UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT

Faculty of Information Science and Technology

www.ftsm.ukm.my

CENTER FOR CYBER SECURITY
FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY

RESEARCH BOOKLET

www.ftsm.ukm.my/cybersecurity

computing.ftsmukm

UNIVERSITI KEBANGSAAN MALAYSIA

UKM have been conducting research in the field of Computer Security since 2000 at the Faculty of Information Science and Technology and also at the Faculty of Engineering and Built Environment. Computer and network security issues has also gained the attention of the Center for Information Technology, UKM with the establishment of UKMCert.

Efforts to foster cooperation between UKM and Cyber Security Malaysia (CSM) has started since 2010. In 2013, an agreement was signed between UKM and CSM to implement cyber security training program in UKM. As a result of the agreement, Master of Cyber Security and Cyber Security Professional Certification programs were conducted. So far a total of 10 courses in Cyber Security have been offered every year and over 70 students attend Master of Cyber Security program. In addition, FTSM also build research collaboration with other stakeholders such as the Royal Malaysian Police (PDRM) and SIRIM Malaysia in line with the motto UKM as the Guardian of the Nation..

Previously cyber security training program in FTSM was conducted through Cyber Security Unit, which consists of a Head of Unit and a managing officer. While research and consultancy in the field of cyber security were conducted in the research laboratories at the Center of Artificial Intelligence Technology (CAIT) and the Center for Software Technology and Management (SOFTAM), FTSM.

To further strengthen the research, teaching and services in the field of cyber security in UKM, Cyber Security Center was established after the proposal was agreed unanimously in the Senate meeting dated 25 January 2017.

CYBERSECURITY @ UKM

Official collaboration between Universiti Kebangsaan Malaysia and Cyber Security Malaysia since 2013

Mission

To develop cutting-edge models and solutions of cyber resilience through research, education and consultation.

Vision

A reputable academic and frontier research center for cyber resilience that able to sustain communities and organization from modern cyber threat landscape.

Objectives

1. To drive strategic intervention on public and enterprise cyber security policies, procedures and best practices.
2. To develop innovations that focusing on the predictive, preventive, detective and responsive controls in cyber security.
3. To produce talents of professional and practitioner in cyber security.
4. To provide advisory service on the fundamental and practice aspects in relation to cyber security landscape.

ORGANIZATION CHART

Management

Chairperson
Center for Cyber Security
Assoc. Prof. Dr. Siti Norul Huda Sheikh Abdullah
Ext : 03-8921 6088

Postgraduate Programme Coordinator
Dr. Rossilawati Sulaiman

Teaching & Learning Coordinator
Assoc. Prof. Ts. Dr. Ravie Chandren a/l Muniyandi

Industry & Community Partnership Coordinator
Ts. Dr. Khairul Azmi Abu Bakar

Head of Lab

Cyber Intelligence (CI) Lab
Assoc. Prof. Dr. Masnizah Mohd

Digital Forensic (DF)Lab
Assoc. Prof. Dr. Siti Norul Huda Sheikh Abdullah

Information Governance (IG) Lab
Prof. Dr. Zawiyah Mohammad

Computer Security & Software Verification (CSSV) Lab
Prof. Ts. Dr. Zarina Shukur

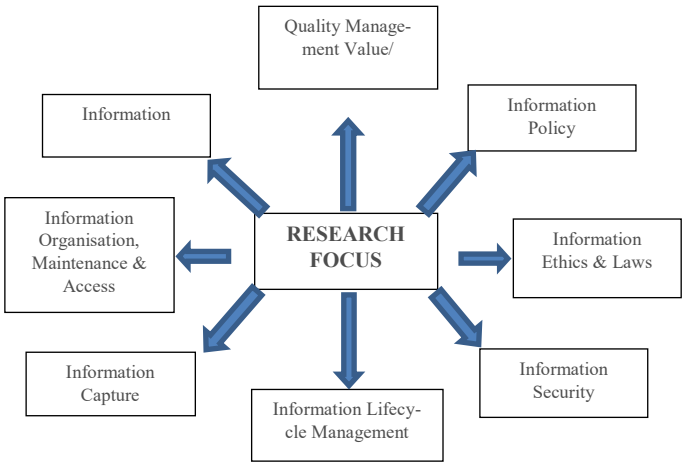
Network & Communication Technology (NCT) Lab
Assoc. Prof. Dr. Rosilah Hassan

INFORMATION GOVERNANCE RESEARCH LAB

Information governance (IG) is a holistic approach to managing information at organisational level in support of, and comply with regulatory, legal, risk, environmental and operational requirements. It implements policies, procedures, processes, roles, control, standards, metrics, technology and people where appropriate to treat information as a valuable business asset. This can means that IG refers to a policy or framework outlining acceptable behaviour for managing , organising and sharing of information. IG also seeks to determine the balance point between two diverging goals i.e. extracting the value from information and reducing the potential risk of information. This allows the organisation to reduce the legal risks associated with unmanaged or inconsistently managed information. The discipline encompasses more than conventional records and information management (RIM) when it incorporates information privacy; security dan protection; risk and compliance; audit, e-discovery; creation, preservation and deletion of information; analytics; big data; IT management; business operations; and business intelligence. IG intiative is executed with the following goals:

