An AI Model for Digital Forensic Readiness in the Cloud Using Secure Access Service Edge

Taurai Hungwe[1] and Hein Venter[2]
[1]Department of Computer Science and Information Technology, Sefako Makgatho Health Sciences University, South Africa
[2]Department of Computer Science, University of Pretoria, South Africa

taurai.hungwe@smu.ac.za
hventer@cs.up.ac.za

Abstract: Computing infrastructure has evolved and has brought about changes to the ways that work and business are carried out. Cloud computing has redefined these workspaces by providing connectivity and tools to enable productivity, collaboration, and flexibility. As work moves outside the centralised office and goes remote, users are accessing the cloud directly, leaving the protection of the corporate network and leaving the users' computing platforms open to threats. In the pre-cloud era, the data centre for organisations was the single location where digital assets would be housed and non-complicated security parameters implemented. The firewall would be the main security perimeter implemented to secure the network in this pre-cloud era. The advent of cloud computing has brought potential areas and gaps in securing the organisational data, information and communication connectivity to the cloud-based resources. As such, there is need to rethink and redesign the models which can be implemented to secure the cloud computing services. The cloud should be in a state of digital forensics readiness in order to facilitate digital forensics investigation. The study focuses on the development of an artificial intelligence model for digital forensic readiness for the cloud using secure access service edge. This integrated approach might assist in the provisioning of cloud security.

Keywords: Digital forensics readiness, Cloud computing, Artificial intelligence, Secure access service edge, Security

1. Introduction

The current working environments have been redefined as organisations embrace the use of cloud computing. The use of cloud computing services results in an increase in remote users and computers. Cloud computing provides connectivity and tools to enable productivity, collaboration, and flexibility (Cisco, 2022). The recent Covid-19 pandemic has also accelerated the adoption of the cloud (Islam et al., 2021). Employees, users and computers connect remotely to the cloud and leave the secure corporate network environments as work is conducted outside the centralized office. This increased the acceptance of the cloud, however, it exposes the organisations and users to security threats and attacks. A need has arisen for a rethink and redesign of security models to be implemented to secure data, information, networks and computers accessing the cloud.

In the day-to-day provisioning of cloud services, security breaches might occur. For example, unauthorised data access by cybercriminals to sensitive personal information and data may occur such as unauthorised access to people's financial records stored on the cloud. When such security infringements occur, an investigation is required to investigate the security transgressions. Digital forensics investigation (DFI) is a process of recovering and investigating digital evidence. The gathered evidence might be used to present arguments in a court of law or used to reconstruct events on a computing system.

In order to facilitate the DFI process, specifically in the cloud, certain controls and processes should be in place prior to the occurrence of a security breach. The cloud should have been made ready for digital evidence collection in some way. Thus, in order to do this, the cloud components must apply digital forensic readiness. Tan (2001) explained digital forensic readiness (DFR) as positioning organisations to have proactive digital forensic (DF) techniques in place. This optimises the collections of evidence to meet legally reliable standards and reduces the overall effective costs associated with DFI processes. Cloud services bring in aspects of volatility. For example, some cloud service providers do not provide persistent storage to virtual machine instances (Purnaye & Jyotinagar, 2015). At any given time or moment, a cloud service might be available and the same service might not be available to the users or organisation in – often soon – subsequent time. Security breaches could have occurred, at the time the cloud service was available to the user and that same service might not be available when a DFI processes would need to be conducted. This volatility on cloud services provisioning poses challenges in carrying out DFI processes as some or all of the data might be lost by the time of investigation. Again, for a successful DF process to be conducted, the cloud components and services must be digital forensically ready. Currently, cloud computing services which are made available or accessed by users through computing edge (referring to a range of networks and devices at or near the user) are not digital forensically ready and not much research has been conducted in this area (MacDonald et al., 2019; van der Walt & Venter,

2022). This paper focuses on security challenges of the cloud and comes up with a model using AI for digital forensics readiness. The objectives are, (1) Identify the security challenges of cloud computing edge components and evaluate if the components and services are digital forensically ready (DFRy); and (2) Design an artificial intelligence (AI) framework for digital forensic readiness for the core components for secure access service edge (SASE). For this, AI unsupervised algorithms should be applied to detect security threats and attacks on the cloud offerings. Secondary data is used for the unsupervised algorithm for learning, testing and then finally for predictions on cloud computing edge core components for DFR.

