Abstracts of Papers
Presented at

The 24th Information Security for South Africa Conference

Century City Conference Centre (CCCC),
Cape Town, South Africa,
1 – 2 December 2025

Edited
by
Mariki Eloff

Introduction

This booklet contains the abstracts of all accepted papers for the ISSA 2025 Conference. Abstracts are listed alphabetically according to their title.

The ISSA conference is co-organised by the Department Computer Science of the University of Pretoria, Centre for High Performance Computing (CHPC), Data Intensive Research Initiative of South Africa (DIRISA) and South African National Research Network (SANReN). ISSA runs as a parallel stream at the well-established annual Centre for High Performance Computing Conference: (https://chpcconf.co.za/).

All papers have been double-blind peer reviewed before final submission to the conference. Final papers will be published in *Communications in Computer and Information Science* by Springer as post conference proceedings.

Program Committee:

Prof Jan Eloff	University of Pretoria
Prof Hein Venter	University of Pretoria
Prof Reinhardt Botha	Nelson Mandela University & Noroff University College
Prof Mariki Eloff	University of Pretoria
Prof Renier van Heerden	SANReN, NICIS, CSIR

Contents

A Holistic Cyber Security Readiness Assessment Tool for Organisations in Developing Countries

Raymond Agyemang [0009-0000-3332-6128], Steven Furnell[0000-0003-0984-7542], and Tim Muller[0000-0003-1263-4230]
University of Nottingham, Nottingham, UK
raymond.agyemang@nottingham.ac.uk

Abstract. Organisations in developing countries face uneven cybersecurity readiness shaped by national laws, institutional capacity and market conditions. This paper proposes a Holistic Cybersecurity Readiness Assessment (CSRA) that links an External Cybersecurity Environment Assessment (Tier 1) with an Internal Readiness Self-Assessment (Tier 2) across governance, people, pro-cess and technology. The tool integrates a structured review of standards and national initiatives with practitioner input to derive profiling dimensions and factors of relevance. The paper presents the instrument design, scoring approach, and reports an initial pilot to examine face and content validity The contribution is a practicable method that aligns organisational control priorities with the external context so that improvement plans are defensible and sequenced. Early findings suggest the two-tier linkage clarifies dependencies be-tween regulation, capacity and internal practices. The paper concludes with limitations and next steps for broader validation across multiple national settings.

A Qualitative Review of Zero-Knowledge Proofs and Bio-metrics in Decentralized Identity Systems

Kedimotse Baruni, Sthembile Ntshangase, Harvest Ngobeni, Lesego Moatshe and Nomalisa Ndhlovu
The Council for Scientific and Industrial Research, Pretoria, South Africa
kbaruni@csir.co.za

Abstract. This paper presents a qualitative review of the integration of Zero-Knowledge Proofs (ZKPs) and biometrics in Decentralized Identity (DID) systems. It explores how these technologies address key challenges in digital identity management, including privacy preservation, security enhancement, and regulatory compliance. Using three research questions, the study systematically reviews the recent literature to identify the problems these technologies solve, the sectors where they are applied, and the standards that govern their implementation. The review further reveals that ZKPs-DID is the most widely adopted method, dominating finance and governance applications, while Bio-DID focuses on healthcare and education under GDPR, and BioZK-DID combines biometrics with ZKPs for enhanced security but with limited regulatory guidance. The findings reveal that ZKPs enable privacy-preserving verification, while biometrics offer robust user-specific authentication. Integration within DID systems is particularly relevant in sectors such as finance, healthcare, governance, and education. However, challenges remain in scalability, interoperability, and regulatory alignment. This paper contributes new insights by proposing technical guidelines, policy recommendations, and future research directions to support the ethical and effective deployment of ZKP-biometric-enabled DID systems.