- Understand andpromote the value of information
- Effectively resolve information related issues and create processes to prevent future occurrences of such issues
- Define and approve information strategies, policies, and standards as well as associated procedures and metrics, and communicating them clearly
- Enforce conformance to policies and standards relating to IG

RESEARCH FOCUS



RESEARCH PROJECTS AND INNOVATION

- GUP-2017-046: Information Governance in the Gov 2-0 Environment
- FRGS/2/2014/ICT01/UKM/01/1: Electronic Records and Information Management (e-RIM) Framework for Empowering Information Governance in Public Agencies
- GUP -2014-007:Empowering Informatics Governance in Enhancing the Quality of Service Delivery of the Public Sector
- UKM-GUP-TMK-07-01-052:Antecedents of Knowledge Sharing: The Impact on Public Sector Service Delivery in Malaysia
- UKM-TT-05-FRGS0013-2006: The Development of Information Policy in Public Agencies in Malaysia
- UKM-GUP-NBT-08-29-117: The Development of Legal Records Management System
- UKM-TT-05-FRGS0013-2006: The Development of Information Policy in Public Agencies in Malaysia
- GGPM-2016-010:Function-based Records Classification: The Records and Information Management Perspective
- IP for Training Module:- Pemantauan dan penilaian pelaksanaan perancangan strategik teknologi maklumat dan komunikasi sektor awam

NETWORK

InterPARES Trust

MAMPU TOGETHER WE TRANSFORM

National Archives of Malaysia (NAM)

RESEARCHERS

Prof. Dr. Zawiyah Mohammad Yusof (Head)
Assoc. Prof. Dr. Mohamad Shanudin Zakaria
Dr. Umi Asma' Mokhtar
Mr. Ahmad Tarmizi Abdul Ghani

CONTACT :

zawiy@ukm.edu.my

LOCATION:

Level 1, Block H FTSM

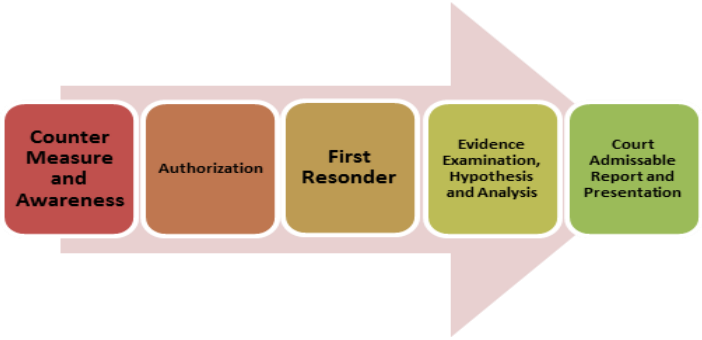
DIGITAL FORENSIC RESEARCH LAB

The word forensic is defined as a process of collecting, analysing and reporting about the data that may subsequently become evidence in the criminal justice system. Thus, digital forensic is about forensics involving the digital devices such as computers, CCTV, mobile phones, cameras and so on. With the proliferation of such equipment, the evidence is increasingly likely to be generated through such media. For example, in cases of paedophilia, incriminating evidence is often found on computers, laptops or mobile phones. With such examples, the needs for the research in digital forensics are required to help and ease the task of the law enforcement in handling, analysing and presenting the digital evidence for the criminal investigation. Digital Forensics Laboratory is responsible to overcome the problem in digital forensics area by involving with the latest research focusing on the digital forensic readiness, enhancing the current framework, developing forensics tools and towards big data and analytics of digital data.

RESEARCH FOCUS

- Data Sanitization
- Cloud Forensics
- Digital Forensics Frameworks & SOP
- Audio, Image and Video Forensics Analyst Tools
- Crowd Analytics
- Deep Learning

FRAMEWORK & ELEMENT



RESEARCH PROJECTS AND INNOVATION

- AP-2017-005/2, Using STEM data through Smart self-crime prevention at Schools for open data readiness
- GGPM-2017-024, Crowd Scenes Understanding via Convolutional Neural Network (CNN) for Visual Surveillance
- GGPM-2017-026, Tracking Social Media and Cloud Application Based On Network Packets in Computer Memory Image, UKM
- PRGS/1/2016/ICT02/UKM/02/1, Intelligent Vehicle Identity Recognition for Surveillance.
- FRGS/1/2014/ICT07/UKM/02/5, Overlapped Irregular Shape Descriptor based on Non-Linear Approach.
- DIP-2015-023, Object Descriptor via Optimized Unsupervised Learning Approaches
- ERGS/1/2013/ICT02/UKM/02/4, Geo-Temporal Crime Navigation Based On Multi-Objective Time Delay Neural Network
- AP-2017-006/4, Resilience and Regenerative Tropical Smart Building: Smart & Responsive Facade, , 01/09/2017-31/08/2017
- FRGS/1/2017/ICT04/UKM/03/1 Robotic Programming Module based on Kolb's model for Primary and Secondary Students in Strengthening Interest in STEM Education, 15/08/2017-14/08/2019
- TT-2017-006, Program Asas Rekabentuk dan Pengaturcaraan Robot, 01/11/2017-31/10/201
- GGPM-2017-024, Crowd Scenes Understanding via Convolutional Neural Network (CNN) for Visual Surveillance

