Overcoming Obstacles to Adopting Artificial Intelligence in Identity and Access Management

Allan Masawi[1], Machdel Matthee[1]
[1] University of Pretoria, Pretoria, South Africa
masawi9@gmail.com; machdel.matthee@up.ac.za

Abstract. Cyber-attacks are on the increase, and are becoming more complicated as technology advances and affecting people as well companies globally. Advanced approaches to mitigating cyber-risk are required. One of the advanced approaches to managing cyber-attacks is the use of Artificial Intelligence (AI) in Identity and Access Management (IAM). The adoption of AI in IAM is slow as there are various obstacles encountered. This study establishes obstacles a survey using semi-structured questions. 15 participants working in the financial services industry as AI, IAM and cybersecurity experts were interviewed in the survey. Enablers for the adoption of AI in IAM were established from these participants as well. Several of the enablers gathered from the interviews are confirmed by literature. A number of interviewees highlighted high levels of maturity of IAM as a precondition for successful use of AI to support IAM. Furthermore, the interviews confirm organisations' uncertainty of AI capabilities, fears of job security and lack of AI skills.

Keywords: Identity & Access Management, Artificial Intelligence, Cybersecurity and adopting Artificial Intelligence

1 Introduction

Cyberattacks, especially automated attacks are on the increase due to a fast growth in bot traffic (Williams, 2022). In addition, cyberattacks are increasing and becoming more complicated (Mohammed, 2020). Some organisations are adopting Artificial Intelligence (AI) to improve identity and Access Management (IAM). IAM is a subset of cybersecurity and it focuses on aspects such as identification, authentication (e.g., role-based access control, rule-based access control, mandatory access controls and discretionary access controls), authorization, as well as the identity and access provisioning lifecycle (e.g., provisioning, reviewing and revoking access) (Gordon, 2015: 635–729). The global market of AI in cybersecurity is anticipated to grow by 23.6% from 2020 to 2027, reaching $46.3 billion **(**Meticulous Research, 2022).

Despite the potential value of AI, researchers such as Mariemuthu (2019) and Biallas and O'Neil (2020) observed in their studies that the adoption of AI is slow global-

Smuts, Hanlie & Hinkelmann, Knut (2024). Proceedings of the 4th Conference Society 5.0 - Innovation for Sustainable and Inclusive Social Good, Volume 2, Mauritius, 26-28 June 2024, DOI: 10.5281/zenodo.11612759

DOI: 10.5281/zenodo.11619876

ly. This paper aims to identity obstacles to adopting AI in IAM and recommend enablers for its adoption in this subsection of cybersecurity.

2 Literature Review

2.1 The Adoption of AI In IAM

AI can be used in IAM to detect anomalies, for authentication, provisioning, responding to Distributed Denial of Service supporting decisions, handling incomplete and imperfect data and data reduction. Below are some examples of how AI can be used in IAM.

Anomaly detection – Traditional methods are no longer capable cope with modern attacks (Zhang *et al.,* 2022). Kanimozhi and Jacob (2019) proposed using Artificial Neural Networks to detect botnet attacks. Aljamal *et al.* (2019) suggests a combination of IDS, K-means clustering algorithms and the Support Vector Machine (SVM) classification algorithm to monitor behaviour on IT systems and the network. Furthermore, AI can identify regression and outliers (Campbell & Ying, 2011).

Analysing biometric information – Artificial Neural Networks (ANNs) can be used to compare fingerprints while confirming the distance between feature points (Sudiro and Lukman, 2015). Genetic feature learning networks and facial expression recognition to authenticate users (Verma *et al.,* 2019). Deep Convolution Neural Networks can be used to recognise the iris for authentication (Gangwar and Joshi, 2016). Recurrent Neural Networks (RNNs) can be used for voice recognition (Amberkar *et al.*, 2018).

Authentication – Benefits of intelligent authentication include efficiency, reliability, continuous protection and situation awareness (Fang *et al.*, 2019). A random forest algorithm can be used for multi-factor authentication combined with Neural Networks (NN) for monitoring typing speed and style (Zhang *et al.,* 2022).

Detecting Distributed Denial of Service (DDoS) - Deep learning (Li, 2018), K-Means and SVM (Jyothi *et al.,* 2016), Deep Learning, CNN and RNNs (Yuan *et al.*, 2017), K-NN, NN and SVM (Khalaf *et al.*, 2019) can be used to detect DDoS attacks.