A Trust Framework for Peer-to-Peer Energy Markets

Boitumelo Leotlela[1,2][0009-0008-5863-9356] Lehlogonolo Ledwaba[2][0000-0002-7292-2835] and Marijke Coetzee[1][0000-0002-9157-3079]
[1] North-West University, Potchefstroom 2531, South Africa
[2]Council of Scientific and Industrial Research, Meiring Naude Rd, Pretoria, 0184, South Africa
{tleotlela, lledwaba4}@csir.co.za, Marijke.coetzee@nwu.ac.za

Abstract. Peer-to-peer energy markets rely on trust to enable secure participation; however existing trust models often address only isolated trust concerns. This fragmented approach leaves significant gaps in ensuring holistic trust across the peer-to-peer energy market and exposes participants to threats in the market. To address this, the paper proposes a trust framework grounded in the Trust over IP (ToIP) model, which integrates technical mechanisms and governance policies to sustain trust in decentralised environments. Using the STRIDE threat model, key threats in the peer-to-peer energy market are identified, while also analysing how existing research mitigates these risks. The corresponding trust and security mechanisms are then mapped to the ToIP architecture, offering a comprehensive approach to trust establishment, that unifies social-behavioural and security dimensions of trust. By leveraging ToIP as a formal foundation for trust establishment in this work, the proposed framework provides a holistic approach to building and maintaining trust in the market, thereby fostering greater user confidence and encouraging broader market participation.

Adaptive−Delta ADWIN for Real−Time Intrusion Detection in Evolving Network Streams

Rodney Sebopelo [0000-0002-1291-1173]
School of Computer Science and Information Systems,
Northwest University, Potchefstroom Campus, South Africa
Rodney.Sebopelo@nwu.ac.za

Abstract. In dynamic network environments, intrusion detection systems (IDS) must adapt to traffic network patterns despite the challenge of concept drift. Traditional drift detection methods, such as ADWIN, DDM, and others, face a challenge between sensitivity and stability, resulting in both delayed traffic attack detection and abnormal false alarms. To address this issue, we propose a novel framework − Adaptive−Delta ADWIN, which adjusts the ADWIN detector's delta parameter using two lightweight online controllers: Volatility Controller (VC) which adapts to fluctuations in prediction error, and Alert−rate Controller (ARC), which control the frequency of drift alarms. We merge the adaptive detector into streaming ensemble of Hoeffding Adaptive Trees and evaluate its performance against a fixed−delta baseline. The proposed metrics: accuracy, ROU-AUC, F1-score are monitored in real time performance. The results from the experiment demonstrate the effectiveness and responsiveness of the Adaptive−Delta ADWIN framework in handling concept drift while reducing false alarms and balancing sensitivity with stability in IDS streaming environments. The framework provides a foundation for future multi−class extensions capable of distinguishing specific attack types in real time.

Aligning cybersecurity education with industry needs: Bridging South Africa's skills development

Marijke Coetzee [0000-0002-9157-3079] Michael de Jager [0009-0004-3846-2304]
Lynette Drevin [0000-0001-9370-8216] Hennie Kruger [0000-0001-8514-4422]
School of Computer Science and Information Systems,
North-West University, South Africa
{marijke.coetzee, michael.dejager, lynette.drevin, hennie.kruger}@nwu.ac.za

Abstract. South Africa faces a critical shortage of cybersecurity professionals. This paper examines the nature of the cybersecurity skills gaps by reviewing re-cent studies and presenting the findings of a recent survey. Findings highlight the importance of practical, hands-on training, embedded certification pathways, and curricula aligned with market demands. Students similarly seek a relevant qualification to enhance their careers, offer hands-on learning, embed certifications, and provide flexible and affordable delivery. To address these needs, the study evaluates two international cybersecurity knowledge frameworks: the ACM Cybersecurity Curricula Guidelines 2017 (CSEC2017) and the Cyber Security Body of Knowledge (CyBOK). Adopting and localising these frameworks can guide the development of a South African cybersecurity postgraduate qualification that is globally benchmarked yet tailored to local threats, legislation, and workforce requirements. By bridging the gap between academic preparation and industry expectations, the study aims to enhance the nation's capacity to respond to evolving cybersecurity challenges.

Assessing Undergraduate Students' Knowledge of Cyber-security at a Public South African University

Errol Baloyi [1, 2][0009-0009-6959-3485] Bertram Haskins [2, 3][0000-0002-9762-7381] and
Kerry-Lynn Thomson [2][0000-0002-6456-9701]
[1] Council for Scientific and Industrial Research, Pretoria, South Africa
[2] Nelson Mandela University, Summerstrand, Gqeberha, South Africa
[3] Noroff University College, Tordenskjoldsgate 9, 4612, Kristiansand S, Norway
ebaloyi2@csir.co.za, bertram.haskins@noroff.no, kerry-lynn.thomson@mandela.ac.za