Piecemeal security offerings might provide security to different cloud services. Such siloed approach might be cumbersome and not being the best way to provide cloud security. Available frameworks on securing cloud components are relatively new and little research has been conducted (MacDonald et al., 2019; van der Walt & Venter, 2022). In year 2022 there were only three (3) relevant articles collectively dealing with the concepts of security, DF and DFR in relation to cloud computing (Van der Walt & Venter, 2022). One of the research gaps identified by Van der Walt and Venter points to the non DFR on cloud computing core components. A model is proposed to achieve DFR in the cloud. Moreso, without an AI model on DFR for cloud computing, it remains costly and time consuming to find out what would have been the security transgressions when a DFI process is conducted. It will assist in making cloud computing components DFRy and align the model to existing models and standards.

The rest of this paper is structured as follows: Section 2 presents the background of the study. Section 3 is a contribution to the study which proposes the first version of the model. Section 4 critically evaluates the proposed model, and then section 5 concludes the paper and outlines future research work.

2. Background

This section discusses relevant concepts related to the research. These concepts are, defining cloud computing, benefits of cloud computing, cloud computing challenges, cloud services and deployment models, edge components and cloud security issues.

Cloud computing (CC) is the on-demand access of computing services over the Internet (Baror et al., 2021; IBM, 2023; NIST, 2015). The computing services include, infrastructure, platform and software provisioned through cloud service providers (CSPs). For example, software applications (MS 365) as a service over the internet with the software hosted by a CSP as opposed to owning and licensing of the software on the organisational (user) premises. Such services can rapidly be provided, scaled up or scaled down depending on demand and usage with very little effort and user interaction (Armbrust, et al., 2010; Armbrust et al., 2009; Maun, 2018). One of the main advantages of CC is that the user pays for the usage (pay-as-go) of the software service, but not for the actual software itself with the user particularly owning the software. However, CCS are dependent on the availability of the internet, without internet connectivity services cannot be accessed.

Accessing of the cloud is through the use of edge components also referred to as endpoint or end things. For example, end points include, routers, gaming controllers, vehicles, cameras, laptops, personal computers (PCs), internet of things (IoT) and mobile devices Thus, the edge component are virtual or physical devices fixed at the end (edge) of the network (Yang, et al., 2020). With many devices connecting to the cloud, concerns on security in the cloud arise.

Cloud security involves the securing of cloud computing systems (Kaspersky, 2022). Cloud security is made up of three categories, namely, data security, identity and access management (IAM) and governance. Data security involves the protection of data (such as data stored in a database) against destruction, unauthorised access and data breaches among others. IAM involves granting of correct rights to authorised users to computing resources. Governance provides the requisite policies, processes and procedures to control, direct and manage security risks, threats, and attacks for an organisation. Security in cloud computing caters for the network, data, data storage, virtualisation frameworks, operating systems (OS), middleware, runtime environments, applications and end-user hardware.

This includes keeping data private and safe across online-based infrastructure, applications, and platforms Cloud security is shared between the cloud user and the CSP. The CSP is responsible for the security of the cloud. Security of the cloud entails safety and awareness of the cloud users in the process of using CCS. The security of the cloud includes hardware, software, networking, and facilities that run the cloud services. The user is responsible for the security in the cloud. This implies that, the user manages security aspects on data, classifying assets, access, and cloud configurations. For example, consider the management of and use of user passwords. Security in the cloud deals with the securing of the cloud in the running of applications, storing data and processing transactions. In other

words, it deals with the safety of the cloud itself. Security in the cloud encompasses ways and technology (tools and machinery) that protects cloud computing environments against cybersecurity threats.

