ARTIFICIAL INTELLIGENCE-BASED ACCESS MANAGEMENT SYSTEM

By

Victoria Adenola

May, 2023

Director of Thesis: Dr. John Pickard

Major Department: Department of Technology Systems

ABSTRACT

The foundation of cybersecurity is identity and access management (IAM). Its methods, procedures, and guidelines control identity access to digital resources and define the scope of identity permission over the resources. Every week, a new data breach or cyber threat is reported. A significant number of data breaches are caused by ineffective security features, software vulnerabilities, human error, malicious insiders, and the misappropriation of access and privileges. Artificial intelligence (AI) techniques can upgrade the access management system. As a result, research into artificial intelligence in IAM is required to enable organizations to take a more detailed and flexible approach to authentication and access control to mitigate cyber threats and other IAM challenges. This study explores the relationship between access management systems and artificial intelligence with regard to AI applications in identity and access management, specifically the monitoring, administration, and control of access privileges. The objective of this study was to provide evidence from the relevant literature to help understand how AI works in mitigating identified IAM challenges. The findings in this study demonstrate how artificial intelligence strengthens identity and access management in mitigating growing cyber threats, automating processes, and keeping up with technological advancements.

Keywords: access control, artificial intelligence, access management, identity management, AI techniques

Artificial Intelligence-Based Access Management System

A Thesis

Presented to the Faculty of the Department of Technology Systems

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Network Technology

By

Victoria Adenola

May, 2023

Director of Thesis: John Pickard, Ph.D.
Thesis Committee Members:
Li Peng, Ph.D.
Popoviciu Ciprian, Ph.D.

ACKNOWLEDGEMENTS

I would like to give sincere thanks to the following individuals for their invaluable support and guidance throughout my research. First and foremost, I would like to thank God for His Grace. His love and favor have sustained me throughout my life. I would like to sincerely thank my advisor, Dr. John Pickard, and my committee members, Dr. Peng Li and Dr. Ciprian Popoviciu, for their commitment, support, and insights. Without them, this research would not have been possible.

I am deeply grateful to my family for providing me with the opportunity to obtain this solid education as well as the tools I need to succeed in life. They have been a tremendous source of inspiration and motivation for me. I would also like to thank Dr. Mohammed (TJ) for encouraging me to start working on my thesis. Finally, I would like to express my gratitude to my friends Ire Fakeye and Nelson Adeniji, who generously gave their time and assisted me in aligning my thoughts throughout this thesis process.

Thank you all for your support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Individuals and organizations interact continuously in today's global and highly interconnected work environment. The internet connects hundreds of millions of systems worldwide that run on various hardware and software technologies to provide communication and commercial services and has become a part of everyday life (Kumar et al., 2010). While organizations are becoming more productive and efficient, they risk becoming targets for data breaches and other cyber threats. For many organizations, determining which individuals should be granted access to a particular information can be a complex task for numerous organizations, and disregarding it could render their systems vulnerable (Mohammed I. A., 2021).

Access management, also referred to as access control, involves the verification, authorization, and accountability of an individual's identity when they are granted access to resources. With defined access management, the access control system determines whether the proper individual is accessing the resources (Mohammed et al., 2018; Schrimpf et al., 2021). The foundation of computer security is access control, which entails the four essential steps of identification, authentication, authorization, and accountability (Lal et al., 2016). The process entails enforcing access control policies to ensure a prompt and effective response to any requests for accessing company resources (Damon, 2019). The core objective of access control is to improve the confidentiality and security of IT assets i.e., improving its resource confidentiality. An effective access control system shields the network from unauthorized access (Mohammed et al., 2018). IAM ensures that end users have a great user experience balanced with the appropriate security practices. Policymakers have passed several regulations mandating corporations to implement IAM technology to safeguard end-users from privacy concerns and identity fraud (Khansa & Liginlal, 2012). These regulations, as well as the concept of fairness and legal requirements, have led to significant changes in individual privacy. Two examples of such changes include the draft US Privacy Bill of Rights and the European Union (EU) General Data Protection Regulation (GDPR).

This paper uses the term "IAM" (Identity & Access Management) interchangeably with access management. IAM manages resource access (Sharma et al., 2016) by identifying and determining the necessary access levels and user privileges through policies and techniques which control access to digital resources. Identity management and access management interact together so that identity management is responsible for authentication while access management oversees authorization (Sharman et al., 2012). This is accomplished by confirming an entity's identification, following which access is provided at the appropriate level based on the protected resource's policy (CSA, 2009; Schrimpf et al., 2021). IAM aims to ensure identity federation by using a single identity across systems and other features such as single sign-on, strong authentication (MFA), access control, account management, and provisioning. In addition, IAM is responsible for determining the proper user access to a system and classifying the user’s access and permission level (Sim et al., 2019). IAM also addresses challenges related to password management, regulating compliance, and securing APIs. According to research by (Mohammed et al., 2018), identity and access management systems collaborate to regulate user access to resources and programs.

Organizations typically emphasize their profit-serving operations in the fast-paced IT environment, losing sight of potential risks. Effective risk management is a time-consuming task requiring close supervision and high expertise (Hosam, 2022). Humans make decisions by adhering to rules, regulations, and standards. However, information security risk management calls for an integrated system. Risk assessment and reduction can benefit from an automated and intelligent approach (Murugan & Kuppusamy, 2016; Hosam, 2022). New technologies are constantly emerging, enabling process automation and providing new insights that can significantly accelerate existing IAM compliance controls and reduce their overall time to market (Mohammed I. A., 2021). IAM continually expands in data security, authentication, synchronizing corporate data, managing customer contact preferences, and meeting regulatory privacy requirements (Nikolova, 2020). The idea behind an AI-based system is that the more intelligent an IAM method is, the lower the security risk. Because AI can detect patterns and learn at the same rate as risk, it will be critical in the future of IAM.

Artificial intelligence reshapes businesses and organizes innovation management (Mohammed I. A., 2021). AI can be defined in two ways: 1- as a field of study that aims to discover the core of intelligence and develop intelligent systems, and 2- as a field of study that aims to solve complex problems that require the use of intelligent methods (i.e., preventing data breaches and improving access control security, authentication, and confidentiality continually). The second definition is more relevant in applying Artificial Intelligence to Access Management systems. This solution significantly automates IAM, improving user and I.T productivity while improving security and compliance (Mohammed I. A., 2015). Combining artificial intelligence and IAM with appropriate monitoring and assessment technologies makes it feasible to evaluate connectivity and reduce breach vulnerability by applying intelligent, adaptive identity and access control regulations (Indu et al., 2018). The intelligent system for next-generation I.T management improves the accuracy and efficiency of digital identification access permissions in near-real-time (Mohammed I. A., 2021).

Problem Statement

Managing IAM is a significant issue for most organizations due to IT security and compliance requirements, with new data breaches or cyber threat reports emerging weekly (Kunz et al., 2018). As the risks to information security grow, so do the technological requirements to mitigate them. Organizations that depend on IT to thrive must practice effective information security risk management (Hosam, 2022). The problem of this study was to examine the significance of artificial intelligence in IAM in mitigating cyber threats, effectively managing user access, and other information security concerns. As traditional IAM authentication methods (such as passwords or fingerprints) are known to be vulnerable to malicious attacks and misuse, AI helps in authentication by providing adaptive retraining for detection models (Qiu et al., 2019). In addition, it enables a more thorough access management level by providing intelligent user access and robust security measures beyond biometrics (Mohammed I. A., 2021).

Significance of the Study

The field of identity and access management has grown significantly. With remote work being standard and mobile device usage at its peak, artificial intelligence is instrumental in the future of IAM. Therefore, understanding the importance of a well-designed and executed IAM strategy is imperative (Mohammed I. A., 2021). The purpose of the research was to explore the relationship between access management systems and artificial intelligence in terms of the applications of AI in identity and access management, particularly the monitoring, administration, and control of access privileges. Access management, as well as artificial intelligence, are critical components of today's digital transformation initiatives. This study is significant to the field of cybersecurity research because it provides evidence from the relevant literature demonstrating how artificial intelligence strengthens identity and access management in mitigating growing cyber threats, automating processes, and keeping up with technological advancements.

Research Questions

To examine the existing literature in the proposed field, three research questions have been developed:

Research question 1:

How can the capability and effectiveness of the authorization-based user access evaluation process be improved using artificial intelligence techniques?

Research question 2:

How do IAM and artificial intelligence work together to automate critical identity management and user authentication processes?

Research question 3:

How can analytical intelligence reduce information security risks, improve control of privileged activities, boost productivity, and significantly reduce financial losses?

Methodology

A meta-analysis qualitative research method and design are employed in this research. The research provides a brief and thorough summary of the findings from qualitative studies that explored the same research area, developing an in-depth analysis and answering the study's research questions. The literature review aims to gather knowledge, explore ideas, and provide an overview of access management systems and artificial intelligence, how they are understood, and how their implementation benefits cybersecurity. The setting discusses artificial intelligence and machine learning transforming access management and industry-based intelligent identity and access management systems, highlighting IBM AI innovations in identity management, Oracle Adaptive Access Manager, and Cisco Identity Services Engine (ISE).

Thesis Organization

This paper is structured as follows: Chapter One – introduction to the topic; problem statement, its significance, research questions, and methodology. Chapter Two reviews relevant studies such as IAM components, challenges in implementing IAM, AI and Machine learning redefining IAM, and other related subjects. The methodology section of Chapter Three describes and develops the research methodology, design, data analysis, and data collection methods used to address the three research questions and the research limitations. Chapter Four presents the findings of the research and its economic benefits. Finally, the thesis concludes in Chapter Five with a summary and future projections of AI in access management systems.

CHAPTER 2: LITERATURE REVIEW

This chapter introduces references to past research that used the concepts outlined in Chapter 1 and a summary of related literature.

Identity and Access Management

Identity and Access Management (IAM) integrates policies, technologies, and methods used to control digital resource access by identities and determine the permission level identity over these resources (Sturrus & Kulikova, 2016). IAM monitors the authentication, authorization, and access control of regular users and administrators, including privileged access (Carnley & Kettani, 2019). Identity and access management revolves around providing authorized users with the appropriate access to necessary resources for legitimate purposes while monitoring the access granted. It centers on uniquely identifying objects and authentication to confirm a two-party identity relationship (Maple, 2017). This ensures that users are given the appropriate permissions and access control to resources.

IAM maintains consistent identity management across all applications while ensuring security (Indu et al., 2018); its services facilitate granting personalized access privileges based on the individual's identity (Khansa & Liginlal, 2012). Previously, it was not easy to fund IAM projects because they did not directly improve profitability or functionality. However, IAM has recently emerged as an essential foundation for attaining financial advantages, increased efficiency, performance management, and fostering eCommerce business growth (Dhamdhere & Karande, 2015). Today, IAM has grown in popularity, and its increasing importance is evident in the quantity of acquisitions made by IT corporations.