Abstract. The increasing reliance on the Internet has exposed the triad of cyber-security, namely, people, processes, and technology, to various cyberattacks. Moreover, factors such as the Coronavirus Disease 2019 (COVID-19) pandemic have contributed to the rise in these attacks. Students, who are heavy Internet users, are not immune to these cyberattacks. Several studies have identified stu-dents as primary targets of cyberattacks at Higher Education Institutions (HEIs), largely due to their limited knowledge of how to protect themselves online. As a result, this study investigated the Cybersecurity Awareness (CSA) of undergraduate students at a South African public HEI. The objective was to measure their awareness levels of cybersecurity concepts through a quantitative survey. The sample consisted of students from seven faculties. The instrument assessed students' awareness across several cybersecurity concepts: phishing, antivirus, identity theft, cyberbullying, piracy, password security, and malware. A total of 381 responses were collected and subjected to statistical analysis. The findings indi-cated that while students demonstrated strong awareness in identity theft and cyberbullying, significant deficiencies were observed in phishing, password management, and

antivirus usage. These findings have significant implications for curriculum development in HEIs, the formulation of institutional cybersecurity policies, and the advancement of national cybersecurity strategies. Further-more, this study contributes to the limited body of research on CSA within the higher education context.

CerebRAN: A Dynamic Behavioural Dataset for Ransomware Detection

Emmanuel Musiiwa[1], Stones Dalitso Chindipha and Moses Moyo
Rhodes University, Grahamstown, South Africa,
[1] g20m4048 campus.ru.ac.za, {s.chindipha, moses.moyo}@ru.ac.za

Abstract. Ransomware remains a significant cyber threat; however, research is often hindered by a lack of modern, well-balanced datasets. This study proposes CerebRAN, a new dataset created through the dynamic analysis of ransomware (400 samples) and goodware (399 samples). We provide a detailed methodology, from sample collection to feature extraction, using the Cuckoo Sandbox on a Windows 7 operating system. To validate the usability of CerebRAN, we conducted machine learning experiments using Random Forests (RF) and Logistic Regression (LR) with the Recursive Feature Elimination and Cross-Validation (RFECV) technique. The results obtained from the experiments show that the RF was the superior classifier, with a CerebRAN scoring accuracy of 0.9625, precision of 0.9628, recall of 0.9625, and F1-score of 0.9625. LR scored an accuracy of 0.9562, precision of 0.9563, recall of 0.9563 and an F1-score of 0.9562. RF outperformed LR using an optimum of 48 features, while LR used 174 features. This experiment highlighted the effectiveness and value of CerebRAN in developing robust detection tools. The dataset and sample metadata are publicly available on GitHub4.

Correlating Memory, Persistent, and Runtime Evidence in Redis

Muhammad Abdul Moiz Zia[1] and Oluwasola Mary Adedayo[2]
[1] Department of Applied Computer Science, The University of Winnipeg, Winnipeg,
R3B 2E9, Manitoba, Canada
[1] zia-m25@webmail.uwinnipeg.ca .[2] m.adedayo@uwinnipeg.ca

Abstract. Databases are an important source of digital evidence, but most forensic methods and tools are focused on relational database systems. In-memory NoSQL databases, such as Redis, are harder to investigate because persistence files and logs capture only parts of the activities, while crucial volatile evidence exists in memory. This paper presents a technique and parser to bring multiple Redis sources: memory snapshots, RDB, AOF, MONITOR, ACL logs, and SLOWLOG together. Three experiments were carried out. The first tested recovery of short and long values from memory, showing that command arguments can be extracted

from an offset even when not preserved in persistence. The second measured coverage across individual sources and demonstrates that combining them gives a broader view of the investigation. The third examines a master-replica scenario, where the parser recovers missing operations by matching memory with monitor logs. Our findings show that cross-source artifact correlation improves completeness in Redis forensic analysis.

Ethical Boundaries of Plagiarism Detection in the Age of AI

Rowen Carl Robinson[1] and Bobby L. Tait[2]
College of Science, Engineering and Technology (CSET),
University of South Africa, Pretoria, South Africa
[1] rowencarlrobinson@gmail.com, 2 Taitbl@unisa.ac.za

Abstract. This paper explores the ethical boundaries of plagiarism detection in the age of artificial intelligence (AI), focusing on the rise of AI-generated text and its implications for academic integrity. While plagiarism detection has traditionally relied on string-matching and authorship attribution, the emergence of generative models like GPT-4 challenges these methods. Institutions now face a dual imperative: uphold fairness and accountability while respecting privacy, transparency, and due process. This paper reviews the evolution of detection systems, contextualizes them within cybersecurity frameworks, and analyzes ethical tensions through global policy comparisons and case scenarios. A conceptual model of AI-enabled detection is presented, alongside a comparative table of international data protection laws. The paper argues for a balanced governance approach that integrates human judgment, safeguards student rights, and acknowledges cultural diversity in plagiarism norms. Recommendations include hybrid detection-prevention strategies, transparent algorithms, and ethics-informed policy design. Ultimately, the goal is to ensure that detection systems serve the goals of education rather than undermine them.