The main advantages or benefits to businesses of CC are the increase of efficiency, productivity, flexibility and scalability. CCS is scalable and flexible since it enables any organisation to set up and manage information technology (IT) infrastructure on a pay-as-you-use basis, enabling cost effective data redundancy, off-site backups, big data storages and IT sourcing (Sarga, 2012). However, despite the many advantages of CC, the cloud also provides an environment for cybercriminals to conduct illegal activities, for example, distributing malware, conducting scams, identity theft and other criminal activities (Pasquale, et al., 2016; Pichan et al., 2015). Criminal activities leave digital footprints behind which can be collected and analysed through DFI process. DFI is presented in the next section.

Digital forensics is part of forensic science which assists in the recovery, preservation, analysis and presentation of digital evidence. Digital evidence can be used in legal evidence processes and assists to posit motive behind an incident with intention to identify the offender.

Several definitions on digital forensics exist in literature (Agarwal et al, 2011; Cohen et al., 2011; Ray, 2009; Vacca, 2005; Gary, 2001). Digital forensics investigation (DFI) is a process of securing, collection, preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purposes of deriving scientific evidence of criminal activities is conducted (Gary, 2001). The following definition captures the core of concept and processes involved in digital forensics. Digital forensics is "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Gary, 2001). An undisputed digital forensic process must be conducted which stands any scrutiny against the law and evidence presentations. Harmonised Digital Forensic Investigation Process (HDFIP) follows applicable standards to conduct DFI process (ISO/IEC 27043, 2015) and will be used in this study. Without having the CC edge components DFR, it is difficult to conduct a DFI.

Digital forensics readiness (DFR) is "the state of the organisation where controls are in place, in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorised actions shown to be disruptive to planned operations" (Pangalos & Katos, 2010). DFR is a proactive way of making sure that there is an ability to carry out a credible DFI when an incident occurs. To achieve DFR, Rowlingson (2004) suggested ten activities to be done before an incident occurs. These ten activities are as follows:

1. Define the business scenarios that require the collection of digital evidence.
2. Identify available sources and different types of potential evidence.
3. Determine the evidence collection requirement(s).
4. Establish a capability for securely gathering legally-admissible evidence to meet the requirement(s).
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full, formal investigation should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Obtain legal review on the incident. This ensures that the evidence collection process is forensically and legally correct and the collected evidence is sufficient in order to link the offenders with the committed crime for prosecution purposes.

The implementation of such activities prepares organisations for carrying out DFIs with minimum costs and less disruption of business continuity in a proactive manner for the cloud. Given the nature of cloud computing being volatile (at any given time a cloud computing service would be available to the cloud user and shortly thereafter might not be available), time is of essence for conducting a successful DFI. Thus, this can be achieved by having the cloud being DFRy. Considering Rowlingson's ten activities to achieve DFR mentioned earlier on, such activities could be automated through artificial intelligence (AI). Definition, use and role of AI in DFR follows.

AI involves process automations of learning, self-correction and reasoning in order to do human activities through the use of computing machines and technologies. For example, AI can be used to conduct and anlyse financial credit ratings of an individual based on the financial behaviour of the individual. AI is, therefore, the process of mimicking human intelligence in machines (Dunsin et al., 2022; Agarwal & Karahanna, 2000). AI replicates or simulate human intellect, such as learning and reasoning with accelerated speed, with intensified

power, and with increased complexity. This study will not dwell much on the history of AI except for a few notable developments in AI. This is presented in the next paragraph.

