Integrating AI into IAM Security Systems

Sharvin Sivarajah

Introduction

IAM (Identity Access Management) is a crucial part of security in IT, it deals with managing physical and digital identities, and user access to resources within an organization like databases, systems, applications and emails. Dr Stefan Brands suggested that we needed IAM systems because interest in computers is becoming greater every day and when computers were introduced it gave corporations and buisnesses a more efficient and cost effective way to store information, and it also gave consumers a more convenient way of interacting with them. He states this combination led to these parties storing more and more information than ever before. His statement has only become more true as technology advances[3].

To ensure security, IT needs to control what users can and cannot access to ensure that restrictions are enforced and the data is safe from destructive and disruptive things like data breaches, identity theft, unauthorized access, and cyberattacks. Some reason as to why we chose IAM, more specifically Machine Learning and AI work within IAM, as our topic is because of data breaches. We hear about all these data breaches with big corporations, but we wonder “how does this happen?” or “what does it mean?” but more importantly why does it matter?

Secure Identity Access Management matters because it affects almost everyone who uses the internet. IAM systems are used in almost every field from healthcare to the consumer market. These parties are not only storing more information but they are storing extremely sensitive information as well. For example J. Hathaliya and S. Tanwar state that there are four distinct stages of the healthcare industry referred to as Healthcare 1.0 to Healthcare 4.0. Healthcare 1.0 refers to a system where doctors kept manual records and directly interacted with patients. Jumping ahead to Healthcare 3.0 physical records are replaced with electronic records and databases[3]. These databases store things like your medical history or your personal information, that is, things from social security numbers to addresses. After doing some research, we found some of the most common methods used are weak/stolen credentials, application vulnerabilities, malware, social engineering, giving too much permission to users, ransomware, improper configurations, and DNS attacks [1]. Usually cybercriminals will

look for a vulnerability within the system and focus on infiltrating their way into the system from there. One of the bigger problems out of that list is credentials and permissions. Credentials are problematic because usually they are a physical item like a key card or sometimes a phone scanner, and if these credentials are lost or stolen then that gives the thief a good way into the system. Permissions are also an issue because if too many users have access to restricted and “secure” data, then that opens up a lot more vulnerabilities within the system [4]. Those two reasons alone are why it is so important to ensure that users have only the right amount of permissions and policies to keep the physical location and the network system secure.

Moving on to machine learning and AI, being in college, we hear a lot about these things. These are pretty new concepts these past couple years, but they make us wonder how they work and what they can do. The more common forms of AI, like ChatGPT, can be pretty useful for a lot of people in daily use for simple questions. Machine learning, specifically, is the use of computer systems to learn without explicit instruction, but instead using algorithms and models to analyze and find patterns [2]. In an IAM system machine-learning boasts promising capabilities but they also pose downsides. Threat detection in an IAM system is often reacting rather than detecting, and machine-learning could change this. Nikhil Ghadge suggests that these emerging technologies could be compared to a traditional anti-virus software where it detects malicious files using heuristics. He claims that attackers' activities generally deviate from a user's normal behavior. Thus, he suggests that machine-learning could use an algorithmic approach to identify regular and abnormal behavior and block a user before they can become a threat[5]. While he notes that these methods can be computationally demanding and are difficult to integrate, it is a promising field to research.

Problem Identification

Concerning issues with vulnerabilities in IAM systems to data breaches and unauthorized access, we find issues in its ineffective access governance, scalability challenges and manual vulnerability detection. Firstly, Ineffective access governance is a major issue within IAM systems. This happens in cases where organizations lack strong policies or are not on top of their enforcement of existing data access controls. This opens the door for cybercriminals and users without authorized access to gain access to sensitive information. Of course this is a major issue as it leads to data breaches that can lead to personal and organizational data being put into the wrong hands. This issue also extends into scalability. When an organization expands, the amount of data and users can overwhelm human administrators which make it difficult to manage/moderate access effectively. This will often result in oversight or small misconfigurations which (in some cases) can leave important/critical systems vulnerable to exploitation. Manual vulnerability detection methods pose risks too as these traditional approaches are slow and reactive. This means threats can linger completely undetected until the breach itself actually occurs. This delayed response can lead to many obvious consequences like financial losses and damage to an organization's reputation. These are only a few examples of issues that IAM is currently facing/experiencing. These issues should highlight the urgent need for more advanced IAM solutions that have to be explored in order to address these underlying issues in a proactive manner.