Ethical principles and social implications of generative AI

Clarissa Weyer[1] [0009-0000-0017-2150] Marijke Coetzee[2] [0000-0002-9157-3079] and Hennie Krüger[3] [0000-0001-8514-4422]

[1,2,3] North-West University, Potchefstroom, 2520, South Africa
[1]34252835@mynwu.ac.za,[2]Marijke.Coetzee@nwu.ac.za, [3]Hennie.Kruger@nwu.ac.za

Abstract Generative Artificial Intelligence has rapidly evolved, transforming numerous sectors. While its potential benefits are widely acknowledged, there are growing concerns about its ethical and societal implications. This paper presents a semi systematic literature review aimed at identifying ethical principles and the impacts of generative AI. This article synthesises key themes related to fairness, accountability, transparency, privacy, and plagiarism, as well as broader societal concerns including job displacement, misinformation, overreliance and digital divide. The findings contribute to ongoing debates in AI governance, policy formulation, and ethical AI design, and offer a foundation for future research in managing the risks and reducing societal impact of generative AI.

Guiding Principles to enhance cybercrime investigative capacity in law enforcement agencies

Aluta V. Dyasi[1[0009−0002−6363−0715]], Bertram Haskins[1,2[0000−0002−9762−7381]], and Reinhardt A. Botha[1,2[0000−0002−6176−3007]]
[1] CRICS, School of IT, Nelson Mandela University, Gqeberha, South Africa
alutadyasi@gmail.com
[2] Noroff University College, Tordenskjoldsgate 9, 4612, Kristiansand S, Norway
{bertram.haskins,reinhardt.botha}@noroff.no

Abstract. Cybercrime poses a significant threat, presenting a unique challenge to law enforcement agencies worldwide. The transnational nature and technical complexity are fundamental challenges that create difficulties in investigating cybercrime, despite advancements in legislation. An Interpol 2025 African Cyberthreat Assessment Report highlights that cyber-related offences continue to increase, while countries report critical gaps in investigative capacity. This study used an extensive literature review to identify several factors that impact investigative capacity. Through reasoning, the factors were synthesised into a list of seven guiding principles. These principles can help shape interventions that address existing gaps in investigative capacity in law enforcement agencies.

Optimising Synthetic Data Generation for Cybersecurity Datasets

Christian K. Devraj and Jan Eloff
Cybersecurity Research Group (CySec), Department Computer Science,
University of Pretoria, Pretoria, South Africa
u20504552@tuks.co.za, jan.eloff@up.ac.za

Abstract. In recent years, cybercrimes have become more prevalent and impactful for all users of modern technology. Consequently, various artificial-intelligence-driven intrusion detection software have been implemented to detect and prevent such cyberattacks. Some well-known tools include Microsoft's Security Copilot and SentinelOne's Singularity. However, such AI tools are of-ten difficult to train and maintain, primarily because of the lack of available cybersecurity datasets. Furthermore, even when real cybersecurity datasets are collected, they may lack balance, reliability, and variety, rendering them inefficient for training cybersecurity AI-based tools such as intrusion detection tools. A trending solution to this predicament is synthetic data generation, particularly for meeting commercial cybersecurity dataset requirements. However, synthetic data generation simply mimics the structure and content of real datasets and of-ten reproduces the poor characteristics of real datasets. Therefore, this study proposes the inclusion of Data Quality Metrics and Data Optimisation techniques during the synthetic data generation process to improve the quality of synthetic cybersecurity datasets. At the pinnacle of this research, an optimal process for producing synthetic datasets for cybersecurity research is proposed.