NETWORK

RESEARCHERS

- Assoc. Prof. Dr. Siti Norul Huda Sheikh Abdullah
- Dr. Khairul Akram Zainol Ariffin
- Dr. Kok Ven Jyn

CONTACT :
snhsabdullah@ukm.edu.my

LOCATION:
Level 1, Block H FTSM

CYBER INTELLIGENCE RESEARCH LAB

The Cyber Intelligence (CyberIntell) lab at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia focuses on the fundamental and applied research in intelligence informatics, social media analytics, cybersecurity and, modelling and simulation.

The CyberIntell Lab has the capabilities of modelling the human in cybersecurity, social-media -based cyber-situational understanding, and intelligent information gathering and analysis.

We are also interested to apply Artificial Intelligence, Machine Learning, and Natural Language Processing into new products to make the cyberspace more secure.

"cyber health does matter"

RESEARCH FOCUS

- Cyber-intelligence informatics, modelling, and simulation
- Modelling the human in cybersecurity
- Social-media-based cyber-situational understanding
- Malware analysis
- Penetration testing and ethical hacking

RESEARCH PROJECTS AND INNOVATION

- GGPM-2017-023, Text discourse analysis on multimedia documents and an instantiation of a multifaceted structured vocabulary for the Web Images
- FRGS/1/2014/ICT02/UKM/01/1, Sentiment-based Model for Recommender Systems
- UKM-AP-ICT-21-2010, An Interactive & Personalized News Content for Crime Investigation (i-Pcrime)
- AP-2017-003/1, Enhancing Connectivity Towards Asean Integration: A Multifaceted Approach
- KRA-2017-008, Modul Graduan Ukm Global Berinovasi Futuristik Revolusi Industri Ke-4
- DCP-2017-007/4. Dana Cabaran Perdana. Sistem Pencadang Indigen berasaskan Semantik bagi Pencadangan Artikel Berita bersifat Serendipiti (2018-2020
- GGP-2017-022. Geran Galakan Penyelidikan. Romance Scam Detection (2017-2019)

NETWORK

RESEARCHERS

- Assoc. Prof. Dr. Masnizah Mohd (Head)
- Dr. Mohd Rosmadi Mokhtar
- Dr. Wan Fariza Paizi @ Fauzi
- Mr. Mohd Zamri Murah

CONTACT : masnizah.mohd@ukm.edu.my

LOCATION : Level 1, Block H FTSM

COMPUTER SECURITY AND SOFTWARE VERIFICATION RESEARCH LAB

Computer security can be defined in many ways. Some relates it with cyber security, some others with information security. Despite whatever definition it is, in this lab, our focus is on the defence technology and science for digital space. The security model that underpinned our work is the CIA triad; standing for Confidentiality, Integrity and Availability.

RESEARCH FOCUS

- Integrity
- Privacy
- Steganography
- Cryptography
- Intrusion Detection System
- Security Evaluation

LOCATION : Level 1, Block H FTSM

CONTACT : zarinashukur@ukm.edu.my

Computer Security & Software Verification

RESEARCH PROJECTS AND INNOVATION

- GGP-2017-078, A Trusted Digital Islamic Legacy Model
- FRGS/1/2015/ICT04/UKM/02/3 ,Membrane Computing to Accelerate the Processing of RNA sequence for effective cancer diagnosis
- AP-2017-003/2, Connectivity through Software Standardization: Metrology Software Certification Criteria
- FRGS/1/2016/ICT01/UKM/01/1, Process Mining Algorithm based on the Learning Automata Families for Detecting Anomalous Event
- INOVASI-2017-015, CenterYou:Upgrading to Commercial Prototype
- PRGS/1/2015/ICT01/UKM/01/1, Software Tampering Solution for Malaysian Regulated Digital Device
- INOVASI-2014-014, A Permission-Based Privacy Framework Using Pseudo Data Technique in Android Environment
- ERGS/1/2013/ICT04/UKM/01/1, SECURITY VERIFICATION FRAMEWORK FOR MOBILE OS

NETWORK

NMIM NATIONAL METROLOGY INSTITUTE OF MALAYSIA

PUSAT PERUBATAN UNIVERSITI KEBANGSAAN MALAYSIA National University of Malaysia

RESEARCHERS

- Prof. Dr. Zarina Shukur (Head)
- Assoc. Prof. Dr. Ravie Chandren Muniyandi
- Dr. Khairul Azmi Abu Bakar
- Dr. Rossilawati Sulaiman
- Dr. Zulkarnain Md. Ali

NETWORK &COMMUNIATION TECHNOLOGY LAB

We aim to be a leader in networking technology and we welcome students who desire to learn more about Networking, Information Technology, and Computer Science. At NCT lab we carry out researches that are related to latest networking technology. Theoretical and practical aspects are blended together to develop novel algorithms, architectures, and data communications methods. Our NCT lab supports recent simulation tools such as MATLAB, OMNET, NS3, OPNET, Qualnet and more. We are actively doing networking research in Cyber Security, Industry 4.0, Internet of Things, Big Data and Cloud Computing. Our recent projects are Information Centric Networking (ICN), IPv6 over Low-Power Wireless Personal Area Networks (6LowPAN), Light Fidelity (LiFi), and Mobile Application.