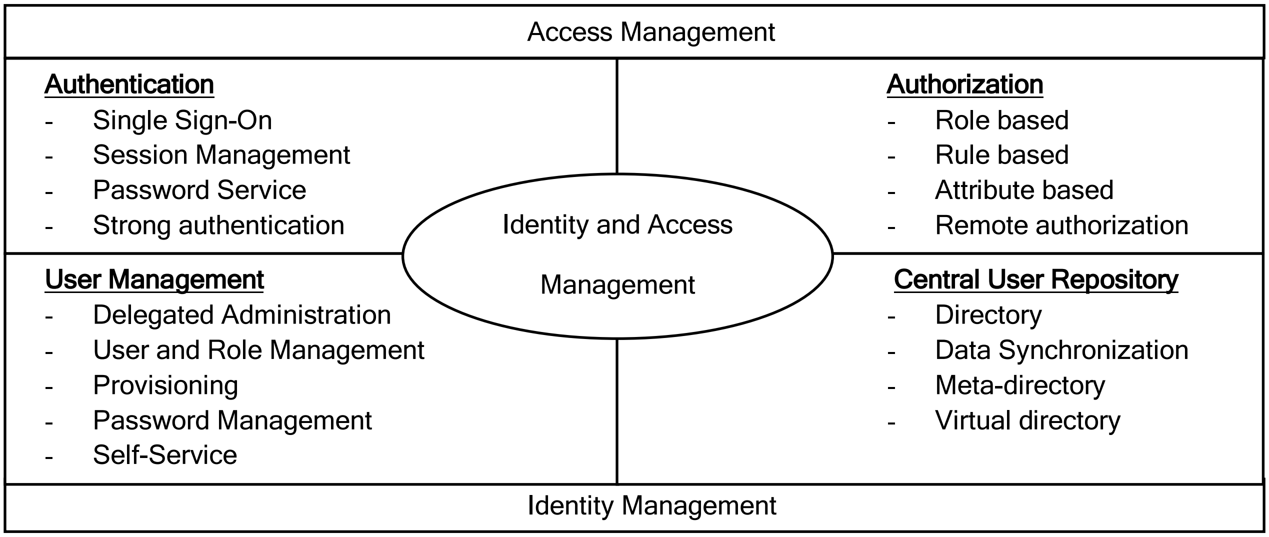
The identity and access management program plan at Harvard University (Harvard University, 2014) states that the program was created to eliminate perceived identity-related complexity. Its goal is to offer secure, convenient access to applications for users, application owners, and IT administrative staff. They also want to develop solutions that require fewer login credentials, enable collaboration across and outside of Harvard, and improve security and auditing (Harvard University Information Technology (HUIT), 2022). Its guiding principles are as follows:

- Tenet #1: Everyone and everything is affected by identity and access management.
- Tenet #2: Identity and access management facilitate user experience.
- Tenet #3: Identity and access management facilitates research and collaboration.
- Tenet #4: Identity and access management protect university assets.
- Tenet #5: Identity and access management promotes technological innovation.

Identity, access, and directory services are the basic categories on which IAM frameworks are based. According to research (Damon, 2019), the importance of IAM is demonstrated by the numerous vendor technology solutions used to facilitate it. As depicted in Figure 1**,** authentication, authorization, user management, and a central user repository are the four key types of IAM components (Dhamdhere & Karande, 2015).

Figure 1

Identity and Access Management Components



Authentication is an access control strategy that involves validating and verifying the identity of an unauthenticated entity. At the same time, authorization is an access control strategy that compares an authenticated entity to a list of data resources and access levels (Whitman & Mattord, 2019). The user management strategy is responsible for various administrative tasks such as creating, propagating, and maintaining user identities and permissions. This section comprises user management, password management, role/group management, and user/group provisioning (Dhamdhere & Karande, 2015), and the central user repository serves as a virtual or combined representation of an organization's identity; it collects and distributes identification information to other services, as well as verifying credentials given by the users.

Secure digital systems inherently involve authentication, authorization, and digital identity management (Sudarsan et al., 2021). Access management leverages identity information to verify the identity of an entity, such as an individual or a device, and grants permission to access the requested resource (Damon, 2019). Identity Management is the foundation for "true" digital transformation, the secure, adaptable, and flexible IT infrastructure that every industry and higher education institution aims to achieve (Rowe et al., 2018). Identity management domains refer to the set of methods and techniques that organizations use to manage user identities throughout the identity management life cycle. The manual or automated processes designed for migrating an identity from one state to another are called Life Cycle Management (Damon, 2019). Identity Life Cycle Management manages the state of identities (Sarkar & Shah, 2018). These processes are not standard and are tailored to each organization's unique identity environment. Although the basic life cycle processes cover most required functions, they must be adaptable enough to meet the organization’s needs (Damon, 2019). Automation technologies are utilized to carry out fundamental operations in managing identity lifecycles, such as user provisioning and de-provisioning, and access privilege management (Hummer et al., 2016). The following are some of the basic life cycle processes (Windley, 2005; Damon, 2019):

- Create - establishes the identity in the identity source
- Modify - changes the identity's attributes
- Delete - removes the identity from the identity source
- Suspend - momentarily disables the identity
- Restore - restores a suspended identity

The identity management system stores all components of the identity management infrastructure. It provides functionalities such as user identification, authentication, authorization, password management, monitoring, centralized management, and delegated administration using this information (Dhamdhere & Karande, 2015). Organizations intend to standardize user management rules for user management to reduce administrative expenses and enhance IT security. These rules are the cornerstone for all identity and access management structures, regardless of whether they are implemented in IT systems or merely exist in the implicit knowledge of experienced identity and access management experts (Hummer et al., 2016). The IAM components are described in more detail as follows:

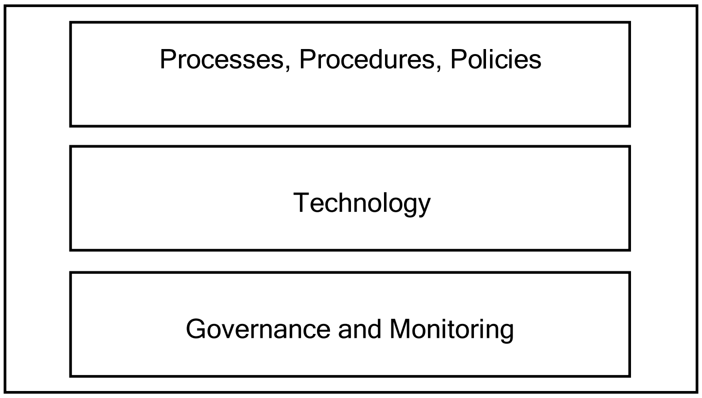
- Compliance control - entails defining and enforcing user access policies.
- Access request and automated provisioning address the identity lifecycle in access request and automated provisioning. Governance features ensure that only the access that the user requires is assigned to the user across the organization.
- Password management – this component minimizes helpdesk calls using policy-driven password processes across all applications.

- Data access governance - the protection of confidential information, ensuring that it is only accessed by authorized personnel and that it is used appropriately and securely.

To define IAM layers that can be used to classify and present IAM components to stakeholders to evaluate organizations' requirements, the three classifications depicted in Figure 2 provide an opportunity.

Figure 2

IAM component model layers



Note. The IAM component model layers are arranged in a hierarchy in which the most critical layer is placed at the top.

An organization's IAM processes, procedures, and policies must be fully understood and inputted into the technology framework, which is confined within the technology layer that determines the technology component selection. Finally, the governance and monitoring layer performs an oversight function by regularly monitoring and reviewing the approved processes, procedures, policies, and technological components.

IAM aims to secure an organization's information technology resources while ensuring a pleasant end-user experience (Osmanoglu, 2013; Damon, 2019). Its systems are currently the most effective mechanisms for mitigating risks; several organizations employ IAM systems to protect data by limiting users' access permissions (Liu et al., 2012). Because its technologies offer an additional layer of protection that may enhance any layer of an IT system, IAM is an essential tool in an organization's cybersecurity armory (Khansa & Liginlal, 2012). IAM can help organizations analyze the threats connected with remote working, bring your own device (BYOD) policies, and mitigate the possibility of data breaches (Mohammed I. A., 2021). Identifying the IAM capability's current state maturity is critical to understanding transformation program requirements and developing the business case for change (Osmanoglu, 2013; Damon, 2019).

Identity and access management features are integrated into organization's infrastructure, deliberately or out of necessity (Damon, 2019), because of the importance of its systems in supporting continuous access to an enterprise's various IT resources by end-users, staffs, and external stakeholders. In addition, IAM systems are crucial in managing access rights by verifying only authorized users with appropriate privileges can access system information (Sharma et al., 2016).

Challenges in the Implementation of IAM

With the growing number of customer/employee accounts and the need to manage them securely, existing identity management approaches have significant difficulties with privacy and interoperability (Wingerde, 2017; Yan et al., 2016). One challenge with IAM is that users are often granted access to resources based on their position within the organization, yet employees are rarely suited to a specific role. Managing employee access to sensitive applications and data is a significant security challenge for many organizations in the digital environment (Hummer et al., 2016; Naik & Jenkins, 2020). In addition, IAM implementations are generally time-consuming and demanding; therefore, many organizations struggle to implement them and entirely use their capabilities (Engström, 2019). As a result, organizations must ensure the setup and management of users' identities and accounts.

Over the last few decades, IAM has become a significant challenge for most organizations to manage fully (Kunz et al., 2018) due to IT security and compliance requirements. All users must also adhere to internal and external regulations; apart from organizational compliance, the organization's personnel must also adhere to external and internal rules for the entire organization to be compliant with existing and future regulations. Ultimately, organizations must ensure that only authorized individuals have access to the right resources at the appropriate time and for the right reasons (Engström, 2019). In addition to the inherent challenges of IAM, cybercriminals have begun to embrace the use of intelligent technology to harm targeted systems potentially. Organizations can withstand this by deploying a mature IAM system, as only an intelligent defense approach can defend equally intelligent threats.

These challenges underline the importance of access management, authorization-based user access levels, and least-privileged implementation. A need-to-know is implied by least privilege, assigning the least level of access required to fulfill the assigned role (Whitman & Mattord, 2019). Due to these existing challenges, the significance of a mature IAM solution is growing in popularity amongst many organizations. Despite its importance, there are few supporting tools for automated detection, modification, and policy management, resulting in outdated policies culminating in security vulnerabilities and inefficiencies (Hummer et al., 2016).

Artificial Intelligence Approach to IAM

Artificial intelligence (AI) transforms identity and access management by allowing organizations to take a more detailed and flexible authentication and access control approach. AI is considered a promising advancement in the modern information age; it has permeated many sectors, including cybersecurity. With all of the cybersecurity concerns with access control (Stallings & Brown, 2018), cybersecurity is undoubtedly one of the most challenging problems. It may gain the most from using AI (Wirkuttis & Klein, 2017). The two broad categories of AI listed below could be integrated into cybersecurity:

1. Data-driven AI - makes predictions and uses machine learning, statistical learning, and evolutionary computing to identify patterns in data.
2. Symbolic AI - concentrates on developing conceptual models, symbolic representations, knowledge-based systems, and logical reasoning to tackle intricate problems, such as optimizing resources, scheduling, and planning, and making decisions based on multiple criteria.

According to various research, the more intelligent an IAM method is, the less security risk. Experts believe that artificial intelligence has the potential to be a strategically important potential driver of the ongoing technological advancement by serving as a tool for intelligence augmentation (IA) rather than a substitute for human thought and reasoning processes (Faruk, et al., 2021). Machine perception, cognitive computing, learning, interaction, reasoning and problem-solving, abstraction, judgment, knowledge representation, and object manipulation are key concepts in AI for developing intelligent systems (Russell & Norvig, 2016). Organizations widely adopt AI technologies for their opportunities (Umurerwa & Lesjak, 2021). However, according to reports from (Gartner, 2017), despite the growing interest in AI, many organizations are still in the data collection phase, and only a limited number have deployed AI. The report also highlights ongoing exploration into how AI can be incorporated into business models, and ignoring AI could pose risks for organizations. AI technologies can be complex and challenging to understand; additionally, blindly embracing AI can lead to various AI-related problems

(Dignum, 2021). Embracing AI as technological innovation will necessitate a continuous digital transformation. As a result, increasing digital organizational readiness through research (such as this thesis) and staying current with technological advances improve the influencing factors (Umurerwa & Lesjak, 2021). Artificial intelligence will transform access control beyond the people, places, and things we currently control as many technology solutions can now interact and learn from each other without human intervention.

Machine learning is a branch of AI that involves building models using algorithms by merging computer science and mathematics. With data-driven training, machine learning models make predictions or decisions comparable to the human brain. And as the number of learning increases, so will the accuracy of the output (Zhu & Al-Qaraghuli, 2022). Planning and scheduling, genetic algorithms, reinforcement learning, neural networks, fuzzy logic, expert systems, computer vision, machine learning (ML), natural language processing (NLP), and robotics are all subfields of AI. According to (Versola, 2021), ML is the most used subfield in cybersecurity. The different types of machine learning include supervised, unsupervised, semi-supervised, and reinforcement learning, which use statistical approaches to enable computer systems to 'learn' from data rather than explicitly programmed. It is most effective when directed at a specific task instead of a broad mission. For example, machine learning includes its application in detecting intrusions or viruses and for user authentication based on biometrics (Dasgupta et al., 2020).