Supporting decisions – AI can be adopted to support decisions where IAM is automated (De Ville, 2013).

Handling incomplete data, imperfect data and data reduction – K-Nearest Neighbour can be used to reduce data for analysis, handle imperfect data and input missing values (Triguero *et al.*, 2019).

Provisioning – Expert systems can be used for user provisioning (Qi *et al.,* 2007).

2.2 Obstacles Towards the Adoption of AI in Organisations

Due to limited literature on obstacles to the adoption of AI in IAM, the researchers considered literature describing obstacles to the adoption of AI in general and barriers to the adoption of AI in cybersecurity more specifically. A list of barriers or obstacles

as identified in the literature is provided below. The barriers are categorized using the Technology-Organisation-Environment (TOE) framework of Tornatzky and Fleischer (1990). Table 1 shows obstacles identified through literature review.

Table 1. Table showing obstacles identified through literature review

Obstacle	Explanation	References
Technology		
Security concerns	Data security concerns	Brynjolfsson & McAfee (2018), Ransbotham *et al.* (2017)
Technology capabilities	Lack of resources required to implement AI	Alsheibani *et al.* (2019)
Data quality	Poor data quality, lack of intent to share data, absence of huge volumes of data, insufficient historical data, unlabeled data	Shrivastav (2021), Thowfeek *et al.*(2020), (Ansari *et. al.*, 2022)
Organisational barriers		
Governance	Absence of regulations, collaborations, government involvement, frameworks for sharing data between business units, undefined roles and responsibilities, ill-defined accountability for algorithms , lack of aligned ethics and governance	Shrivastav (2021), (Stone *et al*., 2022)
Lack of skills	Lack of skills to evaluate, build and implement AI solutions	Alsheibani *et al.* (2019), Ransbotham *et al.* (2017)
Lack of executive support	Unclear business case results in lack of support from top management	Shrivastav (2021), Ransbotham *et al.* (2017), Alsheibani *et al.* (2019), Radhakrishnan and Chattopadhyay (2020)
Lack of funding	Inadequate funding is provided for AI across the organization – value not always clear - ROI	Shrivastav (2021), Alsheibani *et al.* (2019)
Unclear business case	Unclear about which aspects of AI will be of value	Alsheibani *et al.* (2019)
Perceptions of AI	Employees fear of change, fear of job security, unreasonable expectations of AI, inconsistent performance metrics	Shrivastav (2021), Alsheibani *et al.* (2019)
Operationalizing AI	Legacy systems not compatible with AI systems	Shrivastav (2021),
Environmental barriers		
Consumer trust	Privacy concerns	(Stone *et al*., 2022)
Geo-political factors	Absence of regulations, government involvement,	Alsheibani *et al.* (2019)

It is assumed that the obstacles to the use of AI in the Identity and Access Management will be similar to those described in Table 1. The next section describes the method followed to get practitioners' opinion on the obstacles of AI adoption in IAM specifically. In addition, these practitioners' suggestions on how to overcome these obstacles, were also elicited.

3 Method

A survey was conducted using semi-structured questions to identify obstacles to adopting AI in IAM. Fifteen (15) participants (professionals in IAM and cybersecuri-

ty) from four banks in the financial services industry in South Africa participated in the study. These participants were selected using purposive sampling. The designations of the participants were Head: Technology and Digital, Head: IT Security, Head: Logical Access, Head: Technology Risk, Senior Cybersecurity Engineer, CEO of a technology consulting company, a partner responsible for cybersecurity consulting at an audit firm, Enterprise Security Architect, Chief Information Security Officer, Assistant IT Audit Manager, Logical Access Expert and Head: IT Audit. The number of years of experience ranged from 5 to 11 years. The participants worked in both big banks and smaller banks or had done consulting work in banks. The interviews were conducted and recorded via Zoom and transcribed and analysed using thematic analysis guided by the TOE framework. The first part of the interview was on understanding their perceptions of the obstacles towards adoption of AI in IAM in the financial sector. The second part of the interview posed questions categorized according to the TOE framework on elements necessary for the promotion of the adoption of AI in IAM.

