Issues in Information Systems
Volume 26, Issue 2, pp. 14-27, 2025

DOI: https://doi.org/10.48009/2_iis_102

Factors influencing the integration of digital forensics with student information management systems

Alvino Moses, *Cape Peninsula University of Technology*, *mosesa@cput.ac.za*
Tiko Iyamu, *Cape Peninsula University of Technology*, *iyamut@cput.ac.za*

Abstract

Despite the criticality of student information management systems (SIMS), the system is continually confronted with technical glitches such as data breaches, which affect monitoring and evaluation of students' academic performances, resulting in inappropriate validation of academic accreditation and data manipulation. Subsequently, integration of digital forensics with SIMS is argued as the solution. however, the problem persists, primarily because the influencing factors are unknown. The qualitative approach was applied, and existing materials were used as data in the study. This study employed activity theory (AT) as a lens to examine the challenges and gain a deeper understanding of the influencing factors. Data security, relationship, governance, digitalisation, and co-existence were revealed as the factors influencing the integration of digital forensics with SIMS. The study extends to highlight the manifestation of the factors into attributes.

Keywords: student information management systems, digital forensics, data breaches, activity theory

Introduction

Student Information Management Systems (SIMS) is also referred to as a student management system within South African academic institutions. SIMS is critical for the operational and strategic management of academic activities, from both decision-making and information sharing perspectives, in higher education institutions (HEI). SIMS is a collection of steps, activities and functions which facilitate the recovery, storage, processing, and use of student accounts to access and manage information such as final marks and fulfilment of graduation requirements (Mazadu et al., 2022; Magara, 2006). SIMS, therefore, presents several advantages that aid in augmenting transparency, resource allocation, and risk management (Kock et al., 2020; Mazadu et al., 2022). Additionally, the system enhances data reliability and facilitates the governance of data-driven activities of university management (Liu et al., 2010; Daim et al., 2024).

Higher Education Institutions (HEI's) in South Africa are increasingly relying on SIMS to gain insights into the monitoring and evaluation of students' academic performances, including accreditation and graduation processes (Gürkut et al., 2023). However, there is a fundamental problem, which is, SIMS cannot prevent data breaches (Astaman & Mauritsius, 2023). Insofar, there are three consequences associated with the problem: (1) information theft, resulting in inappropriate validation of academic accreditation leading to graduation of unqualified students (Daraghmi et al, 2019); (2) data manipulation, which misrepresents statistical information for national development and growth (Daim et al., 2024); and

(3) disbursement of funds is increasingly unbalanced due to inaccurate information obtained from the system.

Due to the criticality of SIMS' features and reliability, the system is used by administrative staff, academic staff, and students. It can be relied upon for information validation and managerial decisions by providing real-time data regarding student academic performance (Gürkut et al., 2023). As a result, SIMS is increasingly an important enabler for effective and efficient administrative decision-making in HEI (Kundy & Lyimo, 2019; Kifaru et al., 2023). Despite the criticality of the SIMS, there are many challenges with the system, from hacking to infiltration, through which data is manipulated and falsified. These intrusion activities often happen through the internet (Moallem, 2019). According to Mtambeka et al. (2023), staff and students are involved in the contravention of university cybersecurity measures, such as information and security credentials, including policies on malware and anti-virus. Thus, digital forensics is required to enhance and maintain the reliability of the HEIs' data and their integrity, including the qualifications they produce.

Digital forensics techniques, methods and tools are being employed to assist with investigations due to the prevalence of computers being gradually manipulated by cybercriminals (Cook et al., 2023). Digital forensics tools and techniques are increasingly used to safeguard information in the online space as staff and students fall within the ambit of protection of intellectual property rights (Johnson et al., 2022). Digital forensics has achieved major attention from researchers and practitioners alike as it accentuates an important role in cybersecurity (Casino et al., 2022). There have been some breakthroughs in countering cybercrimes using the tools (Alghamdi, 2021). Digital forensics is a subset of cybersecurity that concentrates on retrieving evidence detected on digital platforms that either assists or disputes a security breach (Flores et al., 2021).