The mathematical methods that integrate decision studying, rationale coding, grouping, intensification, and sensory chains make up ML. The classification algorithm is included in its application for detecting malicious software and malicious code, anomaly detection algorithms for identifying anomalies or harmful traffic, and correlation algorithms for linking signals from disparate systems (Korolov, 2022). AI technologies can help overcome many inadequacies of today's cybersecurity tools due to their flexible and adaptable system behavior (Dilek et al., 2015). For example, the system can look up threats in an existing database to monitor the bad actors and transform IAM to help avoid distress by using intelligent algorithms to detect similar patterns and develop a counterattack mechanism. Over time, the system's speed and efficiency in detecting and responding to unknown threats improve (ServReality, 2022). Ellen MacArthur Foundation states that AI has the potential to deal with complexities and enhance understanding of vast quantities of information and can be viewed as a supplement to human abilities that supports more efficient learning from feedback (Ellen MacArthur Foundation, 2019; Ghoreishi & Happonen, 2020). Artificial intelligence has a much faster detection speed compared to current approaches. AI can assist in the optimization of system functionality, the detection of viruses, the creation of a virus database, and the prediction of cybercriminal movements. In addition, AI can facilitate faster detection of unknown attacks and enable the development of appropriate response techniques without relying on pre-existing strategies (ServReality, 2022; Sjöblom, 2021).

Artificial intelligence can aid in implementing IAM successfully, reducing much aggravation and paving the way for proactive or even corrective access management to replace reactive access management (Mohammed I. A., 2015). AI-based techniques have been applied in many scientific and technological fields because of their potential to analyze large amounts of data. Numerous security-related fields, including privacy (Bosri et al., 2021), trust (Guo, et al., 2020), attack detection (Zhang et al., 2021), and encryption (Ding et al., 2021), have found applications for them.

Technological advances provide unique insights to adapt and automate the procedure, potentially allowing present IAM conformity controls to be significantly accelerated (Berlatsky, 2011). AI is well-placed within the larger context of technological advancements. By combining analytics and artificial intelligence, technical and non-technical employees can improve productivity and operational efficiency (Mohammed I. A., 2015). With this, organizations will remain secure and stay abreast.

AI is considered a tool for organizations to improve their IAM strategy, elevating the significance of the IAM process in cybersecurity and identity and access management (Mohammed I. A., 2015; Tappert & Dixon, 1974). By using AI-powered IAM solutions, organizations can shift from a highly technical approach to access management to a coherent system at all levels. Without AI technology, most organizations believe they cannot detect and withstand attacks. According to a Pillsbury global survey, "cybersecurity-related AI investment is expected to grow at a compound annual rate of 24% until 2027, with a projected market value of $46 billion" (Korolov, 2022). From a Capgemini study, "more than 80% of telecommunications businesses employ AI for security, while 75% of banking executives have embraced the technology – and a trend can be seen across all major industries" (ServReality, 2022). IoT 'based,' decentralized identifiers, and verifiable credentials are just a few technologies that have opened new prospects in IAM (Alomari, et al., 2021). With the advancement of technologies like cloud computing, AI, and big data, communications networks face ever-increasing security risks and threats (Yao et al., 2021). Given this, the growing use of artificial intelligence in numerous sectors has spurred the search for more efficient access management methods.

AI Threats for Security

As cyber technology becomes more accessible, the next generation of threats, exploits, and viruses will probably include cyber technology (ServReality, 2022). Because of this, attacks will be more sophisticated and cause significant damage. Such attack has and is not limited to:

- Creating updates: If the anti-virus detects a previous version, the virus may force an updated version and continue its malicious activities.
- Random changes in executable code: polymorphic viruses have already demonstrated this capability, but AI can expand the number of supported variables to new heights.
- Social detection: Viruses could imitate human speech using conversational programming and facial recognition technologies, tricking users into transmitting confidential information, handing over access data, or even cyberbullying.
- Adapting to operating systems: The AI-based virus may devise an intelligent approach to Kernel-level functions or employ rootkits to avoid detection.
- Recognizing and attacking anti-virus software: an AI-enabled virus can detect anti-virus software and develop methods for attacking its code.

AI and ML transforming IAM

Artificial Intelligence and Machine Learning (ML) solutions can be essential in an effective access management system. AI helps overcome the limits of traditional algorithms and offers more efficient and scalable approaches to problem-solving (Zhu & Al-Qaraghuli, 2022). Capgemini's global cybersecurity portfolio lead- Joe McMann, stated, "While artificial intelligence and machine learning technology improve detection and response in some circumstances, organizations must understand that AI and ML are not solutions in and of themselves" (Korolov, 2022). A closer look at artificial intelligence-based authentication is essential to meet the security needs of emerging networks and circumvent performance limitations (Qiu et al., 2019). Their deployments will benefit the industry by automating intrusion detection and prevention techniques compared to conventional approaches, particularly in the face of evolving cyber-attacks and technological advancements.

The traditional authentication method often works well in a perfect communication environment, but when plausible environment intrusion is included, it significantly reduces its detection accuracy (Qiu et al., 2019). As a result, this authentication method has gradually become outdated due to its lack of a robust security system (Yazdinejad et al., 2019; Zhu & Al-Qaraghuli, 2022). AI-infused authentication systems have grown in popularity in recent years to improve authentication security and make it adaptable to as many real-world scenarios as possible (Zhu & Al-Qaraghuli, 2022). Such solutions will empower organizations to shift from an overly technical approach to access management to a more understandable system at all levels. In 2017, Jiang et al. examined the feasibility of employing adaptive learning techniques in future networks. They proposed using machine learning in compelling applications to tap into previously unexplored applications and services, stating that machine learning is a promising field for research in networking with artificial intelligence (Jiang, et al., 2017; Qiu et al., 2019). For IAM solutions, machine learning can be used to assess whether a user is the "right person," that is, verifying their identity and determining if the data or applications they are attempting to access are “appropriate resources” for that user (Versola, 2021).

Automation and Flexibility

IAM policies can be applied to each access request using AI-powered systems, considering the user's requirements and constraints and eliminating the need for IT professionals to manually determine the "least privilege" for each use case (Frankish & Ramsey, 2014;

Mohammed I. A., 2021; Sennovate, 2022). Furthermore, artificial intelligence can sometimes automate authentication for low-risk access scenarios since it maintains track of the specifics of users' activity. As a result, some of IAM management's duties may be alleviated while protecting users from becoming "security fatigued" (Identity Management Institute, 2021). AI can examine the conditions related to access requests, such as time, location, device type, and the resources requested. By analyzing these conditions, AI can grant network access context-specific and precisely and address any issues caused by erroneous resource provisioning or de-provisioning (Mohammed I. A., 2015).

Breach Detection and Prevention

AI can develop effective, robust, and scalable malware detection modules, which can be utilized to improve breach detection and prevention. Machines can handle massive amounts of information and scan it at a rate that surpasses the capabilities of the most dedicated IT personnel. They can also detect anomalies beforehand, allowing organizations to avoid significant network breaches or data loss. With this, data security incorporating machine learning may learn aspects of user behavior by examining how different identities interact with network systems (Sennovate, 2022; Weske et al., 2007). Adopting futuristic strategies for malware detection programs will bring substantial benefits; various industries must prioritize their efforts to protect user data against malware attacks and other security vulnerabilities and data breaches. (Faruk, et al., 2021). The process is continuous, providing constant monitoring and allowing the ML algorithms to establish a clear depiction of routine network activity (Identity Management Institute, 2021). For example, what happens if a hacker uses a valid user's credentials to access the system? During the session, the system detects changes in behavior or unusual activities and either alert IT professionals or automatically respond by blocking access requests.

AI surveillance and visibility optimization

Identity management has evolved beyond just human users and now includes gadgets and apps, posing a challenge for those responsible for IAM. As cloud services enable network access from any setting or gadgets and as remote workers become more prevalent, the environment becomes even more complicated (Identity Management Institute, 2021). With network systems becoming increasingly interconnected, artificial intelligence-based enhanced authentication systems will become essential in ensuring that information is accessible smoothly, continuously, and accurately. AI systems can monitor user activities on the network and detect anomalies by operating within a user's access rights (Mohammed I. A., 2021). In cases where temporary permissions need to be granted, a more sophisticated approach to access management with better control over privileged access and reduced risk of misuse can be achieved through updates to role-based access controls.

Biometric Authentication

The purpose of authentication systems is to create a mapping relationship between users and objectives. With the aid of AI, biometrics, a multifactor authentication method, can support the design of data-driven security standards. AI transforms biometric authentication to provide a dynamic security solution for a business (Marley, 2021). The purpose of authentication systems is to create a mapping relationship between users and objectives. Artificial intelligence approaches hold great potential for combing large and diverse sets of biometric data to provide users with advanced authentication and identification functionality (Liang et al., 2020). According to research by (Manzoor et al., 2019), biometric data are prone to privacy attacks; therefore, the privacy protection mechanism of the authentication process must be supported by applying a privacy preservation algorithm. Behavioral biometrics differs from knowledge-based authentication and physical biometrics because it offers a unique passive mode operating in the background. It is impossible to duplicate or hack because it is collected based on users' behavior during a specific activity.

Biometric systems are becoming increasingly important in many systems and are central to the scientific research community. Among them, handwritten signature verification has piqued many biometric systems' interest; the behavioral biometric system distinguishes between authentic and previously stored known signatures (Bibi et al., 2018). Normalization of signature data within a specific range is done to improve the interoperability of the data from various electronic devices before extracting advanced features. Unlike static authentication information, behavioral biometric data cannot be forgotten, exchanged, or stolen. Machine learning and deep learning AI solutions can determine access control by checking user identities in continuous authentication (Sjöblom, 2021).

IBM AI Innovations in Identity Management

IBM Security (NYSE: IBM) has extended its AI technology, initially intended for securing financial service users, to clients across all industries through its identity-as-a-service (IDaaS) service (IBM, 2019). IBM Cloud Identity now includes AI-powered adaptive access abilities to monitor user risk levels continuously while accessing applications and services. Abnormal user interactions are escalated for further authentication, while low-risk users are expedited to access the necessary apps and services. According to a survey from 2019, hacked or weak credentials are to blame for more than 80% of data breaches (Verizon Enterprise Solutions, 2019).

As data breaches become more frequent, traditional access control methods like passwords are often inadequate to prevent unauthorized access (Mohammed I. A., 2021). As seen by the increase in credential-stuffing attacks, many password combinations have been leaked, in which a hostile actor acquires a list of credentials and uses a bot to test them at many other sites. Also, given the various applications and passwords employees must manage in their personal and professional lives, preventive security controls must not interfere with the user experience (IBM, 2019). IBM Cloud Identity with Adaptive Access leverages AI to provide organizations a holistic understanding of user access context by analyzing indicators like malware and risk, device information, and user behavior, allowing them to prioritize security measures on high-risk logins. Additionally, it provides many users with better accessibility to their accounts and applications without compromising security (IBM, 2019).

IBM Security Verify

Consider deep context, intelligence, and security when determining which users should access the organization's information and services, on-premises or in the cloud. Securing users' identities across many devices and platforms while maintaining a seamless experience poses hurdles for security professionals, but the payoff is worth it. Many organizations are looking to shift their old IAM solutions to the cloud or integrate them with cloud-based solutions to help with this. The IBM Security Verify solution, modernized and modularized, provides a comprehensive, AI-powered context for consumer and worker identity and access management (IBM, n.d.). With a low-friction, cloud-native, software-as-a-service (SaaS) solution that leverages the cloud, users and applications can be protected inside and outside the company. In addition, customers, employees, contractors, and partners will have secure, low-friction access attributable to built-in innovation. Below are features of Core Verify (IBM, n.d.):

- Single sign-on: Control access to cloud and on-premises applications from a specific location. This feature should reduce password fatigue.

- Identity analytics: Verify incorporates AI-powered identity analytics in the same SaaS environment as its access management features to enable predictive and autonomous risk mitigation.
- Advanced Authentication: Adds a security layer such as multi-factor authentication (MFA) or completely password-less access for faster access to data and applications.
- Adaptive access: Continuously uses machine learning to assess user risk for greater accuracy. Verify uses our AI-powered fraud engine to evaluate deeper risk context for adaptive access, leveraging IBM's rich heritage in the fraud detection business.
- Consent management: Verify goes beyond attributes to offer a centralized decision engine that templatizes detailed consent management purposes, EULAs, policies, and regulations all in one place. It enables privacy and risk officers to automate permission decisions to comply with privacy rules without touching code.
- Access recertification campaigns: Verify offers automated access recertification campaigns to reduce the number of human spreadsheet inspections and rubberstamp approvals. As firms emphasize compliance initiatives, these programs also help decrease human error.