4 Findings

4.1 Obstacles to Adopting Artificial Intelligence in Identity and Access Management

In the survey conducted, the researcher asked the question, "What do you think are the obstacles to adopting AI in IAM?". Table 2 depicts the obstacles to adopting AI in IAM identified by participants during in the survey.

Table 2. Obstacles to adopting AI in IAM identified in the survey carried out

	Themes	Freq.
1	AI is a new concept	10
2	Legacy systems may not be compatible with AI technologies	4
3	The basics of IAM are not in place	4
4	Lack of AI skills	4
5	AI is considered an expense and management is not reducing costs.	3
6	Either or both a lack of data and poor data quality	3
7	Concerns over data security	2
8	Fear of AI taking over	2
9	Fear of job losses	2
10	Concerns over regulatory compliance	1
11	Lack of trust in AI	1
12	People not willing to change and embrace new technology.	1
13	Systems are not integrated	1

Listed below are themes that appeared the most frequent as obstacles to adopting AI in IAM. (1) AI is a new concept, for example participants stated that "…AI is still maturing…". (2) Legacy systems may not be compatible with AI technologies, for

example participants stated that "…Systems are not integrated…, …Banks still use legacy systems…" impact adoption of AI. (3) The basics of IAM are not in place, for example participants stated that "…some organisations are still struggling with IAM basics…". (4) Lack of data and/or poor data quality, for example participants stated that "…Lack of data…" impacts adoption of AI. (5) A lack of AI skills. (6) AI is considered a cost, for example participants stated that "…there are costs associated with adoption of AI…".

4.2 Measures to Address Obstacles to Adopting Artificial Intelligence in Identity and Access Management

The Technology Organisation and Environment (TOE) framework was used to obtain feedback from the participants and categorise the findings.

Technology Factors - The researcher asked the question: "From a technology perspective, what needs to be in place to promote the adoption of AI in IAM?". Table 3 contains the technological enablers identified in the survey.

Table 3. Technology enablers for adopting AI in IAM

	Themes	**Freq.**
1	Systems should be integrated	6
3	Quality data should be available	6
5	There should be infrastructure to store and process data	5
2	Experts such as AI, IAM and integration experts are required	4
4	AI use cases should be well articulated	3
6	Organisations setting up learning environments on platforms	2
7	Networks should be reliable	2
8	Data should be secured	2
10	IAM processes need to be reviewed and refined	2
12	Modernise legacy systems	2
9	Confirm service providers with AI technologies to be implemented	1
11	Technology needs to be robust	1
13	Ease of implementation and configuration	1

The most frequent technology related themes to adopting AI in IAM are listed below. (1) Technology should be integrated ("… APIs should be used to integrate legacy systems with AI technologies …"). (2) There should be AI, IAM and Integration skills,, for example participants stated"… The right skills should be in place …". (3) Data should be of good quality, for example participants stated"… Data should be of good quality as AI is based on learning …". (4) There should be infrastructure to store and process data. (5) AI business case should be well articulated.

Organisational Factors - The researcher asked the question, "From an organisational perspective, what key elements need to be in place to promote the adoption of AI in IAM?". Table 4 contains the organisational enablers identified in the survey.

Table 4. Organisational enablers for adopting AI in IAM

	Themes	Frequency
1	Top management support	8
2	A budget for AI adoption should be in place	6
3	Culture of innovation, learning and change	6
4	There should be AI training and awareness	6
5	AI and IAM skills should be in place	5
6	A well-articulated business case	3
7	Change needs to be managed	3
8	Governance of AI	3
9	A drive to implement AI	2
10	Leadership and strategy that drive AI adoption	2
11	A cybersecurity framework/programme needs to be in place	1
12	Cybersecurity needs to be a board agenda	1
13	Orgs. need to recruit the right people to support the AI initiative	1
14	Integration of technologies	1
15	Addressing risks associated with the use of AI	1
16	Acquiring platforms for using and exploring AI,	1
17	Creating efficiencies in IAM	1
18	Stakeholder engagement	1

The most frequent technology related themes to adopting AI in IAM are listed below. (1) There should be a budget for AI adoption. (2) A culture of innovation, learning and change , for example participants stated"… A culture that embraces change and accepts AI…". (3) AI training and awareness, for example participants stated "…Education and awareness on AI …". (4) IAM and AI skills, for example participants stated"… The right skills are required….".