Thus, there is a need to employ the digital forensics approach in proposing a solution to the problem. To do this, it requires integrating digital forensic tools with SIMS to detect errors and conscious or unconscious illegitimate actions by cybercriminals. Thus, the objective of this study was to gain an understanding of the factors that could influence the integration. Corroboratively, the research question was: What are the factors that influence the integration of digital forensics with SIMS? The integration of digital forensics with SIMS facilitates a set of criteria and guidelines from both technology and academic-business perspectives. However, the factors influencing the integration of digital forensics with SIMS remain challenging. Thus, the research question is: What are the factors that can influence the integration of digital forensics with the SIMS? The study, therefore, aimed to help gain a better understanding of the factors that influence how digital forensics can be integrated with the SIMS in South African higher institutions.

Literature review

The literature review covers the core aspects of the study, which are student information management systems, digital forensics, and solution integration. Student Information Management System (SIMS) is also referred to as a student management system. The system is innovative software which streamlines student data by consolidating all information into a single platform and is accessible by staff and students (Mthembu, 2022). In some South African institutions, the implementation of SIMS is one of the biggest investments (Suwardi, 2007). As a result, there is an expectation to significantly improve efficiency and effectiveness, including the quality of services provided to staff and students (Semeon et al., 2010). Hamad (2023) describes SIMS as one of the most active and well-functioning information systems in HEI's. This argument could be attributed to the use of SIMS in accessing real-time data regarding students' academic activities, including performances, for operations and institutional strategic decision-making. Gürkut et al.

(2023) summarised the importance of SIMS in HEIs as organising and managing student data, faculty data, classroom data, and the administration of academic courses, for decision-making.

Despite the criticality of SIMS, there are challenges in using the system. Data security is one of the key challenges with SIMS. Higher education institutions are becoming primary targets from a cybercriminal perspective because of insufficient awareness of data security, as their systems store abundant personal and research data (Hina & Dominic, 2018; Li et al., 2023). The data security challenge exposes students' information to unauthorised access and cyber threats (Taha & Dahabiyeh, 2021; Mtambeka et al, 2023). This challenge is increasingly a concern to many HEI's; hence, some studies have been conducted. Data breach risks are widespread at higher education institutions, and in 2021, data breaches escalated to record-high levels (Li et al., 2023; Verizon, 2022).

Based on existing literature, the most vulnerable element remains the human element, which is exploited by cybercriminals through malware attacks, phishing emails, and social engineering to access the critical infrastructure of organisations. Inadequate awareness of data security due to human errors can also cause data breaches due to negligent security measures and inaccurate data handling (Ulven & Wangen, 2021; Li et al., 2023). Amoresano et al. (2023) argued that human errors unabatedly remain a critical factor contributing to the increasing attacks on IT solutions and data breaches despite precautionary and preventative measures. Since data breaches are increasingly prevalent through digital including cyber threats, hence, it is increasingly essential to employ digital forensics.

Digital Forensics

Digital forensics is a methodology to reconstruct malicious activities using scientifically recognised techniques to preserve, identify, acquire, analyse, understand and document root cause analysis of digital artefacts (Kebande & Venter, 2015; Serketzis et al., 2018). Substantial evidence exists that digital forensics has evolved in the last four decades. Over the years, digital forensics has increased swiftly as organisations continue to depend on information technology (Valjarevic & Venter, 2015). Digital forensics entails a complex process that involves the acquisition, examination, and analysis of various data sets (Khalaf & Varol, 2019; Blancaflor et al., 2023). The analysis enables traces and an understanding of data security breaches including system weaknesses and vulnerabilities (Wang et al., 2024).

Conducting digital forensics on data sets is fundamental. However, it is often confronted with a myriad of challenges when integrating with other solutions such as encryption, anti-forensic techniques, and big data (Thakar et al., 2021). Additionally, machine learning (ML) and artificial intelligence (AI) perform essential roles within the realm of digital forensics by efficiently processing a variety, unprecedented velocity and a large volume of data in conducting assessment and analysis (Dunsin et al., 2024).

Solution Integration

In the context of this study, neither SIMS nor digital forensics can work alone. Therefore, both solutions need to be integrated. For example, organisations can be forensically equipped in situations where it has limited control over individuals by using digital forensic readiness, which is a proactive approach (Kigwana & Venter, 2018). According to Farjon, Smits and Voogt (2019), the integration of digital technology into education is, however, becoming so widespread that it seems inevitable. Li and Tuunanen (2022) suggest that integration is vital because it can be used to gather insights into the involved actors, activities, and interconnected relationships. Due to its importance, Information systems and technology scholars have continued to investigate integration from various perspectives, such as data sources and enterprise (He, Zhang & Li, 2021). Atabek (2020) argues that despite the efforts and investments, there are challenges with the integration of technology.