RESEARCH FOCUS

- Information Centric Networking
- Internet Of Things
- Light Fidelity
- Fog Computing
- Big Data
- Mobile Network

WE ARE READY FOR NEXT GENERATION NETWORKS!

Network & Communication Technology

RESEARCH PROJECTS AND INNOVATION

- Geran Arus Perdana

  Automated Medical Services via IoT, Mobile Application and Big Data Integration

- GGPM-2016-011

  Implementation of The Cluster-based Routing Protocol on Real Test Bed

- FRGS/1/2015/ICT03/UKM/02/2

  Enhancing Data Transmission Velocity and Efficiency For Big Data Analytics Initiatives in Malaysian Public Sector

- GGPM-2015-005

  Kajian Penambahbaikan Mekanisme Protokol Mobiliti IPv6 dalam Persekitaran Rangkaian Mobiliti Dual Stack

- GGPM-2014-045

  A Mobility-Aware Approach for Enforcing Cooperation in Mobile Ad Hoc Networks

- ERGS/1/2012/TK06/UKM/02/15

  Optimizing Spectrum Assignment in Wireless Communication through Dynamic Spectrum Allocation in Malaysia

- GUP-2012-043

  Optimizing Rollout Strategy of High Speed Broadband to Boost Broadband Penetration Rate in Malaysia

NETWORK

한양대학교 HANYANG UNIVERSITY

WASEDA University

UMS UNIVERSITI MALAYSIA SABAH

RESEARCHERS

Assoc. Prof. Dr. Rosilah Hassan (Head)

Dr. Azana Hafizah Mohd Aman

CONTACT : rosilah@ukm.edu.my

LOCATION : Level 1, Block H FTSM

RESEARCH SYNOPSIS

DIGITAL FORENSIC

In the course of digital forensics, the first step is to obtain the authorization from the Court or Law Enforcement Bodies before legally permissible for any searching at the crime scene. Then, the first responder process will take place to secure the evidence from the crime scene. Two types of the investigation done at the crime scene are the physical and the digital crime scenes. At the physical crime scene, the investigator has to preserve the place so that evidence can be later identified and collected by personnel trained in digital evidence identification. Next, the investigator walks through the physical crime scene, identifies the pieces of potential physical evidence, determines the extent of the search, develops a preliminary theory, and documents a narrative such as Photographs, sketches, and videos of the crime scene and the physical evidence. Once all the identified electronics have been determined, it will be transported and delivered to the digital investigation team. In contrast, the digital crime scene investigation will begin with preserving the evidence so that it can be later synchronized and analysed for further evidence. Duplication of evidence (creation of bit-by-bit copies of the seized data) should be performed for use in multiple analysis.A survey process is conducted on the digital devices to identify and separate the potentially useful data from the imaged dataset; for example, the recovery of damaged, hidden, deleted, or manipulated data. The investigative hypotheses are then developed, and in-depth analysis of the digital evidence is consecutively performed. The result will be in the format of correlation, graphing, mapping and timelining of data or files that were used to verify the various investigative hypotheses. At the end of the investigation, the investigator will document the evidence, produce a report and present it to the Court.

CYBER INTELLIGENCE

Cyber intelligence is a focus area under the Science of Security (SoS). It aims to analyze the security threats in social media networks. It also refers to the acquisition and analytics of social data, found to be useful in decision making, forecasting, tracking and monitoring to ensure cyberspace is safe. Artificial Intelligence (AI), Machine Learning (ML) and Natural Language Processing (NLP) are applied in cyber intelligence. Hence Cyber Intelligence (CyberIntell) lab are set up to support cyber security needs by focusing on social media analytics. Issues such as fraud and cyber threats are among issues that are addressed in cyber-intelligence. It focuses on the fundamental and applied research in intelligence informatics, social media analytics, cybersecurity and, modelling and simulation. It has the capabilities of modelling the human in cybersecurity, social-media-based cyber-situational understanding, and intelligent information gathering and analysis. Three important element in cyber intelligence are Human, Language and Intelligence.

1. Human Element: Human Modeling in Cyber Security

Human behaviour and emotion play an important role in the cyber domain and in formulating the basis in decision making. We aim to develop new techniques in analyzing emotions and understanding human behavior in cyber domains. This area has implications for policy making, cyber intelligence analysis and decision support.