Environmental Factors - The researcher asked the question, "From an external environment perspective, what elements need to be in place to promote the adoption of AI in IAM?". Table. 5 contains the environmental enablers identified in the survey.

Table 5. Environmental enablers for adopting AI in IAM

	Themes	Frequency
7	Regulatory bodies should provide guidance and expectations	10
2	AI training and awareness	4
9	Guidelines and best practices should be provided by industry bodies	3

1	AI and IAM skills are required	2
8	Financial regulators need to define standards to protect data.	2
3	Studying external AI success stories	2
4	Regulatory acceptance of the use of AI	2
5	Arms of the government need to be up-to-date with AI (e.g. police)	1
6	Engaging partners and vendors play key roles	1
10	Collaboration at industry level	1
11	External bodies should drive the AI initiative as a roadmap	1

The more frequent themes associated with Environmental enablers are listed below. (1) regulatory bodies should provide guidance and expectations, for example participants highlighted that "… Regulatory bodies should put in place laws on the use of AI ….". (2) AI training and awareness, for example participants stated"… Knowledge and capabilities of what AI can do in IAM…..". (3) Industry bodies should provide guidelines, for example participants highlighted that "… Industry bodies can help educate people and organisations in terms of AI, what AI can do and controls that should be in place ….".

5 Discussion – Obstacles to AI Adoption in IAM

The following obstacles identified through literature review were confirmed through the survey - lack of skills, legacy systems, systems not integrated, lack of trust in AI, fear of job loss, fear of AI taking over, poor data quality, security concerns, perception of AI and concerns over regulatory compliance (see Fig. 1).

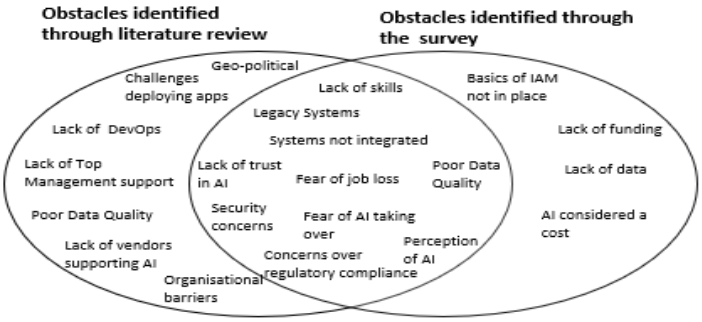

Fig. 1. – Verifying obstacles identified in literature review with obstacles identified through the survey carried out.

Basics of IAM not in place, lack of funding, lack of data and AI considered a cost were identified in the survey but not through literature review. More than one participant mentioned that IAM needs to be at an adequate maturity level before the use of AI can be considered. Note that the literature focused on the adoption of AI in organisations in general. Interesting enough important obstacles identified in the literature

were not mentioned by the participants such as (1) lack of top management support, (2) poor data quality and (3) lack of vendors supporting adoption of AI.

6 Discussion - Overcoming Obstacles to Adopting Artificial Intelligence in Identity and Access Management

From the themes identified in the data analysis and existing literature the following enablers for the adoption of AI in IAM are presented. The enablers are discussed according to the three dimensions of the TOE framework.

6.1 Technological Enablers

Modernising Legacy systems - AI technologies should be compatible with infrastructure, and data sources (Chen *et. al.*, 2023). It was observed in the survey that legacy systems may need to be replaced, upgraded/modernised or have interfaces built.
Integration of Systems -The survey carried out, established that IT systems should be integrated, Experts such as Integration Experts and System Architects should work together and networks should enable system integration.
Data availability and quality - To address lack of data and/or poor data quality, a data strategy and data a management policy should in place (Tyler *et al.*, 2016). In the survey, it was established that data should be structured, be of good quality, infrastructure should be in place to process the data, infrastructure to store data and process data should be in place, the network should be reliable and technology should be robust. Furthermore, there should be huge quantities of data.
Implementing IAM basics – From the survey conducted, it established that the basics of IAM need to be in place, IAM processes should be mature, the organistion should have IAM experts (this could be inhouse or outsourced) and an IAM solution should be in place.
Addressing security concerns – The survey highlighted that data should be secured and data protection standards should be defined.