Integration challenges are in many areas of IT solutions. From multiple data perspectives, He et al. (2021) stated that integration continues to be a challenge in promoting interoperability. Thus, if the integration is not effective, it can potentially weaken the anticipated advantages and might highlight severe challenges (Gyawali & Mehndroo, 2024). According to Johnson et al. (2022), there is currently no evidence of digital forensic deployment in an academic environment, even though a proof-of-concept process was conducted. Atabek (2020) argues that although the factors affecting technology integration are known, challenges persist. Thus, this study pays attention to integration to avoid derailments of its objectives.

Theoretical Framework

Theoretical frameworks from a social system viewpoint offer fresh perspectives and various meanings to phenomena being studied (Iyamu, 2021). This guides the researcher in gaining deeper insights and providing an in-depth explanation concerning the phenomenon being studied (Mueller & Urbach, 2013; Tsang & Ellsaesser, 2011). Thus, activity theory (AT), a sociotechnical theory, was chosen as a theoretical framework to underpin this study. The selection of a theory was based on the objectives, which are to understand the challenges of SIMS, including the data breaches and manipulations of processes, and examine how digital forensics can be employed for detecting and mitigating data breaches in the SIMS in South African higher institutions. This requires the enactment of rules, using various tools, within the context (community) by various people. Through the activity model as shown in Figure 1, AT is most appropriate in underpinning the study.

In this study, the AT model was used as follows: (i) tools – to identify the various instruments (technologies and processes) used in accessing SIMS including those involved in the data breaches; (ii) subject – identify the various actors and their roles in the implementation, use, and management of SIMS in the institution; (iii) rules - gain a better understanding of how SIMS is controlled through enforcement of rules by the ICTS department and how users comply with the rules; (iv) understand the various group of users (such as IT specialists, students, and academic employees) including their intentionality in accessing SIMS; (v) division of labour – gain insights on the deliverables of individuals and groups, in using or accessing SIMS; (iv) object – comprehend the expected outcome from individual and the university perspectives.

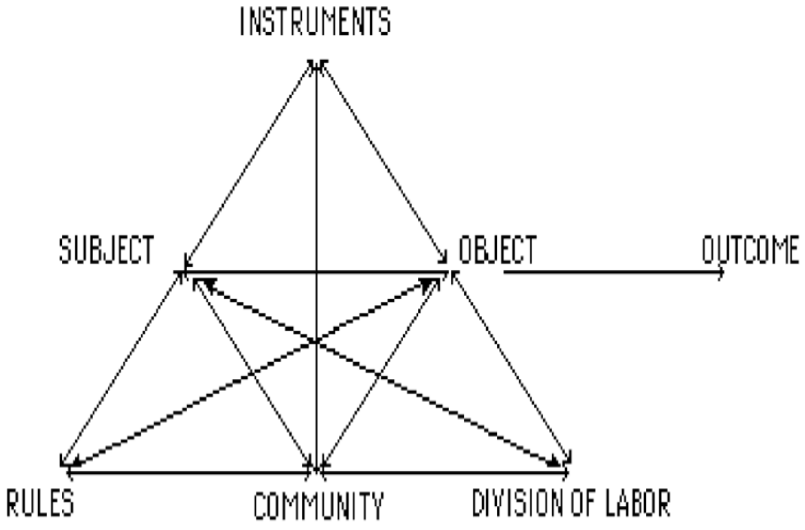

Figure 1. Activity Theory Model (Engeström et al., 2016)

The popularity of AT is attributed to its emphasis on the social activities of individuals (McMichael, 1999; Iyamu, 2021). Primarily, AT is used in qualitative studies (Karanasios et al, 2015) as a lens for analysis and interpretation (Iyamu, 2021). The author further argues that using AT as a lens is of paramount importance for education, evaluation, improvement, development, implementation, and management of IT solutions (Iyamu, 2021). According to Karanasios (2021), AT is a powerful intellectual approach and potentially presents an improved refinement and critical perspective of the human technology relationship.

Research Methodology

The inductive approach is primarily applied to exploring and developing theory, which can be a concept, theme, framework, or model (Jebreen, 2012). Inductive reasoning helps examine individuals or group experiences, including observations of specific patterns, to generate generic perspectives. According to Scholta et al. (2019:64), "inductive methods provide empirical evidence and are realistic solutions to organisational problems, as has been shown in practice". Therefore, the inductive approach focuses on a comprehensive understanding of unedited data to derive concepts and themes, such as frameworks. Creswell et al. (2018) suggest that researchers create a comprehensive set of themes through the inductive process by searching to and fro between the themes and the database. In the study, the integrated influencing factors were articulated. The work focuses on how to integrate digital forensics with SIMS in the South African Higher Education environment.