AI dates back to science, philosophy and history. The development of AI is owed to Alan Turing in 1950. Coining of the term was done by John McCarthy in 1956 at a conference in Dartmouth College (Collins et al., 2021). John McCarthy defined AI as "the science and engineering of making intelligent machines" (McCorduck, 2004). It was during this time that the birth of AI was realised, termed and defined. In defining AI, it is worthy to split the terms to artificial and intelligent, define the two terms, form an understanding of the artificial and intelligence terms and render a combined definition for AI. Trocin et el. (2021) considers intelligence as a way of sense making using of information amassed from previous encounters and dealing with improbabilities of future or new activities. The term artificial is the imitation of human-like cognitive tasks with clear ways of doing things (Benbya et al., 2021). Merging the definitions of the two terms, the following definition emerges which is adopted in this research. AI is defined as a way in which machines use computational power to collect, discover, infer and learn from data to accomplish programmed activities to impersonate humans (Mikalef & Gupta, 2021). Having defined AI, the next aspects is to consider the use and role of AI.

The role of AI is to provide computing machines that can decipher data and perform human-like activities. The human-like activities are performed due to various reasons, for example, a machine can be used to perform an activity that – being performed by a human – could expose the human to hazardous environmental factors. In some instances, AI is used to automate repetitive activities which are easily programmable on a machine, but physically too exhausting for a human. Process, product and service improvements are enabled through the use of AI. Furthermore, AI enables improvement and refinement of algorithms, thereby increasing the accuracy of results when these algorithms are implemented. AI also have self-correcting mechanisms to improve processes and activities. In this study, the role of AI is directed towards digital forensics readiness (DFR) within the cloud, as described in the next section.

DFR, as earlier defined, is the ability to respond proactively and collect digital evidence related to a security incident with minimal cost or interruption to services (Yasinsac & Manzano, 2001; Dunsin et al., 2022). DFR processes might be improved through automation using AI, as the DFR processes are currently conducted manually. For example, AI can be used to predict the occurrence of security incidents in order to provide anticipated responses to reduce security attacks. AI has the potential to engage in multi-step reasoning, to understand the meaning of natural language, to design innovative artefacts, to generate novel plans that achieve certain goals, and even reason about its own reasoning (Langley, 2019). It is through these possibilities that AI can be exploited to untangle security incident reports in order to prepare computing infrastructure to become DFRy.

To assist in the automation of digital forensics investigations, Rughani (2021) came up with an AI-based digital forensics framework which automates major routine operations in digital forensic investigations using intelligence acquired from artificially-trained data. This is an example of process automation and optimisation to specifically increase the efficiency in a specific application area of AI. The future of AI can also be linked with this research focusing on an AI framework for digital forensic readiness for secure access service edge components. This might transform the manner in which digital forensics readiness (DFR) would be applied on the edge components in cloud computing.

3. AI Model for Digital Forensic Readiness in the Cloud using Secure Access Service Edge

Users access the cloud by means of edge components; see Figure 1. Examples of edge components include, among others, mobile devices such as mobile phones, gaming controllers, water sensors, vehicles, cameras and PCs. An AI model is implemented for DFR to enhance cloud security using secure access service edge (SASE).

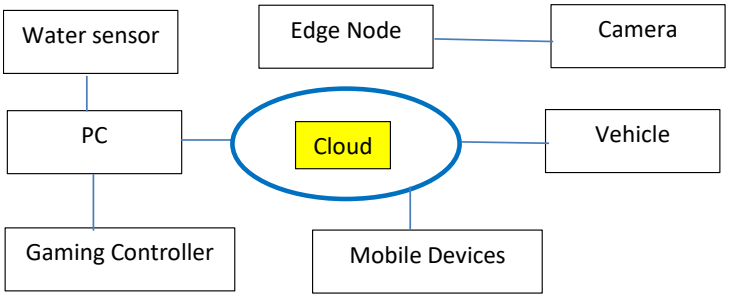

Figure 1: Relationship of the cloud and edge components

Figure 2 illustrates the proposed AI model. The deployment of SASE is implemented in the edge components and the cloud. This is the new contribution to making cloud computing edge components to be digital forensically ready. The model proactively implements SASE and monitors the components and gathers potential digital forensic evidence (PDFE). At the edge side, the security breaches are detected, and remedial actions are conducted. Similarly, on the cloud side, the SASE is deployed.