6.2 Organisational Enablers

Top management support when adopting AI in IAM - Appointing a Chief Data Officer and highlighting the importance of AI is crucial (Solaimani *et al.,* 2023). Top management should understand the basics of AI (Butner and Ho, 2019). There should be commitment to adopt technology AI from executives (Alsheibani *et al*., 2019). Executive management should be engaged to obtain their buy-in (Alsheibani *et al.*, 2020a; Alsheibani *et al.*, 2020b). An AI strategy should be drafted, approved and implemented and it should be aligned to the business strategy (Pumplun *et al.*, 2019). A business case for the adoption of AI in IAM should be documented and presented to the appropriate forums (Solaimani *et al.,* 2023). The business case should articulate the benefits of AI in IAM such as, AI should improve process efficiency (Alsheibani *et al.*, 2020a, 2020b).

Adequate funding for the adoption of AI in IAM - A budget for adoption of AI is crucial for the adoption of AI (Chen *et. al.*, 2023). in IAM. Top management support, AI strategy and business case for adoption of AI in IAM are important for the budget to be approved by top management. Executive management should understand the basics of AI and there should be commitment to adopt new technologies (Solaimani *et. al.,* 2023). AI strategy and business case were discussed above.

Skills available to adopt AI in IAM - Lack of AI and IAM skills can be addressed through learning platforms, partnership with vendors, multi-disciplinary collaboration and talent management. When AI and IAM skills gaps exist in the organisations vendors can be used to address the challenge. However, the vendors should be accessible and provide reliable services (Chen *et. al.*, 2023). The organisation should have programs to reinforce learning, attract talent, partner with recruitment companies, and leverage on internal staff (Lee and Shin, 2020). There should be learning and development plans to familiarize everyone with AI (Agrawal et al., 2017). In addition to the above, It was established in the survey conducted that the organisation should acquire learning platforms to promote learning and adoption of AI. Inter-departmental communication and corporation is important to fill the skills gap when adopting AI (Chen *et al.*, 2023) in IAM. Organisational structures should ensure there is multi-disciplinary collaboration (Bughin *et al.*, 2017a). It may be difficult to recruit professionals with bit AI and IAM skills, in such instances AI experts should work closely with IAM experts.

Addressing fear of job loss and fear of AI taking over - Fear of job loss and AI taking over can be addressed through training (discussed above) and an innovation, learning, change & agile culture. The organisation should have a change management strategy which encourages employees to adopt to new conditions (De Cremer, 2019). The organisation should establish an agile culture which promotes the adoption of new technologies, continuous learning and adjusting to market trends (Brynjolfsson and Mcafee, 2017; Ransbotham *et al*., 2017).

Management of perceptions of AI - The perception of AI is influenced by factors such as AI success stories, Government involvement and AI governance. Based on feedback from the survey carried out, studying organisations that AI has been successfully implemented has a positive impact on the perception of AI. Government support is crucial to assist organisations innovate (Chen *et. al.*, 2023). Executive management should establish authority and governance over AI (Alsheibani *et al.*, 2020a) to build trust in AI.

6.3 Environmental Enablers

Trust in AI - Trust in AI is impacted by factors such as the existence of regulations governing the use of AI as well as AI Governance in organisations. Therefore, regulators and regulatory bodies should provide guidelines on the implementation of AI through laws, standards and frameworks (Lee and Shin, 2018).

A regulatory framework to guide adoption of AI -The survey carried out established that regulatory framework that provides guidance on the adoption of AI is required, regulators need to be aware of the developments in AI, regulatory bodies should em-

brace AI. Organisations should actively monitor changes/ new regulations (Solaimani *et al.,* 2023). Regulators should constantly monitor the change AI landscape and provide appropriate guidelines (Butner and Ho, 2019).
Vendors supporting AI - Should there be no vendors supporting AI, the organisation should consider training and talent management to build the necessary capacity and skills in terms of IAM and AI expertise.