Unsurprisingly, the IT industry is interested in learning more about IBM's current projects, particularly artificial intelligence. Since 1945, IBM has been a pioneer in computer and information technology. Artificial Intelligence is all the rage these days, and IBM is still a significant leader in the field.

Oracle Adaptive Access Manager (OAAM)

With context-sensitive online authentication and authorization, OAAM offers advanced layers of security. As a result, occurrences are analyzed, and pre-emptive actions are taken based on multiple data sources. OAAM is integrated with Oracle Access Management Suite Plus, which provides comprehensive access management solutions that are risk-aware and context-driven (Oracle, 2015). OAAM is a cutting-edge capability that enables organizations to prevent fraudulent activities and misappropriation by providing real-time or offline risk analysis, risk-based authentication, and end-user-facing functionality. It is popularly used by organizations in the United States and the computer software industry (Enyft, n.d.). Traditional authentication mechanisms are bolstered, making OAAM uniquely flexible and practical with authentication challenges based on risk assessment, simplified policy governance, and seamless integration across Oracle's Identity and Access Management Suite and third-party products (Oracle, 2015).

Oracle Adaptive Access Manager Features

Oracle Adaptive Access Manager helps secure sensitive internet processes like data access, financial transactions, and business functions. It allows IT teams to customize the machine learning models, which is a feature that appeals to larger organizations that have already been subjected to specific cyberattacks (Mixon, 2018). OAAM provides a security solution that is solid and structurally stable, concerning its outstanding usability and full integration with back-end identity management infrastructures. The significant authentication, fraud monitoring, and detection features are summarized below (Oracle, 2015).

- Knowledge-based Authentication: OAAM provides secondary authentication in knowledge-based authentication (KBA) questions as a standard. KBA verifies a user's identity based on known personal information and a real-time interactive question-and-answer procedure. The KBA infrastructure handles registration, answers, and question challenges. KBA is presented after successful primary authentication because it is a secondary authentication method.

- Virtual Authentication Devices: The virtual authentication devices are server-based, so they do not have any software or logic running locally on the user's device that could be hacked by keyloggers or other malware. OAAM's virtual authentication systems use customized images and expressions only known to the server and the end-user, making them effective in combating phishing attacks. OAAM can strengthen the security level irrespective of the type of authentication used. Strong authentication credentials alone may not prevent insider threats, credential theft, session hijacking, and other threats. Integrating authentication challenges based on risk assessment with the current authentication process can strengthen security while having a minor impact on the user experience.
- Autolearning: OAAM employs an innovative mix of a real-time, dynamic, and analytical auto-learning system to characterize user behavior and identify anomalies. It continuously understands each user by analyzing and learning real-time behaviors, utilizing feedback from fraud and compliance experts to detect and prevent fraudulent activities. By combining human expertise with machine learning, OAAM provides a solution to prevent fraud and misuse.
- Answer Logic: Answer Logic refers to a set of sophisticated pattern recognition algorithms the technology employs to intelligently detect accurate responses during the interactive authentication process. This feature enables the system to recognize correct responses containing minor typos, acronyms, or spelling errors, thus enhancing the usability of knowledge-based authentication questions. By incorporating answer logic, organizations can achieve a balance between security and usability, giving them more control over security measures.

- Mobile Access Security: OAAM uses the ASDK and RESTful web services to provide mobile security functionality directly and through the Oracle Access Management Mobile and Social Access Services component. Mobile Access Services enable organizations to expand their current access security solutions, including web and mobile access communications. In addition, its security policies can be modified when users access the system through a portable device. As a result, the analysis scope is broadened, and the precision of risk assessment is improved, lowering the number of false positives.
- Configurable Risk Engine: OAAM's risk evaluation system consists of three complementary methods that work in tandem to assess risk in real-time. The OAAM risk engine has a versatile architecture comprising customizable elements that allow administrators to create, edit and delete security policies and associated objects directly from the easy-to-use administration console, empowering business users to manage OAAM policies, access dashboards, and reports with little or no reliance on IT resources.
- Device Fingerprinting: OAAM utilizes device fingerprinting/identification among, other features, to evaluate the risk of a login session or authorization attempt. The system monitors and profiles various device characteristics and tracks device usage to identify potential risks. In addition, OAAM assigns a distinctive single-use cookie value to each user session that corresponds to a distinct device ID. The fingerprinting process may be repeated several times to detect changes in the middle of the session that may indicate session hijacking (Lee, 2015).
- OTP Anywhere: OAAM provides a customizable challenge processor framework that enables organizations to integrate other authentication solutions provided by external vendors or service providers with OAAM's real-time risk assessments to create tailored

risk-based solutions. One of the challenge mechanisms available is OTP Anywhere, which generates a single-use code from a server and sends it to the end-user via a secondary communication channel. SMS, email, and instant messaging are all supported as delivery channels for OTPs.

- Fraud Investigation Tools: Preventing fraud/misuse is fully automated with Oracle Adaptive Access Manager. OAAM's fraud investigation process involves analyzing high-risk situations that require human intelligence and non-automated communication to verify the occurrence of fraud and other related incidents. The OAAM Investigation interface is intended to streamline and improve the investigation process.

Other features include Universal Risk Snapshot, Policy Management, Dashboard, and reports. The OAAM comprises two parts: OAAM_ADMIN and OAAM_SERVER. The Oracle Adaptive Access Manager offers a wide range of implementation offerings to accommodate the unique requirements of virtually any deployment. Deployment options include:

- Single sign-on integration.
- Web services application integration.
- Reverse proxy option for universal installation.
- Built-in application integration.
- Java message service queue integration.

The deployment type is generally determined by the use cases demanded and the systems to be protected (Oracle, 2015). Organizations can cost-effectively protect end-users and themselves against fraudulent attacks and exploits, such as phishing, malware, transaction fraud, and insider threats.

Cisco Identity Services Engine (ISE)

The Cisco Identity Services Engine (ISE) is an innovative platform for identity and access control policy that helps organizations improve network security while implementing compliance and streamlining operations. Cisco ISE's distinct framework supports organizations in collecting real-time contextual data from networks, users, and systems (Cisco, 2017). ISE is a comprehensive solution for reducing operating costs and simplifying security policy management. Users and devices can be identified with ISE, and access can be controlled over wired, wireless VPN, and 5G mobile networks to the company's network (Cisco, 2022). Customers can use ISE to tether Network Access Control tasks to different clouds and ensure business stability in uncertainty. Cisco ISE is also a centralized access control system that consolidates features covered by existing Cisco policy platforms, operating on a policy-based model (Cisco, 2017). The Cisco Security Group Access Solution relies heavily on Cisco ISE. The ISE provides the following features to help manage the entire access network:

- The application integrates posture assessment, authentication, authorization, accounting (AAA), and profiling functionalities.
- ISE offers detailed guest access management for Cisco ISE administrators, authorized sponsor administrators, or both.
- Imposing endpoint compliance for all devices that connect to the network, including those 802.1X environments, by providing effective client provisioning metrics and reviewing device posture.
- Supporting the identification, segmentation, policy-based placement, and tracking of network-connected devices.

- Facilitating centralized and distributed deployments to have a consistent policy, enabling the effective provision of services.
- Using Advanced security measures such as Security Group Access (SGA), Security Group Access Control Lists (SGACLs), and Security Group Tags (SGTs).
- Enabling flexible deployment environments suitable for organizations of all sizes, from small offices to large enterprises.

By linking identity to different networking elements, such as wireless access point, network switches, VPN gateways, and data center switches, the administrator can make proactive governance judgments (Cisco, 2017).

Provide Identity-Based Network Access

The Cisco ISE solution offers context-aware identity management in the key areas below:

- It checks if users use an authorized, policy-compliant device to connect to the network.
- It creates user identity, location, and access history for compliance and audit purposes.
- It allocates services to users based on their role, group, and policy, considering factors such as job function, location, and device type.
- Cisco ISE uses authentication results to authorize users for specific network partitions, applications, services, or a combination.

Cisco AI Endpoint Analytics

Cisco's AI Endpoint Analytics is an innovative solution for device visibility that uses AI-powered analytics and network-based deep-packet inspection, as a method for identifying, verifying, and creating complete profiles for all devices connected to a network (Cisco, 2022).

The ISE is a software application that leverages traditional methods such as RADIUS, DHCP, SNMP, and others to receive device metadata from IT systems, enabling the detection of IT assets within an organization. By providing detection of IT assets, authenticating them, and regulating their network access, Cisco AI Endpoint Analytics overcomes the initial barrier many consumers encounter when implementing security practices: a lack of high-fidelity device visibility (Cisco, 2021).

The endpoint context in connected network infrastructure is critical for identifying IT and IoT devices. Endpoint Analytics leverages AI and ML methods to gather information from various network sources and organize and analyze it to create a comprehensive device profile and group similar devices together (Cisco, 2022). Enhanced visibility, spoof detection, threat evaluation, and threat containment are all advantages of endpoint analytics. In addition, it uses the following techniques to identify and reduce the number of unknown endpoints in the organization (Cisco, 2021):

1. **Deep packet inspection (DPI)** – assembles in-depth device context by inspecting and identifying IT applications and communication protocols, including devices used in automation and healthcare settings.
2. **Machine learning (ML)** – clusters devices based on similar characteristics and assists IT administrators in labeling them. These distinctive labels are then anonymously distributed to other organizations as recommendations for observing similar groups of unknown devices. This enables grouping of new devices based on similar attributes, which helps to reduce the number of unknown endpoints.

3. **Integration –** Cisco and third-party product integrations offer additional information about devices from the network and other sources to improve device profiling and context awareness.

Organizations are increasingly adding devices to their networks as they embark on digital transformation journeys. As per research, there is an anticipated significant increase in devices, including both user and IoT devices, in the future. The ISE solution integrates with third-party mobile device management (MDM) vendors, third-party data sources like Microsoft Active Directory, and device agents like Cisco AnyConnect® to provide additional information to enhance the endpoint context. For many years, this rich context has been used by ISE to profile endpoints on its own (Cisco, 2021). The system profiling rules currently included in ISE can be accessed by Cisco AI Endpoint Analytics along with this data.

CHAPTER 3: METHODOLOGY

This study focused on how artificial intelligence and machine learning revolutionize identity and access management systems and industry-based AI-integrated IAM solutions. A qualitative research method and a research design streamlined from a meta-analysis approach were employed in this study to present a succinct and detailed overview of findings from qualitative studies in the same research area, developing an in-depth analysis, gathering comprehensive data through various data collection methods, and answering the study's research questions.

Qualitative research methods often employ unstructured data collection techniques to thoroughly explore a subject and address questions related to the "how" and "why" of a particular phenomenon (Cleland, 2017). This approach is ideal for fully exploring a system's impacts and unexpected consequences (Kabir, 2016). A meta-analysis approach in qualitative research can extend beyond studies that solely address the research question. Instead, it may include all primary studies on the analyzed topic. The primary objective of conducting a qualitative meta-analysis is to expand the knowledge of the subject matter (Levitt, 2017; Timulak, 2009). This research design provided insights into AI-based identity and access management systems, features, approaches, and practical assessments that helped guide how AI solutions are employed and developed in the access management system. The purpose of this study was to address the effectiveness of AI-based access management system solutions; this chapter outlines the research methodology, including the approach, research design, and data analysis, used to address the following research questions:

Research Questions

Research question 1:

How can the capability and effectiveness of the authorization-based user access evaluation process be improved using artificial intelligence techniques?

Research question 2:

How do IAM and artificial intelligence work together to automate critical identity management and user authentication processes?

Research question 3:

How can analytical intelligence reduce information security risks, improve control of privileged activities, boost productivity, and significantly reduce financial losses?

Research Design

In contrast to quantitative meta-analysis, which aims to obtain detailed evaluations of outcome variables, the rationale and objective of a qualitative meta-analysis are similar. However, they involve analyzing a study area beyond a specific study. Qualitative meta-analysis aims to conduct an extensive analysis and synthesis of qualitative data gathered from primary sources (Levitt, 2017; Timulak, 2009). Therefore, the qualitative method was used in this study because can be customized to incorporate a meta-analytical framework utilizing primary findings instead of unprocessed data. Meta-analysis is an overview of a research subject or field, much like a narrative review. However, a meta-analysis adds further value by offering a quantitative evaluation of the correlation between two target variables or the efficacy of a process, going beyond a narrative description of the main findings (Gurevitch et al., 2018; Hansen et al., 2022). Authors such as (Kaplan et al., 2021; Mehta, et al., 2022) used a meta-analytic research approach based on artificial intelligence studies to examine relationships, determine various relevant factors, or understand the concept of AI in various areas.