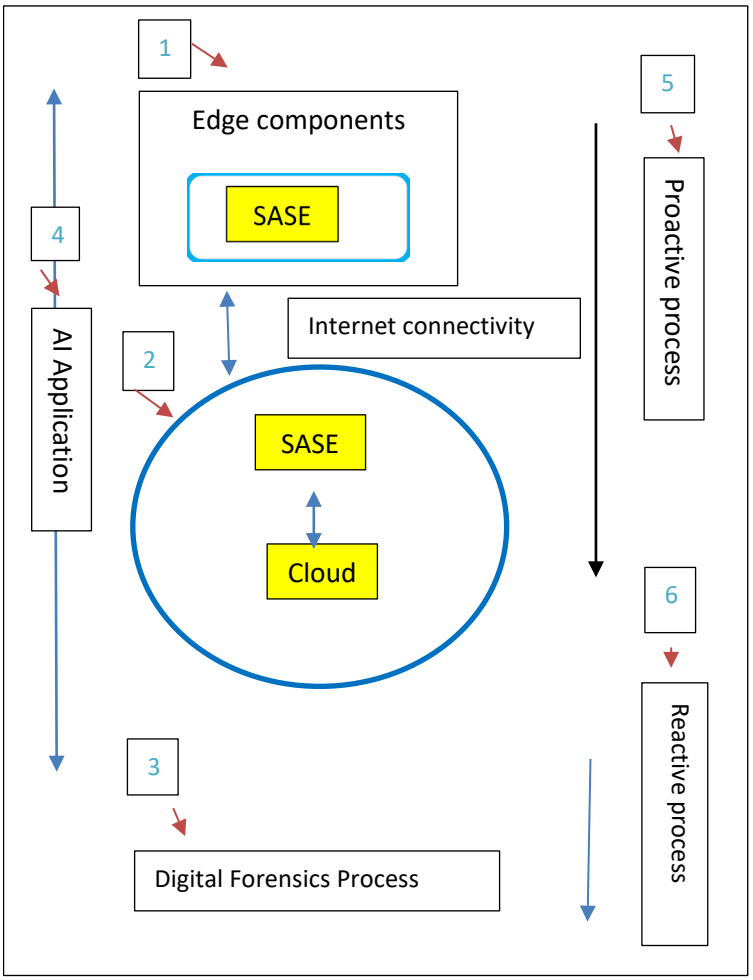

Figure 2: Proposed AI DFRy models

Incoming network traffic from the edge to cloud components and outgoing traffic from the cloud to the edge components is monitored for security breaches. The aspects of detecting the security breaches in the edge components and the cloud could be automated using AI. The AI automated processes feed into the parallel proactive processes of DFRy. The proactive processes approach is based on preparing for DFR based on Rowlingson's (2004) ten activities which should be done before an incident occurs, active monitoring, gathering and retaining digital information within the cloud environment and the edge components. The DFI process is a reactive process, meaning it is conducted after a security incident has occurred. It is then after a security breach has happened that a DFI process is initiated as contrasted to proactive DFR process. The main role of the model is to have the edge components and the cloud to be DFRy. This assists when a need arises to conduct DFI processes. The detailed proposed AI DFRy model is illustrated in the next paragraph.

Annotation "1", in Figure 2, shows how the edge components such as mobile devices access the cloud services. SASE is implemented at the edge components. Mobile devices have the potential to be attacked by malware and introduce the malware to the network, to other connected devices and to the cloud. Thus, the edge components are the entry point of malicious activities which compromise the other components and the rest of the cloud environment. The other entry points would be the network and the cloud. Monitoring of these entry points is implemented and PDFE is also gathered at these edges of the cloud. PDFE is stored in the cloud infrastructure such as storage and servers. Storage and servers will preserve the PDFE to be used for DFR purposes. On the cloud, at annotation "2", SASE is also implemented. Similarly, PDFE is gathered, stored and preserved in the

cloud infrastructure. DFI processes, at annotation "3", are conducted using the information proactively collected, stored and preserved in instances of security breaches.