Personal Information Disclosure on Facebook: An Exploratory Study of Demographic differences of first-year IT students at Nelson Mandela University

Asavela Ndzondzo[1], Kerry-Lynn Thomson[1] and Reinhardt A. Botha[1,2]
[1] Department of Information Technology, Nelson Mandela University, Gqeberha, South Africa
{Asavela.Ndzondzo, Kerry-Lynn.Thomson}@mandela.ac.za
[2] Noroff University College
Reinhardt.Botha@noroff.no

Abstract. This study is an exploratory study to understand the role of gender, home area, and high school area in Willingness to disclose personal information, Benefits, Privacy Risks, Subjective Norms, and Perceived Behavioural Control. This study used Privacy Calculus and the Theory of Planned Behaviour to for-mulate a five-construct questionnaire. Data was collected from a sample of 133 first-year IT students at Nelson Mandela University. The results of the study in-dicate that males are more likely to disclose personal information on Facebook compared to females, and they perceive more Benefits. Additionally, males are more likely to be influenced by others to disclose personal information compared to females. Surprisingly, gender has no significant impact on Privacy Risks and Perceived Behavioural Control. Secondly, students in a Rural area are more will-ing to disclose their personal information on Facebook compared to those in an Urban or Suburban area, they perceive more Benefits compared to those in an Urban or Suburban area, and students in an Urban or Suburban area are more aware of Privacy Risks compared to students in a Rural area. Home Area has no significant impact on Subjective Norms and Perceived Behavioural Control. Lastly, students from Rural high schools perceive more Benefits, and they are more likely to be influenced by others compared to those in Urban or Suburban areas. The high school area has no significant influence on Willingness to dis-close personal information, Privacy Risks and Perceived Behavioural Control.

The Effect of Cybersecurity Fatigue on Employees' Compliance with **Cybersecurity Measures**

Luyanda Mtombeni[1], Wallace Chigona[2][0000-0002-1059-811X] and Teofelus Tuyeni[3][0000-0001-5775-1399]

[1] University of Cape Town, Cape Town, South Africa
[1] mtmluy004@myuct.ac.za, [2] wallace.chigona@uct.ac.za, [3] tynteo002@myuct.ac.za

Abstract. In the modern digital era, cybersecurity has emerged as a critical domain, shaping the security landscape of organisations worldwide. As technological advance-ments redefine how businesses and individuals operate and interact, the need for robust cybersecurity measures become increasingly apparent. The purpose of this research is to explain the effect of cybersecurity fatigue on employees' compli-ance with cybersecurity measures. Cybersecurity fatigue can cause employees to become disengaged from cybersecurity activities, leading to non-compliance. Empirical studies explaining the effect of cybersecurity fatigue on compliance with cybersecurity measures are relatively scarce. The study employed a qualita-tive case study approach. We purposely sampled 11 employees from a single or-ganisation to collect data. The data was analysed using the NVivo software tool. The findings indicate that cybersecurity

fatigue leads to frustration and irritation, which results in negative perceptions of cybersecurity and non-compliant actions, such as ignoring cybersecurity requirements. Additionally, organisational culture and individual factors influence the effects of cybersecurity fatigue. This research seeks to encourage employees' compliance with cybersecurity measures.

Unpacking the effects of Cyber Fraud on Financial Aid students in South Africa

Gershon Hutchinson[1][0009-0000-5232-5497] and Salah Kabanda[2][0000-0002-0490-8417]
[1,2] University of Cape Town, Cape Town, South Africa
htcger001@myuct.ac.za, salah.kabanda@uct.ac.za

Abstract. Due to the exponential growth of the internet, cyber fraud has be-come an increasingly prevalent issue globally, and South Africa is no exception. While several studies address cyber fraud victims, limited research has specifi-cally examined students, particularly those from disadvantaged backgrounds re-ceiving the National Student Financial Aid Scheme (NSFAS), as victims of cyber fraud. Financial aid is critical to enabling higher education for many South African students, making it crucial to understand the effects of cyber fraud on this group. This study has three key objectives: first, to understand how South African higher education financial aid students perceive cyber fraud; second, to identify the perceived events that led to cyber fraud of affected stu-dents; and finally, to understand the effects of cyber fraud on this group of students.
The study used a qualitative research design with purposive and snowball sampling to select participants. Semi-structured interviews were conducted with 30 participants. Thematic analysis was employed for data analysis. The findings underscore the urgent need for training and awareness programs tailored explic-itly for financial aid students, particularly those receiving financial aid for the first time. Beyond the immediate financial losses, the study highlights the ad-verse effects experienced by affected students and emphasises the crucial role of support systems in determining students' academic success.