Researchers can use qualitative meta-analytic methods to combine and summarize findings from primary sources of qualitative data (Levitt, 2017). The objectives of a qualitative meta-analysis are twofold: (a) to offer a thorough depiction of a research problem across a group of studies, including its inconsistencies and variations discovered in primary studies, and (b) to assess the influence of the research methodology on the findings (Timulak, 2009). After considering the growing need for access management in the AI era and the importance of these evolving concepts, a meta-analysis research design was adopted. In this study, the qualitative meta-analytic methodology explored the experiences of industries incorporating AI into their IAM systems and the impact of AI on access management systems. Qualitative research was utilized because AI is a recent development, and qualitative research enables a more in-depth examination of underlying theories and concepts that may no longer be applicable in the AI era and a better understanding of the relationship between artificial intelligence and access management systems (Yang & Siau, 2018). Furthermore, this research design methodology builds confidence in research findings and their transferability by analyzing data objectively rather than relying solely on the subjective interpretation of researchers (Ntinda, 2018; Umurerwa & Lesjak, 2021).

This study's design used these research areas (RA) to support each research question's solution. Therefore, the following research areas are represented in the document and data analysis:

RA1 for research question 1: Research presented in the literature review regarding IAM components, and its model layers and AI/ML transforming IAM identifies how AI techniques can improve the capability and effectiveness of the authorization-based user access levels.

RA2 for research question 2: Research presented in the introduction and literature review regarding the benefits of AI-based access management systems, AI approach to IAM, and AI Identity/Access solutions applied in industries identifies how IAM and AI work together to automate critical identity management and user authentication processes.

RA3 for research question 3: Research presented in the literature review and research findings on intelligent systems, security analytics, industry-based AI systems, and Artificial Intelligence Approach to IAM identifies and establishes that an ability to evaluate information and solve problems accurately will reduce information security risks, improve control of privileged activities, boost productivity, and significantly reduce financial losses.

Data Collection Method

Qualitative data collection methods are crucial in impact assessment because they provide information that can be used to recognize the procedures leading to observed research results (Cleland, 2017). Also, qualitative methods can enhance the accuracy of quantitative evaluations based on surveys by assisting in creating evaluation hypotheses, improving the design of survey questionnaires, and defining quantitative evaluation findings (Kabir, 2016; Noyes, et al., 2019). In a qualitative meta-analysis, the various components of the same study can be published in multiple studies; consequently, caution is required to prevent some findings from being overestimated by their appearance in other reports, even though they are based on the same experiential data (Timulak, 2009). As a result, the meta-analysis search approach should be methodical, consistent, and transparent, producing a sample that covers all relevant studies (Gusenbauer & Haddaway, 2020).

This study used its research questions and searched terms using Boolean operators. Table 1 lists the research topics, the keyword combinations used to frame them, and their importance.

Table 1

A list of the keywords employed for this research.

Research Question	Keywords Combination	Relevance
1. How can the capability and effectiveness of authorization-based user access control be improved using artificial intelligence techniques?	((“effective”) AND (“user authorization” OR “access control”) AND (“artificial intelligence” OR “AI techniques”)) (“access control” OR “user authorization”) AND (“artificial intelligence”)	The research question aims to support the need for a more adaptive, intelligent, and dynamic access control policy.
2. How do IAM and artificial intelligence work together to automate critical identity management and user authentication processes?	((“access management”) AND (“artificial intelligence”) AND ("identity management" OR "IdM" OR "user authentication")) (“access management” OR "identity management") AND (“artificial intelligence”)	The need for automated identity management and user authentication processes in IAM is identified.
3. How can analytical intelligence reduce information security risks, improve control of privileged activities, boost productivity, and significantly reduce financial losses	((“Information security”) AND (“privilege risk” OR “productivity risk” OR "financial risk") AND (“analytical intelligence” OR “analytics”)) (“security analytics”) AND (“intelligence”)	The need for emerging technologies such as analytical intelligence to combat rising information security risks such as privilege access, productivity loss, and financial loss is identified.

Note. The string keywords are created by selecting relevant terms from the research question. Queries are written using keywords, also known as search strings, to find answers to research questions. In addition, simple queries are provided to extract related articles in some databases where a keyword combination does not yield a list of articles.

A keyword search in electronic databases is the most used and essential strategy (Hansen et al., 2022; Harari et al., 2020). This strategy produced the most significant number of relevant studies. Multiple databases were used to avoid biased results due to a single database's scope or journal coverage. After determining the research questions and keyword combinations, the ECU Joyner Library, IEEE Xplore, Google Scholar, ACM Digital Library, Research Gate academic journals, and Science Direct were combed through to gather enough resources for this study. This resulted in more available materials, such as articles on Identity management and AI and top journals in the field. As some articles had limitations on full content downloading, this study also relied on Open Access articles and articles accessible to the researcher through Institutional Sign-in as an East Carolina University student. Relevant webinars on artificial intelligence and identity management published by reputable industries were also considered for this thesis to better understand the underlying concepts.

One industry sector that has been quick to adopt an intelligent IAM system is the internet technology (IT) sector. Although it is not widely used, due to the ever-increasing cyber-attack space, it is gradually becoming a popular and effective solution in access management systems. While collecting data in this sector, the concept of marketecture (or marchitecture, ‘marketing + architecture’) was established to avoid gathering data relating to an organization's vision or marketing spin and instead focus on the existing status of the system and its architectural representation. Researching the IT sector provided data on AI Identity/Access solutions applied in industries to generate relevant concepts from data. The most current developments in AI were reviewed by considering relevant literature in the English language over the last seven years (2017-2023), as well as a few older works, to define terminology, clarify concepts, and establish definitions and differences. Additionally, since AI has many applications in many fields and areas, articles from different sectors were also considered to find the materials most relevant to the research questions.

Data Analysis

During the literature review, the researcher focused on peer-reviewed articles that established the components of how AI and ML revolutionize identity and access management systems. A fundamental topic description was created, with headings describing the emerging vital findings. The data analysis includes the concepts that emerged in response to the study questions and how those concepts relate to the research and theoretical frameworks. In a qualitative meta-analysis, the descriptive interpretative approach of analysis follows the steps below:

1. Domains are assigned to the collected data.
2. Meaning units are defined.
3. Concepts are generated by comparing meaning units and clarifying the core of similar meaning units. The meaning units within the data define the concepts, which can be further categorized or classified based on comparisons and disparities.
4. The main findings are summarized, often using visual aids or storytelling.

Additionally, the study employs several precautionary measures, such as reliability assessments, to guarantee its authenticity (e.g., cross-validation and external validation). This qualitative analysis feature offers detailed information about contextual circumstances or provides insight into the reasons for occurrences typically not addressed by quantitative research. The analysis is used to learn how research participants (in this case, companies using AI-based solutions) integrate AI features into their IAM system and the benefits and drawbacks of it.

During data analysis, articles of low quality were ignored from the summary. In this analysis, a quantitative study was considered of low quality if it did not adequately describe the features of its methodological design. Qualitative studies that failed to provide a comprehensive account of the learning context and outcomes or showed signs of bias rather than being based on observations were disregarded.

Ethical Considerations

Making an argument for a study requires writing about these anticipated ethical concerns, which is a crucial subject in the structure of proposals (Creswell, 2014). Artificial intelligence in access management systems raises ethical concerns about privacy and data security. This research addressed these concerns to ensure ethical practices were not violated and eliminate potential biases. The contemporary issues associated with disclosure of personal information, credibility, and validity of research articles, the function of researchers in multicultural environments, and the potential infringement of individual privacy due to internet data collection all pose ethical dilemmas (Creswell, 2014). Data collection demands a significant period when conducting a qualitative study, regardless of the data type. As appropriate, the researcher must thoroughly, accurately, and systematically document any possibly valuable information using various tools, including field notes, sketches, audio recordings, and others. The data collection techniques utilized must conform to ethical research standards (Kabir, 2016). Researchers must protect against misconduct and improper behavior that could negatively affect their companies or institutions, promote research integrity, and manage new, difficult situations (Creswell, 2014).

Numerous ethical factors must be considered and mirrored in the research process. It is beneficial to discuss them concerning the many stages of inquiry; ethical considerations should be given before performing a study, initiating a study, throughout data collection, data analysis, and data reporting, sharing, and storage (Creswell, 2014). These concerns apply to all phases of research, including qualitative, quantitative, and mixed research methods.

The Economic and Social Research Council (ESRC) has established a framework for research ethics, which outlines the guidelines and prospects for researchers, research network, and research ethics committees. The framework includes six principles for good research practices, three relevant to this study, namely:

- Research goal should be to reduce risk and maximize benefits for society and individuals.
    - The goal of this research is to reduce cybersecurity risks; the results of this study should show how using artificial intelligence to improve identity and access management can help to reduce the growing threat from cyberspace.
- Research must be carried out with integrity and transparency.
    - Utilizing information from reliable sources and verifying it with sources of a similar nature, the data's transparency and integrity were confirmed.
- Research should remain independent, and conflicts of interest should be disclosed when they cannot be avoided.
    - This research was carried out independently and without potential or actual conflicts of interest.

Limitations of the Research

The study has some limitations ha should be considered. Firstly, the data used is based on peer-reviewed articles, as well as industry solutions published by credible organizations that use AI-based solutions, with no data from actual use cases in any industry. This could be due to organizations being reluctant to share too much information about their AI implementations and implementation challenges. As a result, information gathering through interviews was ruled out. In addition, it is essential to note that there is currently no universally accepted standard approach for implementing AI-based access management systems. The efficacy of such systems can vary depending on the industry, organizational structure, or specific context in which they are implemented. Therefore, it can be challenging to compare different systems' effectiveness and generalizability to other settings.

This study was primarily a high-level overview of an AI-based system with highlighted features, benefits, and limitations, with no in-depth evaluation of AI tools and their implementation. Future studies will benefit from including actual use cases and challenges of implementing an AI-based access management system.

CHAPTER 4: FINDINGS

This qualitative meta-analysis aimed to demonstrate how artificial intelligence improves identity and access management amid increasing cyber threats and technological advancements. The research design of this study reviewed the experiences of different industries that have integrated AI into their IAM systems. Specifically, the study sought to understand the overall effect of AI on IAM systems, the changes AI brings to the IAM system and the solutions that intelligent-based IAM provides to keep up with technological advancements. This chapter presents information gathered from multiple peer-reviewed articles, reliable and credible websites that demonstrate expertise, and relevant webinars on artificial intelligence and identity management published by reputable industries to represent the importance, effectiveness, and limitations of an AI-based access management system. The study was guided by and intended to address the following research questions:

Research question 1:

How can the capability and effectiveness of the authorization-based user access evaluation process be improved using artificial intelligence techniques?

Research question 2:

How do IAM and artificial intelligence work together to automate critical identity management and user authentication processes?

Research question 3:

How can analytical intelligence reduce information security risks, improve control of privileged activities, boost productivity, and significantly reduce financial losses?

This chapter presents findings on the research questions, general AI solutions, their economic benefits, and conclusions from the conducted research based on features of an AI-based access management system. The research questions highlighted are proposed with solution ideas, summary limitations of the AI approach, limitations of the study, and economic benefits. This meta-analysis is structured around the research questions. Based on the research questions, the results and discussion are outlined below.

Research Questions Findings

Research Question 1: How can the capability and effectiveness of the authorization-based user access evaluation process be improved using artificial intelligence techniques? The shortcomings of a traditional authorization-based access control system do not allow for fine-grained management of user permissions. In addition, it does not recognize security-related features such as user characteristics, resources, and operations (Yao et al., 2021).

As technology advances, there is a need for a new access control architecture that is based on flexible data structures to identify connections and patterns and uses knowledge to form policies that govern access. This flexible and intelligent approach is necessary to address the challenges and opportunities of the modern world. Such approaches include predictive modeling, behavioral analysis, access control automation, natural language processing, and risk-based access control.