2. Language Element: Understanding Cyber Situation Based on Social Media

Social media analytics are increasingly being used for intelligence analysis and cyber security. The development of social media techniques and analysis that combines analytic, linguistic features and advanced models to extract and analyse user views from large social media data.

3. Element of Intelligence: Informatics, Cybersecurity Modeling and Simulation

Size, speed and data diversity are growing rapidly. New techniques and systems are needed for intelligent analysis, modeling, and simulations on cyber phenomena. We aim to develop new theories, approaches and technologies to analyse data in cyber domains using AI, ML and NLP techniques.

RESEARCH SYNOPSIS

Computer Security & Software Verification

The area of digital devices is gaining popularity among users and devices providers. At the same time it attracts the attackers to exploit and get potential vulnerabilities on the devices. In smartphone operating system frameworks such as Android often missing mechanisms for active privacy control, though recent advances within context modeling, tracking and collaborative localization has resulted into the emergence of a new class involving cellphone apps that may access and reveal embedded sensor information. Among the research on digital devices, we propose a framework related to in-depth protection (CenterYou), which applies pseudo technique and cloud base decision making system to protect and scan smartphone installed applications to identify the probable privacy leakage, and in next stage the framework produce fake data or block the information that may be asked by over privilege applications. Another research focuses on the use of formal methods in verifying Androids OS security mechanism, hence propose a security verification framework for mobiles OS. A model and tool is developed for this purpose. The expected outcome of this work is a framework that enables any mobile security mechanisms to be verified earlier, without having to deploy it. We also collaborate with the National Measurement Standards Laboratory (NMSL) which is under SIRIM, is responsible for maintaining the primary standards of the country. We propose a complete solution to secure the regulated devices at two crucial stages. First stage involves new devices that first arrived at NML-SIRIM. The device functionalities and critical properties will be verified based on the given specification and NMSL requirements. Then the original code embedded in the device is extracted to preserve the authenticity of the code. Cryptography hash function is used to derive the hash of the code. This hashed code will be kept secured at NMSL for future reference. The second stage is when the device is used in the market, and if the code inside the device is changed, the hash value of this code will change (different from the original one at NMSL).

IG
INFORMATION GOVERNANCE
"Ensuring the Integrity and Authenticity of Information"

The Information Governance (IG) Lab is one of the initiatives of the Cyber Security Research Centre to support research, research trainings and teaching in information governance (IG). The Lab conducts both basic and applied research in support of concepts, methodologies and software tools for the IG. The IG is a holistic approach to managing information at organisational level in support of, and comply with regulatory, legal, risk, environmental and operational requirements. It implements policies, procedures, processes, roles, control, standards, metrics, technology and people where appropriate to treat information as a valuable business asset. Hence, the IG refers to a policy or framework outlining acceptable behaviour for managing, organising and sharing of information. IG also seeks to determine the balance point between two diverging goals i.e. extracting the value from information and reducing the potential risk of information. This allows the organisation to reduce the legal risks associated with unmanaged or inconsistently managed information. The discipline encompasses more than conventional records and information management (RIM) when it incorporates information privacy; security and protection; risk and compliance; audit, e-discovery; creation, preservation and deletion of information; analytics; big data; IT management; business operations; and business intelligence. The current area of interests in this Lab are Long Term Digital Preservation; Content Management; ICT Governance; Data Governance; Information Security; Data Privacy; Risks Management; Legal Compliance; Litigation Readiness; Business Intelligence; and Records Management. This Lab actively involved with the International Research on Permanent Authentic Records in Electronic System (InterPARES), National Archives of Malaysia and The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU).

RESEARCH SYNOPSIS

The development of network and communication technology needs endless effort due to its rapidly growing nature. Technology evolved from static to mobile, from wired to wireless, from physical to virtual and more. It is a huge challenge to modify existing technology that satisfy network and communication requirement. New terms, architecture and protocols are proposed to cater these challenges. Among those are ICN, big data, LiFi and Fog Computing.

Information-centric networking (ICN)

Transform the Internet infrastructure away from a host-centric to content-centric paradigm. Data becomes independent from location enabling in-network caching and replication. The expected benefits are improved efficiency, better scalability and better robustness in challenging communication scenarios.

Big Data

Obviously extreme large and complex data sets. Big data networking challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy and data source.

Light Fidelity (LiFi)

Wireless data transfer using LED. The main concept behind this Li Fi is the transfer of data through Illumination. It transmits data with the help of an LED bulb with a speed of actually faster than human visual capability. As the Radio Frequency spectrum is getting saturated by recent advances in wireless communications, enabling LiFi in wireless communications is a necessary revolution.