The AI application, denoted by annotation "4" illustrates the implementation of unsupervised machine learning unsupervised learning algorithms. The algorithms will detect the security threats and incidences. For example, if there is an upsurge of unexplained traffic on the network connecting the edge components and the cloud, it might signify a security incidence. The AI application will also automate the activities proposed by Rowlingson as ways to prepare the cloud and the edge components to be DFRy. The proactive process, at annotation "5", indicates the manner in which the edge components and the cloud are prepared for the next process, i.e. the reactive process at annotation "6" of carrying out a DFI. Annotation "6" is instituted after a security incidence would have been detected, hence it is referred to as a reactive process. The proactive process is implemented in anticipation of a security incidence. Thus, making sure that cloud environments and the edge components are able to collect PDFE, stored in appropriate storage spaces and preserved. To illustrate the DFR process, a run through Rowlingson's activities follows.

Assume that in a business setting, for example, a mobile device such as a mobile phone connects to the cloud through a public cloud service provider. This provides the first activity of defining the business scenario that necessitates the collection of digital evidence. The identification of available sources and different types of PDFE then follows, which is the second activity under Rowlingson's activities. In the process of identifying the phone and possibly the owner, certain PDFE can be identified such as the phone's international mobile equipment identity (IMEI), mobile station international subscriber directory number (MSISDN), subscriber identity module (SIM), international mobile subscriber identity (IMSI) number. More PDFE can be identified but is omitted here due to space constraints. Activity three, determination of the evidence collection requirement(s), is then conducted. This would involve activities such as commissioning of the investigation by the responsible person and identifying the scope of the investigation. Thereafter, the data and information must be stored and preserved. Thus, activity four, establishes a capability for securely gathering legally-admissible evidence to meet the requirement(s) of the mobile phone data. The mobile phone data collected in this scenario will have to be securely stored and handled according to established policies. Activity six then ensures that monitoring is targeted to detect and deter major incidents in the use of the mobile phone. If unwarranted mobile phone usage is detected, then the next activity, activity seven, has to commence. In activity seven, circumstances are specified when such unwarranted mobile phone usage is escalated to a full, formal investigation would be launched. The training of staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivity of evidence, commences in activity eight. Staff are sensitized on matters such as privacy and observing legislative instruments, for example, in South Africa such matters are protected by the protection of personal information act (POPI Act) of 2013 (Government gazette, 2013). In activity nine, documentation of the evidence-based case describing the incident and its impact is put in place. The last activity (activity ten) is obtaining legal guidance of the incident. This ensures that the evidence collection process is forensically and legally correct and the collected evidence is sufficient in order to link the offenders with the committed crime for prosecution purposes. All these activities are there to have the cloud and the connected edge components of the cloud prepared for an eventuality that PDFE can be collected in the event that a DFI has to be conducted. The next section presents the critical evaluation of the model.

4. Critically Evaluation of the Proposed Model

The proposed AI model is a novel concept that automates the activities in the cloud and its edge components by gathering digital information and preserving it forensically in preparation for DFI purposes. This is the contribution of the research which aims at forensic planning and preparation for a DFI process within this particular environment. The AI model identifies and predicts the security challenges of cloud computing edge components and applies unsupervised algorithms in the detection of security threats and attacks. The information detected on incidences prepares the cloud and the edge components to actively collect PDFE. By making the edge components and the cloud ascribe to Rowlingson's activities, the cloud and the components are able collect credible evidence before an incident occurs, thus, making them digital forensically ready (DFRy). The model enables cloud and the edge components to achieve sufficient forensic preparedness from the forensically preserved information by using SASE and implementing Rowlinson's ten readiness activities. Implementing such activities, if an incident is detected, assists the users using the cloud to gather credible forensic evidence that can stand legal tests. The model simplifies the process of evidence collection as required data and information are easily collected from the digital forensically ready environment. The next section concludes this paper.