Alfheim (2022) proposed a knowledge-based access control (KBAC) type of advanced authorization based on knowledge. It probes the constantly changing context to provide granular, dynamic authorization. Yao et al. introduced an innovative access control and authorization approach based on the zero-trust security architecture. Their Trust-Based Access Control (TBAC) model generates user portraits using user behavior, enabling real-time hierarchical control in various scenarios to achieve evolving and precise access control and authorization (Yao et al., 2021). The authorization status is modified dynamically by assessing user trust and permission trust thresholds.

In conjunction with authorization-based user access evaluation, AI solutions are recommended to improve accuracy and efficiency of access management, enhance organization security posture, and improve the capability and effectiveness of authorization-based user access control. By introducing a flexible, intelligent, and more secure system with better user experience and insights to ensure productivity and value for the industry and user.

Research Question 2: How do IAM and artificial intelligence work together to automate critical identity management and user authentication processes? Authentication is integral to identity management; only after users have been adequately 'identified' and 'authenticated' can they be granted access to systems or privileges. However, traditional authentication methods such as passwords or fingerprints are known to be prone to subversion. To address this issue, artificial intelligence can be leveraged to improve authentication by providing adaptive retraining for detection models (Qiu et al., 2019). Various methods, such as user behavior analysis, continuous authentication, identity verification, risk-based access control, and password management, can be used to accomplish this. It can enhance authentication methods using a deep neural network, which can handle multidimensional data phases or a simple learning model (Zhu & Al-Qaraghuli, 2022). Various AI technologies have been increasingly integrated into authentication to obtain a broader and higher accuracy. Artificial intelligence algorithms can be used to design intelligent authentication provisioning by leveraging channel reciprocity, communication link characteristics, and device features. Studies have proposed many advanced functionalities for authenticating users (Shah & Kanhere, 2019).

Chauhan et al. proposed using a user's breathing sound for authentication. This technology can be activated by the user breathing (a deep inhale and a sniff) while holding the phone close to their nose (Chauhan, et al., 2017). Authors in (Where Have You Been? Using

Location-Based Security Questions for Fallback Authentication, 2015) proposed an alternative approach that generates location-based authentication questions by relying on episodic memories in a spatiotemporal context. Fridman, Weber, Greenstadt, and Kam (2017) demonstrated how location data, app usage, typing patterns, and online sessions might all be used to provide active authentication. Qiu et al. (2019) proposed a security authentication scheme based on artificial intelligence for wireless multimedia networks, concluding that it ensures communication privacy and facilitates efficient and streamlined authentication for multiple multimedia devices. It is also stated that the AI-assisted Lightweight Physical Layer Authentication (LPLA) technique can enhance authentication precision while resolving the communication latency issue in wireless multimedia network applications (Qiu et al., 2019). The most suitable technique for user identification in innovative spaces is behavioral biometrics because it is non-intrusive and typically requires no explicit consent from the user (Shah & Kanhere, 2019).

Traditional authentication systems have significant drawbacks, such as inconsistency in low computational costs and high security. Consequently, AI has been increasingly integrated into traditional authentication processes to enhance security and user experience (Zhu & Al-Qaraghuli, 2022). AI-assisted authentication integrates artificial intelligence and traditional identity authentication methods such as password authentication. As a result, cutting-edge technology based on AI-assisted lightweight authentication is instrumental in meeting the requirements of today's authentication systems while also providing overall environment security.

Research Question 3: How can analytical intelligence reduce information security risks, improve control of privileged activities, boost productivity, and significantly reduce financial losses? Information security risks are growing, which has expanded the technological requirements to mitigate the risks. For any corporation that is dependent on IT to thrive, effective information security risk management is imperative (Hosam, 2022). Automated and real-time analysis is essential in detecting and preventing cyberattacks in conventional information security systems (Trellix, n.d.). Analytical intelligence provides the information required to make informed choices, it provides access control, predictive analysis, threat detection and response, incident response automation, and privileged activity monitoring. Security analytics involves using software, algorithms, and analytical processes to detect and prevent potential cyberattacks by analyzing data from multiple sources and looking for anomalies and similarities. According to Microsoft, predictive analytics and data interpretation systems are the most used AI-driven technologies in the financial services sector, accounting for 52% of their adoption (Microsoft News Center UK, 2019).

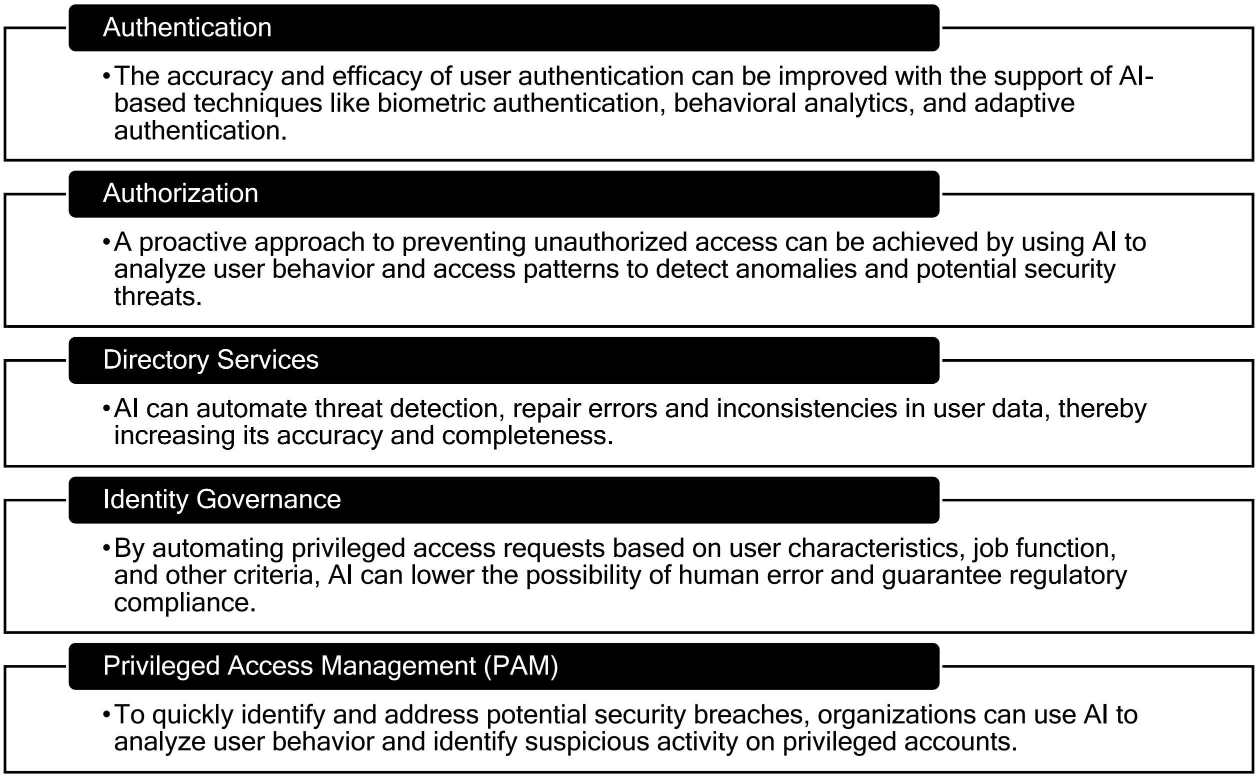
As proposed by Davenport, “Analytics 4.0: the era of artificial intelligence” is the next level of analytical expertise for enterprises in the age of AI or cognitive technology (Davenport, 2018). Hosam proposed using a Genetic algorithm (GA) as an external tool to aid risk analysts in identifying the most effective criteria to mitigate risk (Hosam, 2022). The intelligence of GA aids in risk assessments, resulting in high precision in risk assessment and thus increasing organizations' ability to mitigate unexpected events. Nezamoddini et al. suggested a framework for risk-based supply chain optimization. To lower risk, the algorithm utilizes GA and artificial neural networks (Nezamoddini et al., 2020).

Analytics combined with artificial intelligence provides concentrated insights enabling technical and non-technical employees to work longer while maintaining productivity. Companies can make more feasible decisions by using AI-based analytical models that collect and analyze large amounts of information from customers and products (Ellen MacArthur

Foundation, 2019; Ghoreishi & Happonen, 2020). It also helps bridge the talent gap and streamline business operations by automating tasks, increasing productivity, reducing expenses, and improving outcomes. In addition, it is crucial to use analytical intelligence to monitor and manage the risks associated with information security since it brings risks under control in any corporate setting providing rapid detection, response, and compliance. As a result, control over privileged activities will improve, productivity will increase, and financial losses will be significantly reduced. Figure 3 and Table 2 illustrate the potential applications of AI in identity and access management (IAM) components and the various AI-based solutions that can enhance IAM functions.

Figure 3

AI integrated into IAM components.



Authentication

- The accuracy and efficacy of user authentication can be improved with the support of AI-based techniques like biometric authentication, behavioral analytics, and adaptive authentication.

Authorization

- A proactive approach to preventing unauthorized access can be achieved by using AI to analyze user behavior and access patterns to detect anomalies and potential security threats.

Directory Services

- AI can automate threat detection, repair errors and inconsistencies in user data, thereby increasing its accuracy and completeness.

Identity Governance

- By automating privileged access requests based on user characteristics, job function, and other criteria, AI can lower the possibility of human error and guarantee regulatory compliance.

Privileged Access Management (PAM)

- To quickly identify and address potential security breaches, organizations can use AI to analyze user behavior and identify suspicious activity on privileged accounts.

Table 2

AI Solutions in IAM

	AI Solutions in IAM
1	Increased Visibility – artificial intelligence monitoring
2	Fine-grained access control – insightful identity intelligence, access modeling, access insights, access recommendation
3	Breach Detection and Prevention – privileged behavior analytics, user and entity behavior analytics (UEBA)
4	Intelligent Adaptive Authentication – risk-based authentication, continuous authentication, password-less authentication
5	Automation and Flexibility – automated and adaptable processes
6	Going beyond Compliance – increased effectiveness in ensuring compliance

Note. Applying AI solutions in Identity and Access Management (IAM) can improve security and user experience while mitigating the risk of security breaches.

Economic Benefits

Apart from gradually improving our daily lives, AI's integration has resulted in numerous benefits across multiple industries. Many research areas, such as healthcare, pattern recognition issues, big data, transportation, and many more, have significantly benefited from the incorporation of artificial intelligence (Alomari, et al., 2021). Its processes are more effective and efficient, technology is more widely available, and projections are more precise. Integrating AI into IAM can positively impact the economy by creating more job opportunities.

With automation, organizations can benefit from increased productivity and higher production levels. According to PWC research, AI technology could generate $15.7 trillion in revenue by 2030. Increasing the GDP of regional economies by 26% and the global GDP by 14% (PricewaterhouseCoopers, 2017). Automation in business operations will have an impact on AI's economic impact as it increases productivity, as will productivity gains from organizations that use AI technologies to augment their current workforce (PricewaterhouseCoopers, 2022). The report also predicts that by 2030, 45% of the total economic gains from AI integration will come from product improvements, leading to increased market demand. AI will enable a greater range of products, customization, desirability, and availability, driving this growth over time (PricewaterhouseCoopers, 2022). Furthermore, automation and Artificial Intelligence (AI) advancements in identity and access management can contribute to unprecedented economic benefits (Mohammed I. A., 2018).

With decision-making, it provides forecasts to help organizations make the most informed choices and increase business efficiency. It also aids in the resolution of complex problems by identifying the most appropriate solutions—reduced expenses and increased productivity result from improved problem-solving efficiency. Research by Accenture suggests that AI has the potential to provide an average increase of 38% in profitability rates by 2035, resulting in a $14 trillion economic boost across 16 industries in 12 economies (Purdy & Daugherty, 2017). In cloud computing solutions, IAM is crucial because such services often involve third-party data handling, meaning data handling and access must be strictly outlined and controlled. Furthermore, the integration of artificial intelligence in the future IAM systems will appropriately identify users, evaluate the user's behavior, and automatically send alerts when anomalies are identified (Mohammed I. A., 2021). This will significantly benefit organizations' security architecture by consolidating resources and reducing costs.

