2017 NATIONAL

4. Perundingan - Panel Pakar Penilai MySEAL

Cyber Security Malaysia

National

AWARDS/RECOGNITION

1. ANUGERAH PENERBITAN JURNAL BERINDEKS WOS/SCOPUS/MYCITE

2025 UNIVERSITY

2. ANUGERAH PENERBITAN PROSIDING BERINDEKS WOS/SCOPUS/MYCITE

2025 UNIVERSITY

3. VISITING SCHOLAR

UNIVERSITAS MUSLIM INDONESIA

2025 INTERNATIONAL

4. A HYBRID LLM-GAN AUDIO STEGANOGRAPHY METHOD FOR SECURE MENTAL HEALTH COMMUNICATION

Final Year Project & Postgraduate (FYPP): Research & Innovation Poster Competition 2025

2025 KEBANGSAAN GOLD

5. A CLOUD-BASED HYBRID CERTIFICATE AUTHORITY MODEL INTEGRATING THRESHOLD CRYPTOGRAPHY AND TEMPORAL SHARED KEYS

INNOVATION BANK CHALLENGE 2025

2025 ANTARABANGSA SILVER

6. PSYSAFE: A HIPAA-COMPLIANT TELETHERAPY PLATFORM WITH HYBRID LLM-GAN STEGANOGRAPHIC METHOD

INNOVATION BANK CHALLENGE 2025

2025 ANTARABANGSA SILVER

7. ENHANCING CRYPTOGRAPHIC RESILIENCE THROUGH SYMMETRIC ENCRYPTION ALGORITHM UTILIZING VARIABLE LENGTH CHROMOSOMES GENETIC ALGORITHM

Final Year Project & Postgraduate (FYPP): Research & Innovation Poster Competition 2025

2025 KEBANGSAAN GOLD

8. SAKTI-CHATBOX

Malaysia Technology Expo (MTE) 2023

2023 ANTARABANGSA SILVER

9. A NEW DNA-INSPIRED SYMMETRIC ENCRYPTION ALGORITHM

INNOVATION BANK CHALLENGE 2023 (IBC2023)

2023 UNIVERSITI BRONZE

10. SAKTI: SECURE CHAT-BOX

SCIENCE AND TECHNOLOGY RESERACH EXPO (SCITEX@20TH FST)

2023 UNIVERSITI GOLD

11. GOLD AWARD - DEFENSE, SECURITY AND SUSTAINABILITY EXHIBITION 2022 (DSS 2022)

2022 NATIONAL

12. FINAL YEAR PROJECT & POSTGRADUATE: RESEARCH & INNOVATION POSTER COMPETITION (RIPC) SERIES 2/2022

2022 NATIONAL

13. 33RD INTERNATIONAL INVENTION, INNOVATION & TECHNOLOGY EXHIBITION 2022

2022 INTERNATIONAL

14. GOLD AWARD - 2ND INNOVATION BANK CHALLENGE (IBC 2022) SAKTI : SECURE APP FOR ENKRIPTING TEXT INFORMATION

2022 UNIVERSITY

AWARDS/RECOGNITION

15. GOLD AWARD - 2ND INNOVATION BANK CHALLENGE (IBC 2022)COVER-SELECTION-BASED AUDIO STEGANOGRAPHY (CAS) BASED ON LEAST SIGNIFICANT BIT (LSB) FOR BALANCED PERFORMANCE

2022 UNIVERSITY

16. SAKTI

33RD INTERNATIONAL INVENTION,INNOVATION & TECHNOLOGY EXHIBITION, MALAYSIA (ITEX'22)

2022 ANTARABANGSA SILVER

17. SAKTI: SECURE APP FOR ENKRIPTING TEXT INFORMATION

Persidangan dan Ekspo Ciptaan Institusi Pengajian Tinggi Antarabangsa (PECIPTA22)

2022 ANTARABANGSA GOLD

18. SAKTI: SECURE APP FOR ENKRIPTING TEXT INFORMATION

INNOVATION BANK CHALLENGE (IBC 2022)

2022 UNIVERSITI GOLD

19. COVER-SELECTION-BASED AUDIO STEGANOGRAPHY (CAS) BASED ON LEAST SIGNIFICANT BIT (LSB) FOR BALANCED PERFORMANCE

INNOVATION BANK CHALLENGE (IBC 2022)

2022 UNIVERSITI GOLD

20. DEVELOPMENT OF SECURE LIGHTWEIGHT BLOCK CIPHER BASED ON 3D ROTATION METHOD FOR DATA PROTECTION ON MOBILE APPLICATION

INNOVATION BANK CHALLENGE (IBC 2022)

2022 UNIVERSITI GOLD

21. SAKTI: SECURE APP FOR ENKRYPTING TEXT INFORMATION

Defence, Security and Sustainability Exhibition 2022 (DSS) National Defence University of Malaysia

2022 KEBANGSAAN GOLD

22. FAST LAB: SCIENCE EDUCATIONAL KIT

INTERNATIONAL CONFERENCE AND EXPOSITION ON INVENTIONS BY INSTITUTIONS OF HIGHER LEARNING (PECIPTA'19

2019 ANTARABANGSA GOLD

23. INTERNATIONAL UNIVERSITY CARNIVAL ON E-LEARNING (IUCEL 2018)

2018 INTERNATIONAL

24. ECOBOX - RAISING ENVIRONMENTAL AWARENESS THROUGH CODING

INVENTION,INNOVATION & DESIGN ON E-LEARNING 2018(IIDEL) UNDER THE INTERNATIONAL UNIVERSITY CARNIVAL

2018 ANTARABANGSA GOLD