7 Conclusion

This paper established obstacles to adopting AI in IAM and enablers for the adoption of AI in IAM. While obstacles to adopting AI in IAM exist, it is possible to overcome barriers through the enablers identified in this paper. It was noted that technology and organisational factors are within the control of the organisation. Environmental factors may not always be within the control of the organisation for example, regulations. In the event where there are no or minimum regulatory guidelines (depending on industry and size of the organisation), it may be advisable to engage the industry regulatory bodies to ensure there is alignment in terms of expectations from the regulator. From the literature and the survey, it is clear that government has an important role to play in the adoption of AI. In addition, higher education institutions should adopt curricula to reduce the gap between what industry needs and what is taught regarding cybersecurity and AI. Limitations include a small sample size: only four banks were considered in the sample. As such, the obstacles and enablers identified towards the use of AI in IAM suggested here, may not exhaustive. In addition, the enablers are more general and applicable to the adoption of AI in general due to the fact that most of the banks are still in the process of implementing AI for IAM.

References

1. Agrawal, A., Gans, J. and Goldfarb, A., 2017. What to expect from artificial intelligence.
2. Aljamal, I., Tekeoğlu, A., Bekiroglu, K. & Sengupta, S. 2019. Hybrid intrusion detection system using machine learning techniques in cloud computing environments. In *2019 IEEE 17th international conference on software engineering research, management and applications (SERA)* (pp. 84–89). IEEE.
3. Alsheibani, S.A., Cheung, D. & Messom, D. 2019. Factors inhibiting the adoption of artificial intelligence at organizational-level: A preliminary investigation. *Twenty-fifth Americas Conference on Information Systems*, Cancun.
4. Alsheibani, S., Messom, C. and Cheung, Y., 2020a. Re-thinking the competitive landscape of artificial intelligence.
5. Alsheibani, S.A., Cheung, Y., Messom, C. and Alhosni, M., 2020b. Winning AI Strategy: Six-Steps to Create Value from Artificial Intelligence. In *AMCIS* (Vol. 11).
6. Amberkar, A., Awasarmol, P., Deshmukh, G. & Dave, P. 2018, March. Speech recognition using recurrent neural networks. In *2018 International conference on current trends towards converging technologies (ICCTCT)* pp. 1–4. *IEEE*.
7. Ansari, M.F., Dash, B., Sharma, P. and Yathiraju, N., 2022. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering*.

8. Biallas, M. & O'Neill, F. 2020. Artificial intelligence innovation in financial services. *International Finance Corporation* 85(6).
9. Brynjolfsson, E. & Mcafee, A. 2017. Artificial intelligence, for real. *Harvard Business Review*, *1*, pp.1–31.
10. Bughin, J., McCarthy, B. and Chui, M. 2017. Havard Business review*: A Survey of 3,000 Executives Reveals How Businesses Succeed with AI* [Online] Available from :https://hbr.org/2017/08/a-survey-of-3000-executives-reveals-how-businesses-succeed-with-ai [Accessed 2-24-02-29].
11. Butner, K. and Ho, G., 2019. How the human-machine interchange will transform business operations. *Strategy & Leadership*, *47*(2), pp.25-33.
12. Campbell, C. & Ying, Y. 2011. Learning with support vector machines*. Synthesis lectures on artificial intelligence and machine learning*, 5(1):1–95.
13. Chen, H., Li, L. and Chen, Y., 2021. Explore success factors that impact artificial intelligence adoption on telecom industry in China. *Journal of Management Analytics*, *8*(1), pp.36-68.
14. De Cremer, D., 2019. Leading artificial intelligence at work: A matter of facilitating human-algorithm cocreation. *Journal of Leadership Studies*.
15. De Ville, B. 2013. Decision trees. *Wiley Interdisciplinary Reviews: Computational Statistics*, 5(6):448–455.
16. Fang, H., Wang, X. & Tomasin, S. 2019. Machine learning for intelligent authentication in 5G and beyond wireless networks. *IEEE Wireless Communications*, *26*(5), pp.55–61.
17. Gangwar, A. & Joshi, A. 2016. DeepIrisNet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition. *2016 IEEE international conference on image processing (ICIP)*, pp. 2301–2305. *IEEE*.
18. Gordon, A. 2015. *Official (ISC)^2 guide to the CISSP CBK*. Broken Sound Parkway, NW: Taylor & Francis Group.
19. Kanimozhi, V. & Jacob, T.P. 2019. Artificial intelligence-based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *2019 International Conference on Communication and Signal Processing (ICCSP)*. pp. 0033–0036. *IEEE*.
20. Khalaf, B.A., Mostafa, S.A., Mustapha, A., Mohammed, M.A. & Abduallah, W.M. 2019. Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access*, *7*, pp.51691–51713.
21. Jyothi, V., Wang, X., Addepalli, S.K. & Karri, R. 2016. Brain: Behavior based adaptive intrusion detection in networks: Using hardware performance counters to detect DDOS attacks. *2016 29th international conference on VLSI design and 2016 15th international conference on embedded systems (VLSID)* (pp. 587–588). *IEEE*.
22. Lee, I. and Shin, Y.J., 2018. Fintech: Ecosystem, business models, investment decisions, and challenges. *Business horizons*, *61*(1), pp.35-46.
23. Lee, I. and Shin, Y.J., 2020. Machine learning for enterprises: Applications, algorithm selection, and challenges. *Business Horizons*, *63*(2), pp.157-170.
24. Li, J.H. 2018. Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), pp.1462–1474.
25. Mariemuthu, C.O.R. 2019. *The Adoption of Artificial Intelligence by South African Banking Firms: A Technology, Organisation and Environment (TOE) Framework*. Doctoral Dissertation, University of the Witwatersrand, Faculty of Commerce, Law and Management).
26. Mathew, A. 2020. Human-centered AI and security primitives. *Journal of Computer Science Research*, 2(4):32–35.
27. Pumplun, L., Tauchert, C. and Heidt, M., 2019. A new organizational chassis for artificial intelligence-exploring organizational readiness factors.