Qualitative methods involve more intense engagement with the empirical field (Venkatesh et al., 2013). Goldkuhl (2019) argues that one of the fundamental strengths of qualitative methods various aspects and sources accessed in the empirical field. Sihotang et al. (2023) suggest that other factors of interest emerge in the qualitative exploration process. This is important as this study seeks to gain an understanding of the challenges of SIMS that lead to data breaches and manipulations of processes in South African higher institutions. Additionally, qualitative methods by their inherent nature are inductive, and that reality is socially constructed (Rovai et al., 2014; Asenahabi, 2019).

Data Collection

The document analysis technique allows the gathering of related and relevant documents. One of the benefits is that the documents collected triggered a historical balance of the meaning associated with events and incidents. Also, the documents complement different cases that were previously studied. This enriches the data. Some of the documents that would be collected for this research include documentation relating to SIMS and digital forensics operations, strategies, and policies. This includes incident management systems, access control policy, and information security policy documents.

Table 1. Data collection

Focus	Journals	Conferences	Books	Total
Digital Forensics	11	2	1	14
SIMS	11	3	1	15
Integration	4	0	0	4
Total	26	5	2	33

Data analysis

The thematic analysis was applied in the analysis of the data from existing materials, including documentation. Qualitative researchers use thematic analysis as it is a prominent technique for analysing qualitative data (Naeem et al., 2023). One of the advantages of this research method is that it frequently leads the researcher to innovative insights and understanding through identifying and interpreting patterns

or themes in data sets. (Elliot, 2018; Naeem et al., 2023). Using the thematic techniques, activity theory (AT) was used as a lens to guide the analysis of the qualitative data. This approach is not new (Karanasios, 2015). Iyamu (2021) provides a model on how to apply AT as a lens in IS studies. AT makes provision for integrated influencing factors to comprehend and analyse individual activity, which includes the views of technical and non-technical actors (Sekgweleo et al, 2017). The analysis of the qualitative data focuses on:

i. Technical and non-technical activities, to gain an understanding of the factors that lead to challenges in the integration of digital forensics with SIMS, which cause data breaches and manipulations of processes.
ii. How rules, including the tools that can be employed, influence the integration process.
iii. The roles of actors and IT solutions in integrating digital forensics with SIMS.

Factors influencing the integration of digital forensics with SIMS

Applying AT as a lens, the analysis of the existing materials was conducted at two levels. The first level entails extracting the factors that can directly influence the integration of digital forensics with SIMS. This was done by following the subjective approach in the analysis of the existing materials presented in Table 1. Data security, relationship, governance, digitalisation, and co-existence were revealed as the factors influencing the integration of digital forensics with SIMS, as shown in Table 2. In the second level of analysis, the manifestations of the influencing factors were identified. In this study, the manifestations of the factors that influence the integration of digital forensics with SIMS are referred to as attributes. The attributes are highlighted in bold and italic in Table 2. In Table 3, the attributes of the influencing factors are presented.

Table 2. Integration Influencing Factors

Activity theory	Factor	Integrated influence
Tools	*Data security*	For data security, various tools (software and hardware) such as are used to protect digital data from **breaches**, including unauthorised access, corruption, or theft. It entails **interoperability** of data and processes, from both technical and non-technical perspectives. This includes the use of AI and machine learning. Literature suggests that integration supports **interoperability** and enables data security, to predict and prevent incidents, including breaches, before they occur (Mekala et al., 2024; Zia, Liu & Han, 2017).
Subject	*Relationship*	The relationship between humans (subject) and technology in the context of digital forensics integration lies in the interplay where IT innovative solutions enable the collection and analysis of digital evidence. Advancements in technology are constantly evolving the field, impacting tools and techniques, including **IT personnel** and **non-IT personnel**, in the integration of digital forensics and SIMS. Relationship is critical for integration purposes for two primary reasons. Firstly, it influences the users in their various activities. Secondly, it allows social networks and nodes to be modelled (Albtosh, 2025; Wang et al., 2024).
Rules	*Governance*	Governance in digital forensics (DF) guides roles and responsibilities, including ethics in integrating digital forensics with SIMS. The governance helps and focuses on setting **standards** and formulating **policies** (rules) in managing the chain of responsibility, authority, and communication channels related to digital evidence within SIMS. Through standards and principles, governance eases the challenges posed by the digital forensics ecosystem due to its inherent requirements (Nath et al., 2024).