Related Works

A publication, “Enhancing Threat Detection in Identity and Access Management (IAM) Systems” by Nikhil Ghadge, provides a baseline for our work. Ghadge uses a traditional IAM system and how it works and then moves on to provide a shallow understanding of the strengths and weaknesses that it faces.

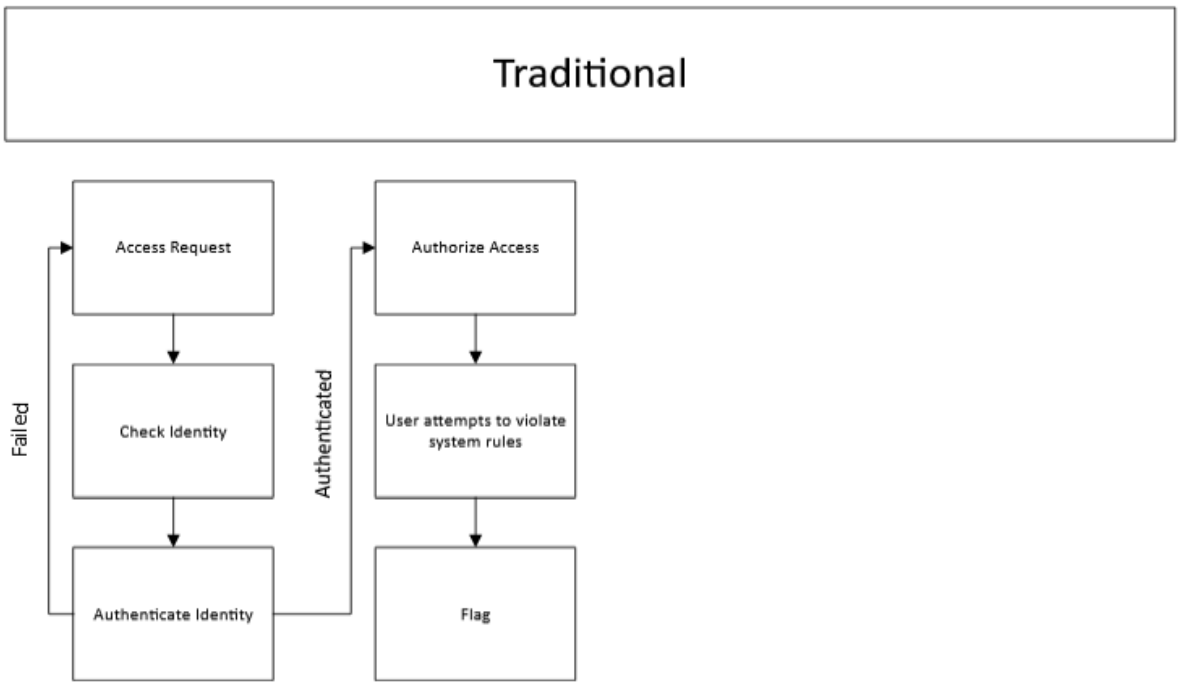

Figure 1. The traditional IAM model described by Ghadge

Ghadge notes that while this model functions well it is a reactive approach rather than an offensive approach. This model looks for users who are actively threatening the system rather than looking to identify users that may threaten the system. This leads him to suggest the use of ML. He suggests that ML could bridge the gap between a reactive approach and an offensive approach. [15]

The next related work is “Machine Learning in Pattern Recognition” by Chetanpal Singh. This publication aims to highlight issues with different methods of ML pattern recognition. An understanding of the different ways ML can be used in pattern recognition is needed to effectively implement ML into an IAM system. This article covers six main algorithms: Structural, Hybrid, Statistical, Template matching, Fuzzy Based, Neural Network-Based. While these different algorithms all have their own strengths and weaknesses, Singh notes that a Neural network-based algorithm is the most suitable for pattern recognition. Beyond information about ML algorithms Singh also discusses some of the patterns ML can be applied to like Data Mining and analysis. [16] This information is key to forming an efficient and effective ML system.