Fog computing

Uses edge devices to carry out a substantial amount of computation, storage, communication locally and routed over the internet backbone. Applications are distributed in the most logical, efficient place between the data source and the cloud it is an enhancement of cloud computing

LIST OF PUBLICATIONS

1. ABD, Maan Tareq; MOHD, Masnizah. A Comparative Study Of Word Representation Methods With Conditional Random Fields And Maximum Entropy Markov For Bio-Named Entity Recognition. Malaysian Journal of Computer Science, [S.l.], p. 15-30, dec. 2018.
2. Nadeem Alherbawi Email ShukurRossilawati Sulaiman, JPEG image classification in digital forensic via DCT coefficient analysis, Multimedia Tools and Applications, May 2018, 77(10): 12805–12835
3. Mukred, M., Yusof, Z. M., Mokhtar, U. A., & Fauzi, F. (2018). Taxonomic framework for factors influencing ERMS adoption in organisations of higher professional education. Journal of Information Science. https:// doi.org/10.1177/0165551518783133
4. Manar Abduljabbar Ahmad Mizher, Mei Choo Ang, Siti Norul Huda Sheikh Abdullah, Kok Weng Ng, (2018) An Improved Action Key Frames Extraction Algorithm for Complex Colour Video Shot Summarization, Journal of Information and Communication Technology (JICT). M. Sahri et al., "The Efficiency of Wiping Tools in Media Sanitization," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.
5. A. Alwi and K. A. Zainol Ariffin, "Information Security Risk Assessment for the Malaysian Aeronautical Information Management System," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.
6. M. A. Ibrahim, N. Marzuki, Z. Shukur and N. Zainal, "A Proposed Plan in Legalising Software for Measuring Instruments in Malaysia," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.
7. S. N. Huda Sheikh Abdullah et al., "Assessment of Self-Identity Among Teens Towards Self-Crime Prevention Program," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.
8. N. Ahmad, U. A. Mokhtar, W. Fariza Paizi Fauzi, Z. A. Othman, Y. Hakim Yeop and S. N. Huda Sheikh Abdullah, "Cyber Security Situational Awareness among Parents," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-3.
9. A. A. Ali and M. Zamri Murah, "Security Assessment of Libyan Government Websites," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.
10. S. A. binti Mohd Kasim and I. bin Mohamed, "Level of Readiness in IT Disaster Recovery Plan," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.
11. S. Kamil, M. Ayob, S. N. H. Sheikh Abdullah and Z. Ahmad, "Optimized Data Hiding in Complemented or
12. Non-Complemented Form in Video Steganography," 2018 Cyber Resilience Conference (CRC), Putrajaya,
13. Malaysia, 2018, pp. 1-4.
14. M. E. Saad and S. Norul Huda Sheikh Abdullah, "Victimization Analysis Based On Routine Activitiy Theory for Cyber-Love Scam in Malaysia," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-3.
15. M. A. F. Salah, M. Fadzli Marhusin and R. Sulaiman, "A Two-stage Malware Detection Architecture Inspired by Human Immune System," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4.

LIST OF PUBLICATIONS

16. S. Safavi, A. M. Meer, E. Keneth Joel Melanie and Z. Shukur, "Cyber Vulnerabilities on Smart Healthcare, Review and Solutions," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-5.
17. Waleed Abdel Karim Abu-Ain, Siti Norul Huda Sheikh Abdullah, Khairuddin Omar, Siti Zaharah Abd. Rahman, Automatic multi -lingual script recognition application, GEMA Online® Journal of Language Studies WOS, SCOPUS, ERA. 2018.
18. Wan Noor Aziezan Baharuddin, Siti Norul Huda Sheikh Abdullah, Shahnorbanun Sahran, Ashwaq Qasem, Rizuana Iqbal Hussain, Azizi Abdullah, Breast tissue classification via interval type 2 fuzzy logic based rough set, 2018
19. Yusri Hakim bin Yeop, Zulaiha Ali Othman, Siti Norul Huda Sheikh Abdullah, Umi Asma Mokhtar, Wan Fariza Paizi@Fauzi. BYOD implementation factors in schools: a case study in Malaysia. 2018
20. Islahuddin Jalal, Maryati Mohd Yusof, Zarina Shukur, Mohd. Rosmadi Mokhtar. A model for Afghanistan's cyber security incident response team International Journal on Advanced Science, Engineering and Information Technology SCOPUS. 2018
21. Arash Ghazvini, Zarina Shukur. A serious game for healthcare industry: information security awareness training program for Hospital Universiti Kebangsaan Malaysia International Journal of Advanced Computer Science and Applications SCOPUS. 2018
22. Azlina A. Aziz, Zawiyah M. Yusof, Umi A. Mokhtar, Dian I. Jambari, (2018). A conceptual model for document and records management system adoption in Malaysia public sector International Journal of Advanced Science, Engineering and Information Technology, 8(4): 1191-1197
23. Omar H. Salah, Zawiyah M. Yusof, Hazura Mohamed. Factors affecting customer relationship management system adoption in small and medium enterprise in Palestine (2018) International Journal of Information Systems And Engineering, 6 (2):52-75
24. Erizamsha Hassan, Zawiyah M. Yusof, Kamsuriah Ahmad. Factors influencing quality of information in Malaysian public sector and its effects on decision-making and organisational performance International Journal of Engineering and Technology
25. Maan Tareq Abd, Masnizah Mohd, A comparative study of word representation methods with conditional random fields and maximum entropy markov for bio-named entity recognition Malaysian Journal of Computer Science WOS, SCOPUS, ERA. 2018
26. Mohammad Rustom Al Nasar, Masnizah Mohd, Nazlena Mohamad Ali, Personal information management: evaluation of the PHOTO REFINDER system Advanced Science Letters ERA 2018
27. Mushtaq Mohammed Abdulnabi, Rosilah Hassan, Nor Effendy Othman, Azizah Yaacob. A fuzzy-based buffer split algorithm for buffer attack detection in internet of things Journal of Theoretical and Applied Informtion Technology SCOPUS, ERA 2018.