Possible Challenges of an AI-Based Access Management System

Future market leaders will be AI-enabled systems with strict security profiles and access control. However, there have been numerous instances where AI-enabled systems have made incorrect decisions. The widespread application of artificial intelligence raises several ethical and legal concerns that must be addressed. AI-related ethical issues fall into two categories (Khisamova et al., 2019):

1. Digital data collection, analysis, and processing issues
2. Issues with AI decision-making based on generic data.

In AI adoption, cybersecurity defense will become even more permeable if AI applications are only partially adopted, giving hackers a tactical edge since they can heavily rely on AI to introduce new attacks. However, it is far from sufficient to rely just on AI tools without any human interference and achieve effective use of intelligence. Regulations are necessary to ensure ethical behavior, protect human rights, and establish legal accountability for those involved in AI development and deployment (Taddeo, 2019). AI frequently needs scalable computationally intensive hardware architectures, such as graphics processing units (GPUs). Although internal development of these skills might be prohibitively expensive, they can be accessed through the cloud for comparatively less money (Davenport, 2018). In the AI decision-making process, a lack of transparency exists because there is no real explanation for why the AI model generates the final decision results. Although AI models can achieve high accuracy, it is still being determined how accurate their results will be when challenged with unexpected events (Zhang, et al., 2021). Objections to the AI model's decision-making results hinder its adoption as people are skeptical of the decision-making results. Also, many AI models require vast amounts of high-quality data. Enterprise data must be well-organized and easily accessible (Davenport, 2018). Therefore, addressing any lingering problems with corporate data (such as quality, consistency, availability, etc.) is crucial.

Technological research organizations provide recommendations to security experts to stay competitive with emerging business opportunities while offering customers the reliable and seamless user experiences they demand (Forgerock, 2020). Gartner's Continuous Adaptive Risk & Trust Assessment (CARTA) security model recommends that organizations implement an access management approach that encourages ongoing monitoring and evaluation of security choices based on multiple attributes and uses the most comprehensive and most profound insights available to evaluate the risks of user interactions with their electronic communication channels (Forgerock, 2020; Gartner, 2019). According to the Zero Trust model developed by Forrester, there is no intrinsic difference between trusted and untrusted elements, such as devices, data, networks, sessions, users, or services. Before establishing trust, various contextual, behavioral, and risk-based signals must be considered. Even if one or two-factor authentications are advanced, more is needed. As a result, it becomes crucial to consider additional factors such as setting, behavior, and risk to enable adaptive authentication (Holmes & Burn, 2022).

The first step in achieving AI success is having a fundamental idea of what AI is, how it will influence the system, its functionalities, and what a practical strategic plan should be (Davenport, 2018). Organizations considering adopting an AI-based access management system should conduct an in-depth assessment of their current access management system and identify specific use cases for the AI-based system. Organizations that utilize their current system capabilities will likely get started with AI considerably faster and more successfully. However, most organizations need more internal capabilities to thrive with AI. Corporations such as IBM, Microsoft Azure, Cisco, Oracle, SailPoint, ForgeRock, Okta, Saviynt, and so on employ AI-based techniques in their identity and access management operations. They also offer their services and solutions to modern enterprises to tackle the issue of securing resource access without risking development or productivity and adapt to organizational changes, ensuring that every user has the access they require when they require it.

CHAPTER 5: CONCLUSION

Organizations may save time and money by implementing AI solutions while being more prepared for future threats. AI adoption has proven very significant with the increased complexity of cyber threats. AI-based machine learning solutions ease users' authentication complexity, which helps balance user convenience with security considerations. By implementing operational identity management and access controls based on detailed individual-specific regulations, a high level of security can be maintained without burdening users or IT employees. The primary objective of an AI-based access management system is to transition from reactive access management to a preventative or corrective access management system, ensuring that organizations remain secure and updated with security features. The successful implementation of this AI solution requires serious analysis of the ethical and legal consequences and the potential limitations and challenges associated with artificial intelligence. Organizations should emphasize the evolution of accountable and transparent AI algorithms, and the formation of clear guidelines and policies for AI governance and monitoring, to entirely appreciate the benefits of AI-based access management systems.

The findings of this research, which is a pioneering effort to understand the impact of artificial intelligence in identity and access management, inform IT professionals, academics, and relevant parties about the effectiveness of an AI-driven access management system in mitigating growing cyber threats and staying up to date with technological advancements. Although making precise and comprehensive predictions for the distant future is difficult, technology is expected to continue transforming our lives in the years ahead, necessitating a fresh approach to identity and access management. More research is required to examine the prospects of AI-based access management systems in different industries and environments and address the limitations and challenges of the AI solution.

REFERENCES

Alfheim, P. (2022, July 20). *The next generation of authorization*. Retrieved from Indy Kite: https://www.indykite.com/blogs/the-next-generation-of-authorization

Alomari, M. K., Khan, H. U., Khan, S., Al-Maadid, A. A., Abu-Shawish, Z. K., & Hammami, a. H. (2021). Systematic Analysis of Artificial Intelligence-Based Platforms for Identifying Governance and Access Control. *Security and Communication Networks*, 1-10.

Berlatsky, N. (2011). *Artificial intelligence.* Detroit: Greenhaven Press.

Bibi, K., Naz, S., & Rehman, A. (2018). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. *Multimedia Tools and Applications*, 289–340.

Bosri, R., Rahman, M. S., Bhuiyan, M. Z., & Omar, A. A. (2021). Integrating Blockchain With Artificial Intelligence for Privacy-Preserving Recommender Systems. *IEEE Transactions on Network Science and Engineering, 8*, 1009-1018.

Carnley, P. R., & Kettani, H. (2019). Identity and Access Management for the Internet of Things. *International Journal of Future Computer and Communication*, 129-133.

Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., & Lee, Y. (2017). BreathPrint: Breathing Acoustics-based User Authentication. *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services* (pp. 278–291). Association for Computing Machinery.

Cisco. (2017). Overview of Cisco ISE. In *Cisco Identity Services Engine User Guide, Release 1.0 OL-22974-01* (pp. 1.1 - 1.4). Retrieved from https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.pdf

Cisco. (2021, February 09). *Cisco AI Endpoint Analytics: A New Path Forward White Paper*. Retrieved June 17, 2022, from Cisco.com: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html

Cisco. (2022, May 24). *Cisco Identity Services Engine Data Sheet*. Retrieved June 16, 2022, from Cisco: https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html?ccid=cc001033&dtid=odicdc000016&oid=dstsc025999

Cisco. (2022, February 16). *What Is Endpoint Analytics?* Retrieved June 21, 2022, from Cisco.com: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-endpoint-analytics.html

Cleland, J. A. (2017). The qualitative orientation in medical education research. *Korean Journal of Medical Education*, 61-71.

Creswell, J. W. (2014). *Research design : qualitative, quantitative, and mixed methods approaches 4th edition.* SAGE Publications, Inc.

CSA. (2009, December). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* Retrieved from Cloud Security Alliance: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

Damon, F. (2019). *A framework for identity and access assurance, Doctoral Thesis.* Johannesburg: Creative Commons.

Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine learning in cybersecurity: a comprehensive survey. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 1-50.

Davenport, T. H. (2018). From analytics to artificial intelligence. *Journal of Business Analytics, 1*, 73-80.

Dhamdhere, M., & Karande, S. (2015). Identity and access management: concept, challenges, solutions. *International Journal of Latest Trends in Engineering and Technology*, 300-308.

Dignum, V. (2021). The role and challenges of education for responsible AI. *London Review of Education, 19*(1), 1-11. doi:10.14324/LRE.19.1.01

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications*, 21 - 39.

Ding, Y., Tan, F., Qin, Z., & Cao, M. (2021). DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. *IEEE Transactions on Neural Networks and Learning Systems, 99*, 1-15.

Economic and Social Research Council. (2021, August 17). *Framework for research ethics - core principles*. Retrieved from UKRI- UK Research and Innovation: https://www.ukri.org/councils/esrc/guidance-for-applicants/research-ethics-guidance/framework-for-research-ethics/our-core-principles/#contents-list

Ellen MacArthur Foundation. (2019). *Artificial intelligence and the circular economy - AI as a tool to accelerate the transition*. Retrieved from ellenmacarthurfoundation.org: https://ellenmacarthurfoundation.org/publications

Engström, P. (2019). *Exploring the non-technical challenges: A case study of identity and access management projects (Master of Science Thesis).*

Enyft. (n.d.). *Oracle Adaptive Access Manager commands 0.11% market share in Identity & Access Management*. Retrieved 06 03, 2022, from Enyft.com: https://enlyft.com/tech/products/oracle-adaptive-access-manager

Faruk, M. J., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., . . . Wu, F. (2021). Malware Detection and Prevention using Artificial Intelligence Techniques. *2021 IEEE International Conference on Big Data (Big Data)* (pp. 5369-5377). IEEE.

Forgerock. (2020). *Introducing ForgeRock Intelligent Access.* Retrieved from Forgerock.com: https://www.forgerock.com/resources/whitepaper/introduction-forgerock-intelligent-access

Frankish, K., & Ramsey, W. (2014). *The Cambridge handbook of artificial intelligence.* London: Cambridge University Press.

Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2017). Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. *IEEE Systems Journal, 11*, 513-521.

Gartner. (2017). *Applying Artificial Intelligence to Drive Business Transformation: A Gartner Trend Insight Report.*

Gartner. (2019, June 12). *The Gartner IT Security Approach for the Digital Age*. Retrieved from Gartner.com: https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age

Ghazizadeh, E., & Cusack, B. (2019). Defining Cloud Identity Security and Privacy Issues: A Delphi Method. *Twenty-fifth Americas Conference on Information Systems (AMCIS) 2019 Proceedings.* Cancún, México.

Ghoreishi, M., & Happonen, A. (2020). New promises AI brings into circular economy accelerated product design: a review on supporting literature. *7th International Conference on Environment Pollution and Prevention (ICEPP 2019). 158*, pp. 1-10. E3S Web of Conferences.

Guo, K., Ren, S., Bhuiyan, M. Z., Li, T., Liu, D., Liang, Z., & Chen, X. (2020). MDMaaS: Medical-Assisted Diagnosis Model as a Service With Artificial Intelligence and Trust. *IEEE Transactions on Industrial Informatics, 16*, 2102-2114.

Gurevitch, J., Koricheva, J., Nakagawa, S., & Stewart, G. (2018). Meta-analysis and the science of research synthesis. *Nature, 555*, 175–182.

Gusenbauer, M., & Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Res Synth Methods* , 181-217.

Hang, A., Luca, A. D., Richter, M., Smith, M., & Hussmann, H. (2015). Where Have You Been? Using Location-Based Security Questions for Fallback Authentication. *Conference: To appear in Proceedings for the Symposium on Usable Privacy and Security (SOUPS'2015)* (pp. 169–183). Ottaw, Canada: USENIX Association.

Hansen, C., Steinmetz, H., & Block, J. (2022). How to conduct a meta-analysis in eight steps: a practical guide. *Management Review Quarterly, 72*, 1–19.

Harari, M. B., Parola, H. R., Hartwell, C. J., & Riegelman, A. (2020). Literature searches in systematic reviews and meta-analyses: A review, evaluation, and recommendations. *Journal of Vocational Behavior, 118*.

Harvard University. (2014). *Harvard University - Identity and Access Management Program Plan.* Harvard University Information Technology.

Harvard University Information Technology (HUIT). (2022). *About Identity & Access Management*. Retrieved from Identity & Access Management: https://iam.harvard.edu/overview

Holmes, D., & Burn, J. (2022, January 24). *The Definition Of Modern Zero Trust*. Retrieved from Forrester.com: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

Hosam, O. (2022). Intelligent Risk Management using Artificial Intelligence. *2022 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 1-9). UAE: IEEE.

Hummer, M., Kunz, M., Netter, M., Fuchs, L., & Pernul, G. (2016). Adaptive identity and access management—contextual data based policies. *EURASIP Journal on Information Security*, 1-16.