28. Qi, J., Wu, F., Li, L. & Shu, H. 2007. Artificial intelligence applications in the telecommunications industry. *Expert Systems*, *24*(4), pp. 271–291.
29. Radhakrishnan, J. and Chattopadhyay, M., 2020. Determinants and barriers of artificial intelligence adoption–A literature review. In *Re-imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation: IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2020, Tiruchirappalli, India, December 18–19, 2020, Proceedings, Part I* (pp. 89-99). Springer International Publishing.
30. Ransbotham, S., Kiron, D., Gerbert, P. & Reeves, M. 2017. Reshaping business with artificial intelligence: Closing the gap between ambition and action. *MIT Sloan Management Review*, *59*(1).
31. Shrivastav, M.: Barriers Related to AI Implementation in Supply Chain Management. Journal of Global Information Management (JGIM), 30(8), 1-19 (2021).
32. Solaimani, S., Dabestani, R., Prentice, T.H., Ellis, E., Kerr, M., Choudhury, A. and Bakhshi, N., 2023. Exploration and Prioritization of Critical Success Factors in Adoption of Artificial Intelligence: a mixed-methods study. *Int. J. Bus. Inf. Syst.(Forthcom.)*.
33. Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., Kraus, S. and Leyton-Brown, K.:Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence. arXiv preprint arXiv:2211.06318, (2022).
34. Sudiro, S.A. & Lukman, S. 2015. Minutiae matching algorithm using artificial neural network for fingerprint recognition. *2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)*, pp. 37–41. *IEEE*.
35. Thowfeek, M.H., Samsudeen, S.N. & Sanjeetha, M.B.F. 2020. Drivers of artificial intelligence in banking service sector. *Solid State Technology*, *63*(5), pp.6400–6411.
36. Tornatzky, L. G., & Fleischer, M. 1990. *The processes of technological innovation*. Lexington, MA: Lexington Books.
37. Triguero, I., García-Gil, D., Maillo, J., Luengo, J., García, S. & Herrera, F. 2019. Transforming big data into smart data: An insight on the use of the K-nearest neighbors algorithm to obtain quality data. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(2):1289.
38. Tyler, B., Abercrombie, C. and Shockley, R. 2016. *The Chief Data Officer Playbook: Creating a Game Plan to Sharpen your Digital Edge,* New York: Somers.
39. Verma, M., Vipparthi, S.K. & Singh, G. 2019. Hinet: Hybrid inherited feature learning network for facial expression recognition. *IEEE Letters of the Computer Society*, *2*(4), pp.36–39.
40. Yuan, X., Li, C. & Li, X., 2017. Deep defense: Identifying DDoS attack via deep learning. *2017 IEEE international conference on smart computing (SMARTCOMP)* pp. 1–8. *IEEE*.
41. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F. & Choo, K.K.R. 2022. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), pp.1029–1053.