5. Conclusion

The increase in the use of cloud computing (CC) has also increased the number of connected edge devices and remote users. With such an increase, the wider CC environment is littered with more security risks. Security incidents in the course of using the cloud require DFI processes to unearth the security breaches. Efficient DFI are premised by how digital forensically ready (DFRy) the devices are. Cloud computing edge components are not DFRy. Without having the DFR components in place, it is difficult to conduct a DFI. The research focuses on making the cloud computing components and services DFRy and proposes an AI model for DFR in the cloud using SASE. The proposed model was illustrated as it deploys integrated SASE and edge components in the cloud. AI is then applied to identify, predict and report security incidences. The reports are then used to prepare the cloud edge components for DFR. The proactive preparations for the edge components provide for an efficient and cost-reduced DFI process. This achieves the aim of the research for putting forensic preplanning processes in place for the proactive preparation of a DFI.

References

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S.C. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS),* Vol. 5 No. 1, 2011, pp. 118 – 131.

Agarwal, R., & Karahanna, E. (2000). Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Quarterly*, 24(4), p.665.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee., G, Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. A view of cloud computing. (2010). Commun ACM. 2010;53:50–58. doi:10.1145/ 1721654.1721672.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing. Department of Electrical Engineering and Computer Science. Univ. California, Berkeley, Rep. UCB/EECS; Pg1-26, 2009. Online available at http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html Last Accessed 10 February 2024.

Baror, S.O., Venter, H.S. & Adeyemi, R. (2021). A natural human language framework for digital forensic readiness in the public cloud. Available at: https://repository.up.ac.za/bitstream/handle/2263/78877/Baror_Natural_2021.pdf?sequence=1&isAllowed=y> Last accessed 12 April 2023.

Benbya, H., Pachidi, S., Jarvenpaa, S.L. (2021). Special issue editorial: artificial intelligence in organizations: implications for information systems research. *J. Assoc. Inf. Syst.* 22, 281–303.

Cisco. (2020). How cloud security reduces threat risk and paves the way to SASE. Modern solutions for protecting the new way businesses work. Available at https://umbrella.cisco.com/info/ebook-how-a-cloud-security-solution-reduces-risk-and-paves-the-way-to-sase. Accessed 19 February 2023.

Collins, C., Dennehy, D.; Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda*. International Journal of Information Management* 60 (2021) 102383. https://doi.org/10.1016/j.ijinfomgt.2021.102383.

Cohen, F., Lowrie, J., & Preston, C. (2011). *The State of the Science of Digital Evidence Examination.* In: Peterson, G. and Shenoi, S. (Eds), Advances in Digital Forensics VII. Cohen, F. (2012). Digital Forensic Evidence Examination. (4ed), California: Fred Cohen & Associates

Dunsin, D.; Ghanem, M. & Ouazzane, K. (2022). The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment. August 2022. *International Journal of Information and Communication Technology* 16(6):280-285. Available at: https://repository.londonmet.ac.uk/7708/3/Australia_Dip_paper.pdf. Accessed 24 June 2023.

Gary, P. (2001). A Road Map for Digital Forensic Research, Report from DFRWS 2001, *First Digital Forensic Research Workshop*, Utica, New York, August 7 – 8, pp. 27–30.

Government Gazette, REPUBLIC OF SOUTH AFRICA. Vol. 581 Cape Town 26 November 2013. /https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf. Accessed 11 December 2023.

IBM. (2023). IBM X-Force threat intelligence index 2023 report. Available at: www. https://www.ibm.com/reports/threat-intelligence. Accessed 12 June 2023.