Activity theory	Factor	Integrated influence
Community	*Digitalisation*	Digitisation enables the integration of digital technologies into SIMS operations to optimise processes and **users'** (community) experiences. From an integration viewpoint, Brunetti et al. (2023) suggest that digitalisation is used by both **technical** and **non-technical users** to accomplish various goals, such as increasing operational efficiency and minimising human errors. When the solution is fragmented, some students and educators often explore alternatives using various digital tools (Bygstad et al., 2023).
Division of labour	*Data growth*	Data growth increases the complexity of processes and activities (division of labour) required in the integration of digital forensics with SIMS, which necessitates various skills, such as **software developers** and **business analysts**. The unprecedented growth of data has overwhelmed the traditional systems (Gupta & Rani, 2019), such as SIMS. The growth is exponential because of the continued activities of learners and educators.
Object	*Co-existence*	Coexistence is an approach that supports and enables the **integration** of digital forensics with SIMS and allows both technologies to evolve continuously and adapt to new technologies (objects) and challenges. This implies a dynamic relationship between the technical and non-technical from a digital landscape standpoint. Through **information processing**, co-existence reduces fragmentation and enables a construct of a model, which can guide integration, including algorithms (Odat & Yaseen, 2023; Azhan et al., 2022).

The attributes manifest from the influencing factors shown in Table 2. Thus, the attributes determine the properties of the factors, which help to gain a deeper understanding of the integration and addressing challenges during the integration of digital forensics and SIMS. The attributes of the influencing factors are shown in Table 3. There are compelling arguments that attributes should be prioritised in creating new components (Chatzipetrou et al., 2020).

Table 3. Influencing factors attributes

Activity theory	Factor	Attribute	
		Technical	Non-technical
Tools	Data security	Interoperability	Breaches
Subject	Relationship	IT Specialists	Non-IT personnel
Rules	Governance	Standards	Policies
Community	Digitalisation	Technology Users	Non-technology Users
Division of labour	Data growth	Developers	Business analyst
Object	Co-existence	Integration	Information Processing

Each attribute requires a template, which defines the requirements for implementation from both technical and non-technical viewpoints. The templates cover technical and non-technical aspects of the integration. The templates provide a standard for the selection and implementation of technologies for the integration of digital forensics with SIMS, from a technical angle. From the non-technical front, the templates focus on streamlining processes and improving consistency. Thus, the templates enable tracing of each entity's

properties, ensure consistency, uniformity, and reduce disjoint in the integration process. Table 4 describess in the impliations of the study.

Table 4. Implications of the study

Factor	IT Specialist	Non-IT personnel
Integrated governance policies	How does encompassing data security affect IT people? IT staff are responsible for the formulation of policies and procedures, ensuring systems are safeguarded from internal and external sources. IT staff have administrative access to the IT infrastructure in comparison to non-IT employees (Fatoki et al., 2024). IT staff are responsible for security awareness as they are the custodians of data and need to train staff to utilise systems without compromising the integrity of the systems.	Encompassing data security affects non-IT people by familiarising themselves with the policies of the institution and ensuring they remain compliant by adhering to these respective policies. . Participation in awareness training to build capacity and being aware of governance policies at the institution, and being aware of the implications of non-compliance.
Human-centric design for digital forensics tools	How do we ensure that the integration of digital forensics with SIMS minimises human error, improves compliance, and facilitate more proactive data breach detection and response? Through the enablement of more robust systems integration where IT staff are fully knowledgeable about safeguarding of systems and the being capacitated of identifying any potential threat to reduce data breaches.	How do we ensure that the integration of digital forensics with SIMS minimises human error, improves compliance, and facilitate more proactive data breach detection and response? Improve oversight and monitoring of the systems where access is strictly validated continuously, and verify that the integration has the desired effect to reduce errors through training and awareness initiatives.

Conclusion

The study seeks to help gain a better understanding of the factors influencing the integration of digital forensics with SIMS. Using the activity theory, the study not only reveals the influencing factors but it also highlights the manifestation of the factors. The particular significance of this research lies in its contributions. The contribution lies in gaining an understanding of the challenges of SIMS that lead to data breaches and manipulations of processes in the systems. Currently, it is difficult to find case studies on how digital forensics has been integrated with SIMS despite the escalating volume of data breaches, and this research intends to close that gap. Despite the fulfilment of the study, there exist limitations. One of the main limitations is its non-empiricism. Thus, future studies that are based on natural settings using approaches such as the case study.