LIST OF COURSES

INFORMATION SECURITY MANAGEMENT (TX6144)

This course gives a conceptual overview and practical approach to information security management. It focuses on risk management, business continuity management and incident management.

FUNDAMENTALS OF DIGITAL FORENSIC (TD6104)

This course introduces the methodology of conducting digital forensics related cases, including the standards and guidelines of handling quality investigation. This course also includes forensic laboratory and challenges in present and future digital forensics.

NETWORK SECURITY (TX6124)

This course introduces the concept and knowledge of network security protocols and its applications. Topics covered include application level security, transport level security, IP security, network management security and wireless network security.

CYBER LAW & ETHICS (TX6134)

The main aim of the course is to enable participants to analyse the phenomena of cyber crime, legal and investigation/ evidential issues. This will enable participants to associate the evolution of criminal behaviour and technology advancement. Such knowledge will also inculcate the culture of cyber security and ethics among participants.

ETHICAL HACKING & PENETRATION TESTING (TX6244)

This course concerns with assessing target networks and systems to identify security vulnerabilities from both internal and external threats. Participants will learn how to perform penetration testing and ethical hacking procedures.

INTRUSION DETECTION & PREVENTION (TX6224)

The course covers methodologies, techniques and tools for monitoring events in computer network for preventing and detecting unwanted activities as well as recognizing and recovering from malicious behaviour.

SECURITY AUDIT & ASSESSMENT (TX6254)

This course introduces techniques in internal audit, and security control in ICT environment including the networks, applications and operating systems

DIGITAL MEDIA FORENSIC ANALYSIS (TD6314)

This course is about forensics analysis on various types of digital files; documents, audio, video and images. This course also discusses about file structure and analysis method. At the end of the course, participants should be able to understand digital forensics case solution and writing forensic case report.

DATA RECOVERY & ANALYSIS (TD6214)

This course introduces the fundamental of data recovery and analysis methods for different types of digital devices and scenarios. Participants will be exposed to the advance techniques and methods in analyzing evidences on cyber world. Participants will also be exposed with software tools based on artificial intelligence techniques.

CYBER THREAT INTELLIGENCE

This course will teach the student in the tactical, operational and strategic level of cyber threat intelligence skills. Further, through this course, it able to create better security teams, more efficient and accurate incident response and the student more aware of the evolving threats landscape.

CYBER SENTIMENT ANALYTICS

Analytical sentiment of social media resources could leverage the operational aspect, strategic and prediction analysis. Social media is highly potential as a vector in cyber domain. Therefore, this course discusses the analytical approach to social media focusing on cyber domain.

DIGITAL BANKING AND FINANCIAL SERVICES (TX6334)

This course aims to provide understanding on the application of technology in banking and other financial institutions. The module covers financial system components and digital banking system which consists of banking network infrastructure, bank core applications, as well as online banking. Security measures and standard practiced by banking and financial institution to ensure security of the system, will be discussed.

FINANCIAL TECHNOLOGY AND RISK (TX6344)

The module covers various type of FinTech and its risk, especially payment gateway, digital wallet. and Secure Electronic Transaction protocol. Regulations and standards that govern FinTech will also be discussed. The discussion continues with the block chain and cryptocurrency, from the perspective of security.

STRATEGIC INFORMATION

This course will give student a holistic view of information and understanding its importance as the strategic source to organizations and the strategy for managing it. This course addresses the fundamental concepts and operational issues surrounding strategic information handling in organizations, thus, It equips students with the necessary basic knowledge and competencies and the need to utilize information efficiently and effectively

CYBER SECURITY IN STRATEGIC STUDIES AND INTERNATIONAL RELATIONS

This course introduces cyber security from the disciplines of strategic and security studies. Students will be exposed to the approaches and paradigms of cyber security in the languages of politics and international security. Students will learn about cyber policy and strategy, cyber conflict ranges from cyber warfare to cyber espionage

ORGANIZATION-WIDE CYBER SECURITY STRATEGY

In this course, students will be exposed to current cyber threat through the analysis of cyber security annual reports by reputable organization

LIST OF RESEARCHERS

Prof. Dr. Zarina Shukur
Research Interest : **Formal Verification**
Email : zarinashukur@ukm.edu.my
Phone No. : +603– 8921 6669