Islam, M.N., Colomo-Palacios, R., & Chockalingam, S. "Secure Access Service Edge: A Multivocal Literature Review," 2021 21st International Conference on Computational Science and Its Applications (ICCSA), Cagliari, Italy, 2021, pp. 188-194, doi: 10.1109/ICCSA54496.2021.00034.

ISO/IEC 27043. (2015). *Information technology – Security techniques – Incidents investigation principles and process.* Geneva: ISO

Kaspersky. (2022). What is Cloud Security? Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security (Accessed: 27 May 2022).

Langley, P. (2019,). An integrative framework for artificial intelligence education. *In Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 33, No. 01, pp. 9670-9677).

MacDonald, N., Orans, L., & Skorupa, J. (2019). *'The Future of Network Security Is in the Cloud'.* Gartner, (August).

Maun, U. (2018). Future of Cloud Computing 2025: Trends & Predictions. [Online]. https://www.seasiainfotech.com/blog/history-and-evolution-cloud-computing/. Last Accessed 10 February 2024.

McCorduck, P. (2004*). Machines who think: A personal inquiry into the history and prospects of artificial intelligence (2nd ed.).* A. K. Peters.

Mikalef, P., & Gupta, M. (2021). Artificial Intelligence capability: conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance*. Inf. Manage.* 58, 103434 https://doi.org/10.1016/j.im.2021.103434.

NIST. (2015). *The NIST Definition of Cloud Computing.* Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. Accessed 12 April 2023.

Pangalos, G., & Katos, V. (2010). Information Assurance and Forensic Readiness. *e-Democracy*, 181-188.

Pasquale, L., Hanvey, S., McGloin, M., Nuseibeh, B., Pasquale, L., & Hanvey, S. Adaptive evidence collection in the cloud using attack scenarios. *Computer Security.* 2016;59:236–254. doi:10.1016/j.cose.2016.03.001.

Pichan, A., Lazarescu, M., Soh, S.T., Cloud forensics: technical challenges, solutions and comparative analysis. *Digit Investigation*. 2015;13:38–57. doi:10.1016/j.diin.2015.03.002.

Purnaye, P., & Jyotinagar, V. (2015). Cloud forensics: Volatile data preservation. *International Journal of Computer Science Engineering (IJCSE).* ISSN: 2319-7323 Vol. 4 No.02 March 2015, pp 41 – 43.

Ray, C. (2009). *Distributed Database Systems*. New Delhi: Pearson Education.

Rowlingson, R. (2004). "A ten step process for forensic readiness". *International Journal of Digital Evidence,* 2(3), 1-28.

Rughani, P.H. (2021). Artificial Intelligence Based Digital Forensics Framework*. International Journal of Advanced Research in Computer Science.* Volume 8, No. 8, September-October 2017. DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4571.

Sarga, L. (2012). Cloud Computing: An Overview. *Journal of systems integration* (2010). 3 (4), 3–14.

Tan, J. (2001). *Forensic readiness.* Cambridge, MA: @ Stake, 1-23.

Trocin, C.; Våge Hovland, I., Mikalef, P., & Dremel, C. How Artificial Intelligence affords digital innovation: A cross-case analysis of Scandinavian companies. *Technological Forecasting & Social Change* 173 (2021) 121081.

Vacca, J. (2005). *Computer Forensics: Computer Crime Scene Investigation. (2ed*). Massachusetts: Thompson Course Technology

Van der Walt, S.P., & Venter, H. (2022). Research Gaps and Opportunities for Secure Access Service Edge. *Proceedings of the 17th International Conference on Information Warfare and Security,* 2022, pp 609 – 619.

Yang, C., Lan, S., Wang, L., Shen, W., & Huang, G. G. (2020). Big data driven edge-cloud collaboration architecture for cloud manufacturing: a software defined perspective. *IEEE access, 8,* 45938-45950.

Yasinsac, A., & Manzano, Y. (2001). Policies to Enhance Computer and Network Forensics*. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. United States Military Academy, West Point, NY, June 2001.