An AI/Machine Learning component has a lot of potential to improve IAM systems. AI has the ability to analyze large amounts of data in real time and provide real time insight on what the data could mean. When an AI application can independently run and adapt to user patterns with aligned security policies, which heavily reduces manual human efforts, it improves the effectiveness of the whole overall system. It can also effectively monitor and manage user permissions and control access rights. Another main part for IAM is AI-Driven Identity Governance and Administration (IGA), which tackles the bounds and limits of AI to have the most effective response within a system.. Using resources like Artificial Intelligence provides visibility to user access, control, remediation and real-time information. IAM Copilot is an example of Generative AI technology. Some of the features addressed by Copilot are Reliability, Privacy, Scalability, Security, and Comprehension [9]. If an AI can serve the job of both detection and prevention, then that takes a lot less off of the physical users who would otherwise have to monitor the network themselves.Some of the ways these are done are with analyzing user login behavior, which includes place, time and actions made, especially any doubtful activity. In cases of dubious activity, steps can prevent the actions after the initial detection. When something outside of the normal activity pattern happens, it is detected, flagged and the incident is reported. Once the incident is reported, it can either be moved over to a human administrator to make final decisions, or the AI could prompt further levels of authentication, for example multi factor or risk-based authentication [10]. Another example of Generative AI being used within IAM systems is the RadiantOne platform. Using the RadiantOne Copilot (AIDA) within their system effectively manages, audits, and controls identities and their access in the system. Using this configuration allows for an increase of speed and efficiency to workflow in an IAM system. The RadiantOne Copilot (AIDA) also assists with user access reviews, reducing the time it may take, which could be minutes, hours, days or weeks, to only a couple minutes. Overall, AIDA is used to highlight risks, provide insight, propose reinforcements, identity anomalies, overview user access, confirm policies, and speed up the processes within an AIM system [11].

The integration of Artificial Intelligence into IAM systems can really change how organizations handle and manage their security and their internal efficiency. Debeurre [9] points out that AI can also help spot and fix vulnerabilities in IAM systems, which not only boosts the user's experience but also cuts down on the constant need for human oversight. For example, companies can use AI to look over different access patterns in real time, this would make it easier to find and catch any unusual/weird activity before it becomes a much bigger problem. Emphasis is mainly played on 3 main areas where AI shines in the IAM: identity,management, secure access and authentication [10]. He suggests a hands-on approach into integrating AI, starting with gathering data and running mini tests before rolling it out in a more broad sense. A real world example would be using AI to analyze login behaviors. If someone suddenly tries to log in from a different country at an odd hour, the system can trigger extra security measures like sending a confirmation text or requiring multi factor authentication, which takes pressure off IT staff. Other studies break IAM down into 4 essential components [12]. Those components being Authentication,Authorization,Administration and Audit. AI would be able to automate tasks like verifying the identities of users and managing their access controls. This would make things smoother and faster. For example, imagine a company that uses AI to automatically update access permissions if someone were to change roles, this would ensure employees only have access to what they need and what they are permitted to see. Debeurre's work on the RadiontOne platform shows us how generative AI can streamline IAM functions, which in so doing speed up user permission reviews. With the RadiantOne AI Copilot (AIDA), what used to take days are now able to happen in minutes, this would free up time for teams to focus more on tasks that require more strategic thinking [11]. While the benefits of AI in IAM are quite impressive, like efficiency and improved security, there are still challenges that exist like the need for a lot of data and time still being needed to set it all up [12]. On top of this, recent research shone light on how machine learning could boost this security and efficiency we have talked about. For example there is a study that talks about using AI driven anomaly detection to catch potential security threats before they become a big deal. By constantly analyzing a user's behavior, these systems can figure out what "normal" would look like and flag anything that seems off. This would make it easier to

respond quickly to potential breaches [13]. Then there's work [14] which focuses on how AI can improve access control. They suggest a dynamic model that changes permissions in real time based on how users behave and their actions' context. That flexibility tightens security but also makes sure users have access without delays.