References

Albtosh, L. (2025). Digital Forensic Data Mining and Pattern Recognition. In *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices,* 245-294. IGI Global Scientific Publishing.

Alghamdi, M.I. (2021). Digital forensics in cyber security—recent trends, threats, and opportunities. *Cybersecurity threats with new perspectives*, 13.

Amoresano, K. & Yankson, B. (2023). Human error - A critical contributing factor to the rise in data breaches: a case study of higher education, *Holistica Journal of Business and Public Administration*, 14(1), 110-132.

Asenahabi, B.M. (2019). Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researchers*, 6(5), 76-89.

Astaman, F.P. & Mauritsius, T.U.G.A. (2023). An analysis of student perceptions of blockchain technology and its implication for education. *Journal of Theoretical and Applied Information Technology*, *101*(14), 5805-5820.

Atabek, O. (2020). Experienced educators' suggestions for solutions to the challenges to technology integration. *Education and Information Technologies*, 25(6), 5669-5685.

Azhan, N. A. N., Ikuesan, R. A., Razak, S. A., & Kebande, V. R. (2022). Error Level Analysis Technique for Identifying JPEG Block Unique Signature for Digital Forensic Analysis. *Electronics,* 11(9), 1468.

Blancaflor, E., Saunar, B.Y.P., Bilbao, T.D.C., Villarias, I.H.B. & Mapue, I.P.V. (2023). The Use of Cloud Computing and its Security Risks in a Philippine Education System: A Literature Review. In *2023 11th International Conference on Information and Education Technology (ICIET)*. 18-20 March, Fujisawa, Japan. 66-70. IEEE.

Brunetti, F., Bonfanti, A., Chiarini, A., & Vannucci, V. (2023). Digitalization and academic research: knowing of and using digital services and software to develop scientific papers. *The TQM Journal*, *35*(5), 1135-1155.

Bygstad, B., Øvrelid, E., Ludvigsen, S., & Dæhlen, M. (2022). From dual digitalization to digital learning space: Exploring the digital transformation of higher education. *Computers & Education*, *182*, 104463.

Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M. & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 25464-25493.

Chatzipetrou, P., Papatheocharous, E., Wnuk, K., Borg, M., Alégroth, E., & Gorschek, T. (2020). Component attributes and their importance in decisions and component selection. *Software quality journal*, 28(4), 567-593.

Cook, M., Marnerides, A., Johnson, C. & Pezaros, D. (2023). A survey on industrial control system digital forensics: challenges, advances and future directions. *IEEE Communications Surveys & Tutorials*, 25(3), 1705-1747.

Creswell, J.W. & Poth, C.N. (2018). *Qualitative Inquiry and Research Design Choosing among Five Approaches.* 4th Edition, SAGE Publications, Inc., Thousand Oaks.

Daim, T., Gungor, D.O., Basoglu, N., Yarga, A. & VanDerSchaaf, H. (2024). Exploring student information management system adoption post pandemic: Case of Turkish higher education. *Technology in Society*, *77*, 102557.

Daraghmi, E.Y., Daraghmi, Y.A. & Yuan, S.M. (2019). MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access*, 7, 164595-164613.

Dunsin, D., Ghanem, M.C., Ouazzane, K. & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response, *Forensic Science International: Digital Investigation*, 48, 301675.

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. Qualitative Report, 23(11), 2850–2861.

Engeström, Y., Lompscher, J. & Rückriem, G. (eds.). (2016). *Putting activity theory to work: Contributions from developmental work research*. 13th ed. Berlin: Lehmanns Media.

Farjon, D., Smits, A. & Voogt, J. (2019). Technology integration of pre-service teachers explained by attitudes and beliefs, competency, access, and experience. *Computers & Education*, 130, 81-93.

Flores, R., Namin, A.S., Tavakoli, N., Siami-Namini, S. & Jones, K.S. (2021). Using experiential learning to teach and learn digital forensics: Educator and student perspectives. *Computers and Education Open*, 2(3), 100045.

Goldkuhl, G. (2019). The generation of qualitative data in information systems research: the diversity of empirical research methods. *Communications of the Association for Information Systems*, *44,* 572-599.