Prof. Dr. Zawiyah Mohamad Yusof
Research Interest : **Information Governance, Knowledge management, Smart government**
Email : zawiy@ukm.edu.my | Phone No. : +603 - 8921 6198

Assoc. Prof. Dr. Siti Norul Huda Sheikh Abdullah (Chairperson)
Research Interest : **Digital Media Forensic, Computer Surveillance, Pattern Recognition, machine learning**
Email : snhsabdullah@ukm.edu.my | Phone No. : +603 - 8921 6088

Assoc. Prof. Dr. Masnizah Mohd.
Research Interest : **Information Retrieval, Topic Detection and Tracking, Natural Language Processing**
Email : masnizah.mohd @ ukm.edu.my | Phone No. : +603 - 8921 6090

Assoc. Prof. Dr. Rosilah Hassan
Research Interest : **Communication and Distributed System Architecture Computer Systems & Network Technology**
Email : rosilah @ukm.edu.my | Phone No. : +603– 8921 6186

Assoc. Prof. Dr. Ravie Chandren a/l Muniyandi
Research Interest : **Computer security, Programming & Software Testing, Natural & Distributed Computing, Process Mining**
Email : ravie@ukm.edu.my | Phone No. : +603 - 8921 6715

Assoc. Prof. Dr. Mohamad Shanudin Zakaria
Research Interest : **Pattern Recognition, Computer System Security, Service Science**
Email : msz @ukm.edu.my
Phone No. : +603 - 8921 6738

Dr. Khairul Azmi Abu Bakar
Research Interest : **Mobile Networks, Computer System Security**
Email : khairul.azmi@ukm.edu.my
Phone No. +603 - 8921 6759

LIST OF RESEARCHERS

Dr. Kok Ven Jyn
Research Interest : **Computer and Machine Vision, Pattern Recognition , Image Processing**
Email : vj.kok@ukm.edu.my
Phone No. : +603 - 8921 6810

Dr. Mohd Rosmadi Mokhtar
Research Interest : **Trusted System**
Email: mrm @ ukm.edu.my
Phone No. : +603 - 8921 6665

Dr. Rossilawati Sulaiman
Research Interest : **Applied Cryptography**
Email : rossilawati@ukm.edu.my
Phone No. : +603 - 8921 6651

Dr. Wan Fariza Paizi@Fauzi
Research Interest : **Information Processing & Management, Natural Language Processing, Semantics Technology**
Email: fariza.fauzi @ ukm.edu.my

Dr. Umi Asma' Mokhtar
Research Interest : **Record Management**
Email : umimokhtar@ukm.edu.my
Phone No. : +603 - 8921 6714

Dr. Zulkarnain Md. Ali
Research Interest : **Computer System Security, Computer Systems & Network Technology**
Email : zma@ukm.edu.myPhone | No. : +603 - 8921 6084

Dr. Ahmad Tarmizi Abdul Ghani
Research Interest : **Service Science, IT Governance**
Email: atag@ukm.edu.my
Phone No. : +6 03 - 8921 6707

Dr. Khairul Akram Zainol Ariffin
Research Interest : **Cyber Security, Digital Forensics, Data Recovery**
Email : k.akram @ukm.edu.my
Phone No. : +603 - 8921 6349

LIST OF RESEARCHERS

Dr. Azana Hafizah Mohd Aman
Research Interest : **Computer Networking, Mobile Networks Database , Computer System**
Email : azana @ukm.edu.my
Phone No. : +603– 8921 6669

Mr. Mohd Zamri Murah
Research Interest : **Web-based System Security**
Email: zamri @ ukm.edu.my
Phone No. : +6 03 - 8921 6717

ADMINISTRATION

Mohd Syazwan Baharuddin
Research Officer (Q41)
Email: syazwan@ ukm.edu.my
Phone No. : +6 03 - 8921 6089

Rustam Ikmal Ahmad Kamal
Assistant Information Technology Officer (FA29)
Email: rustam@ ukm.edu.my
Phone No. : +6 03 - 8921 6082

ACTIVITIES

CYBER RESILIENCE WORKSHOP (CRW2018), 1-2 NOVEMBER 2018,
IMPERIAL HOTEL, KUCHING SARAWAK

CYBER RESILIENCE CONFERENCE (CRC2018),
13-25 NOVEMBER 2018,
FACULTY OF INFORMATION SCIENCE & TECHNOLOGY, UKM BANGI

CENTER FOR CYBER SECURITY RESEARCHERS

MASTER IN CYBER SECURITY STUDENTS

Networking

Assoc. Prof. Dr. Siti Norul Huda Sheikh Abdullah

Center for Cyber Security (CYBER)
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor Darul Ehsan, Malaysia
03-8921 6082 / 6090 / 6088
03-8921 6094
cybercenter@ukm.edu.my / snhsabdullah@ukm.edu.my

Dean

Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor Darul Ehsan, Malaysia
03-8921 6173 / 6172
03-8925 6732
dftsm@ukm.edu.my

Scan me

www.ftsm.ukm.my/cybersecurity