IBM. (2019, December 10). *IBM AI Innovations Sharpen Risk Detection in Identity Management*. Retrieved April 18, 2022, from Newsroom IBM: https://newsroom.ibm.com/2019-12-10-IBM-AI-Innovations-Sharpen-Risk-Detection-in-Identity-Management

IBM. (n.d.). *IBM Security Verify*. Retrieved April 18, 2022, from IBM: https://www.ibm.com/verify/verify-identity

IBM. (n.d.). *OKTA - IDaaS | IBM*. Retrieved April 18, 2022, from IBM.com: https://www.ibm.com/security/identity-access-management/ibm-okta-idaas/

Identity Management Institute. (2021, April 22). *Artificial Intelligence and Machine Learning are Transforming IAM*. Retrieved April 13, 2022, from Identity Management Institute®:

https://identitymanagementinstitute.org/artificial-intelligence-and-machine-learning-are-transforming-iam/

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, 574 - 588.

Jiang, C., Zhang, H., Ren, Y., Han, Z., Chen, K.-C., & Hanzo, L. (2017, April). Machine Learning Paradigms for Next-Generation Wireless Networks. *IEEE Wireless Communications, 24*, 98-105.

Kabir, S. M. (2016). Methods of Data Collection. In *Basic Guidelines for Research: An Introductory Approach for All Disciplines* (pp. 201-275). Bangladesh: Book Zone Publication.

Kaplan, A. D., Kessler, T. T., Brill, J. C., & Hancock, P. (2021). Trust in Artificial Intelligence: Met-Analytic Findings . *Human Factors: The Journal of the Human Factors and Ergonomics Society*.

Khansa, L., & Liginlal, D. (2012). Regulatory Influence and the Imperative of Innovation in Identity and Access Management. *Information Resources Management Journal*, 78-97.

Khansa, L., & Liginlal, D. (2012). Whither information security? Examining the complementarities and substitutive effects among IT and information security firms. *International Journal of Information Management*, 271-281.

Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). rtificial Intelligence and Problems of Ensuring Cyber Security. *International Journal of Cyber Criminology, 13*(2), 564–577.

Korolov, M. (2022, February 4). *Top Three Use Cases for AI in Cybersecurity*. Retrieved April 6, 2022, from Data Center Knowledge: https://www.datacenterknowledge.com/security/top-three-use-cases-ai-cybersecurity

Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. *Artificial Intelligence Review*, 369–387.

Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2018). Attribute Quality Management for Dynamic Identity and Access Management. *Journal of Information Security and Applications*, 1-36.

Lal, N. A., Prasad, S., & Farik, M. (2016). A Review Of Authentication Methods. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH , 5*(11), 246-249.

Lee, P. (2015). Device Fingerprinting and Identification. In Oracle, *Fusion Middleware Administering Oracle Adaptive Access Manager* (pp. E1 - E42). Oracle Corporation.

Levitt, H. M. (2017). How to conduct a qualitative meta-analysis: Tailoring methods to enhance methodological integrity. *Psychotherapy Research*, 367-378.

Liang, Y., Samtani, S., Guo, B., & Yu, Z. (2020). Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet of Things Journal*, 9128-9143.

Liu, Q., Wang, G., & Wu, J. (2012). Secure and privacy preserving keyword searching for cloud storage services. *Journal of Network and Computer Applications*, 927-933.

Manzoor, A., Shah, M. A., Khattak, H. A., Din, I. U., & Khan, M. K. (2019). Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. *International Journal of Communication Systems , 35*(12).

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, 155-184.

Marley, R. (2021, May 28). *Biometric Authentication is Smart but AI Makes it Smarter – Here is How*. Retrieved from Shufti Pro: https://shuftipro.com/blog/ai-making-biometrics-smarter/

Mehta, P., Jebarajakirthy, C., Maseeh, H. I., Anubha, A., Saha, R., & Dhanda, K. (2022). Artificial intelligence in marketing: A meta-analytic review. *Psychology & Marketing, 39*(11), 2013-2038.

Microsoft News Center UK. (2019, October 1). *Financial sector leading the way in using AI, Microsoft report reveals*. Retrieved from news.microsoft.com: https://news.microsoft.com/en-gb/2019/10/01/financial-sector-leading-the-way-in-using-ai-microsoft-report-reveals/

Mixon, E. (2018, 05 29). *Identity and access management tools add AI, microservices*. Retrieved 06 01, 2022, from SearchMobileComputing: https://www.techtarget.com/searchmobilecomputing/news/252441320/Identity-and-access-management-tools-add-AI-microservices

Mohammed, I. A. (2015). The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study. *International Journal of Creative Research Thoughts (IJCRT)*, 668-671.

Mohammed, I. A. (2018). A literature review on the application of AI to Identity Access Management. *Journal of Emerging Technologies and Innovative Research (JETIR), 5*(10), 96-99.

Mohammed, I. A. (2021). Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored and Controlled. *International Journal of Creative Research Thoughts (IJCRT)* , 4719-4723.

Mohammed, K. H., Hassan, A., & Yusuf, M. D. (2018). Identity and Access Management System: a Web-Based Approach for an Enterprise. *Path of Science, 4*(11), 2001 - 2011.

Murugan, S., & Kuppusamy, K. (2016). Functioning of Intelligence Intrusion Multi Detection Prevention Systems (IIMDPS). *i-manager's Journal on Information Technology, 5*(1), 18-27.

Naik, N., & Jenkins, P. (2020). uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain. *2020 IEEE International Symposium on Systems Engineering (ISSE)* (pp. 1-7). Vienna, Austria: IEEE.

Nezamoddini, N., Gholami, A., & Aqlan, F. (2020). A risk-based optimization framework for integrated supply chains using genetic algorithm and artificial neural networks. *International Journal of Production Economics, 225*.

Nikolova, I. (2020, April 16). *The Interaction Between Artificial Intelligence and Identity & Access Management*. Retrieved from patecco.com: https://patecco.com/en/the-interaction-between-artificial-intelligence-and-identity-access-management/

Noyes, J., Booth, A., Moore, G., Flemming, K., Tunçalp, Ö., & Shakibazadeh, E. (2019). Synthesising quantitative and qualitative evidence to inform guidelines on complex interventions: clarifying the purposes, designs and outlining some methods. *BMJ Global Health*, 1-14.

Oracle. (2015). *Fusion Middleware Administering Oracle Adaptive Access Manager, 11g Release 2 (11.1.2.3.0).* Oracle Corporation. Retrieved 06 02, 2022, from https://docs.oracle.com/cd/E52734_01/oaam/AAMAD/AAMAD.pdf

Osmanoglu, E. (2013). *Identity and Access Management: Business Performance Through Connected Intelligence.* Syngress, Elsevier.

PricewaterhouseCoopers. (2017). *Sizing the prize What's the real value of AI for your business and how can you capitalise?* PwC.

PricewaterhouseCoopers. (2022, December 9). *Sizing the prize PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution. What's the real value of AI for your business and how can you capitalise?* Retrieved from pwc.com: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

Purdy, M., & Daugherty, P. (2017). *How AI boosts industry profits and innovation .* Accenture.

Qiu, X., Du, Z., & Sun, X. (2019). Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks. *IEEE Access, 7*, 172004-172011.

Rowe, G., Nikols, N., & Simmons, D. (2018). *The Future of Identity Management (2018-2023).* TechVision Research.

Russell, S. J., & Norvig, P. (2016). *Artificial Intelligence : A Modern Approach.* Malaysia: Alan Apt.

Sarkar, A., & Shah, A. (2018). *Learning AWS: Design, build, and deploy responsive applications using AWS Cloud components, 2nd Edition.* Packt Publishing Ltd.

Schrimpf, A., Drechsler, A., & Dagianis, K. (2021). Assessing Identity and Access Management Process Maturity: First Insights from the German Financial Sector. *Information Systems Management*, 94-115.

Sennovate. (2022, May 22). *Increasing Importance of Artificial intelligence in IAM*. Retrieved from Sennovate.com: https://sennovate.com/increasing-importance-of-artificial-intelligence-in-iam/

ServReality. (2022, January 25). *Artificial intelligence in cybersecurity: pros and cons*. Retrieved April 6, 2022, from ServReality: https://servreality.com/blog/artificial-intelligence-in-cybersecurity-pros-and-cons/

Shah, S. W., & Kanhere, S. S. (2019). Recent Trends in User Authentication - A Survey. *7*, 112505-112519.

Sharma, D. H., Dhote, D. C., & Potey, M. M. (2016). Identity and Access Management as Security-as-a-Service from Clouds. *Procedia Computer Science*, 170 – 174 .

Sharman, R., Smith, S. D., & Gupta, M. (2012). *Digital Identity and Access Management: Technologies and Frameworks.* Hershey PA: IGI Global.

Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management: The Implications to Personal Data Protection. *IEEE Conference on Application, Information and Network Security (AINS)* (pp. 30-35). IEEE.

Sjöblom, C. (2021). Artificial Intelligence in Cybersecurity and Network security. *Master's thesis Faculty of Science and Engineering (FNT) Åbo Akademi University*.

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice, 4th ed.* Pearson.

Sturrus, E., & Kulikova, O. (2016). Identity and Access Management. In *Encyclopedia of Cloud Computing, First Edition* (pp. 396 - 405). John Wiley & Sons, Ltd.

Sudarsan, S. V., Schelén, O., & Bodin, U. (2021). Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT. *IEEE Access, 9*, 98169-98184.

Taddeo, M. (2019). Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity. *Minds and Machines, 29*, 187–191.

Tappert, C., & Dixon, N. (1974). A procedure for adaptive control of the interaction between acoustic classification and linguistic decoding in automatic recognition of continuous speech. *Artificial Intelligence*, 5(2), 95–113.

Timulak, L. (2009). Meta-analysis of qualitative studies: A tool for reviewing qualitative research findings in psychotherapy. *Psychotherapy Research*, 591-600.

Trellix. (n.d.). *What is Security Analytics*. Retrieved from Trellix.com: https://www.trellix.com/en-us/security-awareness/operations/what-is-security-analytics.html

Umurerwa, J., & Lesjak, M. (2021). AI implementation and usage: A qualitative study of managerial challenges in implementation and use of AI solutions from the researchers' perspective. *Umea University, Faculty of Social Sciences, Department of Informatics*, 1-34.

Verizon Enterprise Solutions. (2019, May 07). *2019 DBIR Summary of Findings*. Retrieved April 18, 2022, from Verizon Enterprise: https://www.verizon.com/business/resources/reports/dbir/2019/summary-of-findings/

Versola, L. (2021, August 01). *Machine Learning in Identity and Access Management*. Retrieved April 12, 2022, from Zero Trust Edge: https://www.zerotrustedge.com/blog/machine-learning-in-identity-and-access-management/

Weske, M., Hacid, M.-S., & Godart, C. (2007). *Web Information Systems Engineering – WISE 2007 Workshops.* Springer London, Limited.

Whitman, M. E., & Mattord, H. J. (2019). *Management of Information Security 6th Edition.* Boston, MA: Cengage Learning, Inc.

Wingerde, M. V. (2017). *Blockchain-enabled Self-Sovereign Identity - An exploratory study into the concept Self-Sovereign Identity and how blockchain technology can serve the fundamental basis.*

Wirkuttis, N., & Klein, H. (2017). Artificial Intelligence in Cybersecurity. *Cyber, Intelligence, and Security*, 103 - 119.

Yan, Z., Wang, M., Li, Y., & Vasilakos, A. V. (2016). Encrypted Data Management with Deduplication in Cloud Computing. *IEEE Cloud Computing*, 28-35.

Yang, Y., & Siau, K. L. (2018). A Qualitative Research on Marketing and Sales in the Artificial Intelligence Age. *Thirteenth Annual Midwest Association for Information Systems Conference (MWAIS 2018).* St. Louis, Missouri.

Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2021). Dynamic Access Control and Authorization System based on Zero-trust architecture. *Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System* (pp. 123–127). New York: Association for Computing Machinery.

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Choo, K.-K. R. (2019). Blockchain-Enabled Authentication Handover With Efficient Privacy Protection in SDN-Based 5G Networks. *EEE Transactions on Network Science and Engineering, 8*, 1120-1132.

Zhang, G., Li, J., Bamisile, O., & Cai, D. (2021). Spatio-Temporal Correlation-Based False Data Injection Attack Detection Using Deep Convolutional Neural Network. *IEEE Transactions on Smart Grid*, 1-1.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., . . . Choo, K.-K. R. (2021). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1029–1053.

Zhu, G., & Al-Qaraghuli, Y. (2022). AI-Assisted Authentication: State of the Art, Taxonomy and Future Roadmap. *Cryptography and Security*, 1-25.