Gürkut, C., Elçi, A. & Nat, M. (2023). An enriched decision-making satisfaction model for student information management systems. *International Journal of Information Management Data Insights*, 3(2), 1-13.

Gupta, D., & Rani, R. (2019). A study of big data evolution and research challenges. *Journal of Information Science*, *45*(3), 322-340.

Gyawali, Y.P. & Mehndroo, M. (2024). Navigating the digital frontier: Exploring opportunities and challenges in the integration of technology in higher education, *International Journal of Education and Development using Information and Communication Technology,* 20(1), 119-133.

Hamad, W.B. (2023). Evaluating the students' behaviour intention toward the use of the Student Information Management System (SIMS): a case of the Institute of Social Work. *Education and Information Technologies*, *28*(6), 7005-7029.

He, W., Zhang, Z.J., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International journal of information management*, 57, 1-8.

Hina, S. & Dominic P.D.D. (2018). Information security policies compliance: a perspective for higher education institutions, *Journal of Computer Information Systems*, 60(3), 201–211.

Iyamu, T. (2018). Collecting qualitative data for information systems studies: The reality in practice. *Education and Information Technologies*, 23, 2249-2264.

Iyamu, T. (2021). *Applying Theories for Information Systems Research*. Abingdon, Oxon; Routledge.

Jebreen, I. (2012). Using inductive approach as research strategy in requirements engineering. *International Journal of Computer and Information Technology*, 1(2), 162-173.

Johnson, C., Davies, R. & Reddy, M. (2022). Using digital forensics in higher education to detect academic misconduct, *International Journal for Educational Integrity,* 18(1), 1-19.

Karanasios, S., Allen, D. & Finnegan, P. (2015). Information systems journal special issue on: Activity theory in information systems research. *Information Systems Journal*, 25(3), 309-313.

Karanasios, S., Nardi, B., Spinuzzi, C. & Malaurent, J. (2021). Moving forward with activity theory in a digital world. *Mind, Culture, and Activity*, 28(3), 234-253.

Kebande, V. & Venter, H.S., (2015). A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis. In *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015:* 2-3 July, University of Hertfordshire, Hatfield, United Kingdom (UK), *ECCWS 2015,* 373-382.

Khalaf, R.S. & Varol, A. (2019). "Digital Forensics: Focusing on Image Forensics". *7th International Symposium on Digital Forensics and Security (ISDFS)*, 10-12 June, Barcelos, Portugal, 1-5.

Kifaru, F.R., Kavuta, K.D. & Semlambo, A.A. (2023). Assessment of the impacts of cyber security on student information management systems: a case of Ruaha Catholic University. *The Journal of Informatics*, 3(1), 51-67.

Kigwana, I & Venter, H.S. (2018). A digital forensic readiness architecture for online examinations, *South African Computer Journal*, 30(1), 1-39.

Kock, A., Schulz, B., Kopmann, J. & Gemünden, H. G. (2020). Project portfolio management information systems' positive influence on performance–the importance of process maturity. *International Journal of Project Management*, 38(4), 229–241.

Kundy, E.D. & Lyimo, B.J. (2019). 'Cyber security threats in higher learning Institutions in Tanzania', A case of the University of Arusha and Tumaini University Makumira. Olva Academy –School of Researchers, 2(3).

Li, J., Xiao, W. & Zhang, C. (2023). Data security in universities: identification of key factors affecting data breach incidents, *Humanities & Social Sciences Communications*, 10(1), 270-289.

Li, M. & Tuunanen, T. (2022). Information Technology–Supported value Co-Creation and Co-Destruction via social interaction and resource integration in service systems. *The journal of strategic information systems*, *31*(2), 101719.

Liu, Z., Wang, H. & Zan, H. (2010). Design and implementation of student information management system, in: Proceedings - International Symposium on Intelligence Information Processing and Trusted Computing, IPTC 2010, 607–610.

Magara, E. (2006). *A framework for an integrated student information management system for higher education in Uganda,* 68(05).

Mazadu, U.H., Ibrahim, M.M., Ibrahim, A.S. & Mansur, M.S. (2022). Examining the instructor management benefits of student information system: An empirical investigation. *Social Sciences & Humanities Open*, 6(1), 1-8.

McMichael, H. (1999). An activity based perspective for information systems research. In the *10th Australian Conference on Information Systems,* Melbourne, Australia.

Mekala, S. H., Baig, Z., Anwar, A., & Syed, N. (2024, April). Evaluation and Analysis of a Digital Forensic Readiness Framework for the IIoT. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS),* 29-30 April, San Antonio, TX, USA, 1-6. IEEE.

Moallem, A. (2019). Cyber security awareness among college students. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity,* 21-25 July*,* Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9. 79-87. Springer International Publishing.

Mtambeka, P., Mtegha, C.Q., Chigona, W. & Tuyeni, T.T. (2023). Factors affecting how university students comply with cybersecurity measures: A case of South Africa. *Proceedings of NEMISA Digital Skills Conference*. 15-17 February, Durban, South Africa, 5, 1-16.

Mthembu, T. (2022). What are the Benefits of the Student Management Systems, 25 May, Available at, https://education.adaptit.tech/blog/what-are-the-benefits-of-the-student-management-system/ (Date accessed 25 May 2024)

Mueller, B. & Urbach, N. (2013). The why, what, and how of theories in IS research. *Thirty Fourth International Conference on Information Systems*, 18 December, Milan, Italy.

Naeem, M., Ozuem, W., Howell, K. & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods*, 22, 1-18.

Nath, S., Summers, K., Baek, J., & Ahn, G. J. (2024). Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. In *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA),* 28-31 October, Washington, DC, USA, 11-20. IEEE.

Odat, E., & Yaseen, Q. M. (2023). A novel machine learning approach for Android malware detection based on the co-existence of features. *IEEE Access*, *11*, 15471-15484.

Rovai, A. P., Baker, J. D., & Ponton, M. K. (2014). Social Science Research Design and Statistics. Chesapeake, VA: Watertree Press LLC.

Scholta, H., Niemann, M., Delfmann, P., Räckers, M. & Becker, J. (2019). Semi-automatic inductive construction of reference process models that represent best practices in public administrations: A method. *Information Systems*, 84, 63-87.

Sekgweleo, T., Makovhololo, P. & Iyamu, T. (2017). The connectedness in selecting socio-technical theory to underpin information systems studies. *Journal of Contemporary Management,* 14(1), 1097–1117.

Semeon, G., Negash, S. & Musa, P. (2010). The Success of Student Information Management System: The Case of Higher Education Institution in Ethiopia. *Proceedings of the Sixteenth Americas Conference on Information Systems,* 12-15 August, Lima, Peru.

Serketzis, N. Katos, V. Ilioudis, C. & Pangalos G.J. (2018). Actionable threat intelligence for digital forensics readiness, *Information & Computer Security*, 27(2), 273-291.

Sihotang, D. M., Purwandari, B., Eitiveni, I., Putri, M. F. & Hidayanto, A. N. (2023). Factors influencing village information systems adoption in Indonesia: A qualitative study. *The Electronic Journal of Information Systems in Developing Countries*, 89(5), e12271.

Suwardi, I.S. (2007). New Integration Model of Information System on Higher Education Institution, *Proceedings of the International Conference on Electrical Engineering and Informatics Institut Teknologi*, 17- 19 June, Bandung, Indonesia.

Taha, N. & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, 26(2), 1721–1736.

Thakar, A.A., Kumar, K. & Patel, B. (2021). Next Generation Digital Forensic Investigation Model (NGDFIM) – Enhanced, Time Reducing and Comprehensive Framework, *Journal of Physics: Conference Series,* 1767(1), 012054.

Tsang, E.W. & Ellsaesser, F. (2011). How contrastive explanation facilitates theory building. *Academy of Management Review*, 36(2), 404–419.

Ulven, J.B. & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet,* 13(2), 1-39.

Valjarevic, A. & Venter, H.S. (2015). A Comprehensive and Harmonised Digital Forensic Investigation Process Model, *Journal of Forensic Science*, 60(6), 1467-1483.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *Management Information Systems (MIS) quarterly*, 37(1), 21-54.

Verizon (2022). 2022 Verizon data breach investigations report. Verizon, New York.

Wang, H., Yang, W., Man, D., Lv, J., Han, S., Tan, J., & Liu, T. (2024). Anchor Link Prediction for Cross-Network Digital Forensics from Local and Global Perspectives. *IEEE Transactions on Information Forensics and Security*, 19, 3620-3635.

Zia, T., Liu, P., & Han, W. (2017). Application-specific digital forensics investigative model in Internet of Things (IOT). In *Proceedings of the 12th International Conference on Availability, Reliability and Security,* 29 August - 1 September, Reggio Calabria, Italy, 55, 1-7.