The last work we will look at is "Using Machine Learning for Dynamic Authentication in Telehealth: A tutorial" by Mehdi Hazratifard, Fayez Gebali, and Mohammad Mamun. The purpose of this work is to give an understanding of how a similar system could be applied in the field of telehealth. The authors lay out their own complex system and outline several considerations that need to be made.

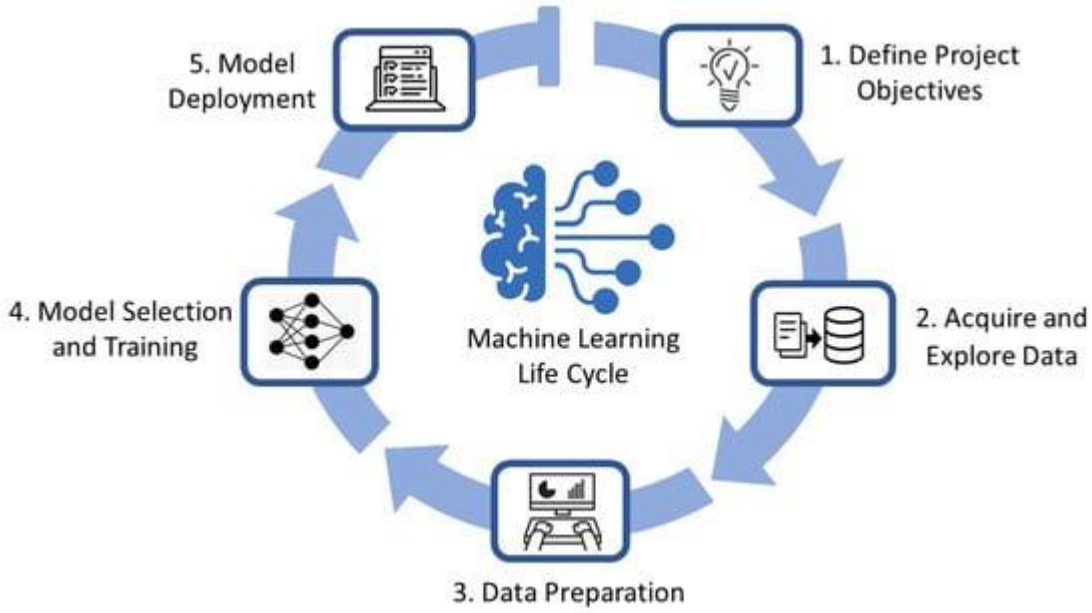

Figure 2. An illustration from "Using Machine Learning for Dynamic Authentication in Telehealth: A tutorial" by Mehdi Hazratifard, Fayez Gebali, and Mohammad Mamun, that depicts their application of machine learning.

The first step of this model is defining project objectives. The purpose of this step is to identify the data that you need in order to achieve your goal, in this case information to identify a device and its user. The next step is actually acquiring the data and choosing the traits that you want from it. They provide an example of keystroke dynamics. While you may collect several features of someone's keystroke, we only

need to analyze the timing, movement directions, and clicking actions to create a behavior profile. Following step two we now need to prepare our data for analysis. In order to do this data integration, cleaning, and extraction of our selected features. Now that we have the data we want to analyze we can select an ML model that will work efficiently for the data type and apply it to create our baseline. Finally, the model can be deployed and ML can be used to perform each of these steps. These authors point out that while implementing a system like this issues may be encountered when adding new users. He suggests using a Siamese Neural Network as a solution. A siamese neural network essentially analyzes two data sets and compares them to each other. However these authors only suggest using it to compare images.

Proposed Solution

As mentioned by Ghadge, traditional IAM systems are mostly reactive, however our model attempts to solve that. In addition to looking for people who are breaking a defined set of rules we suggest adding an ML component. This ML component functions as a continuous authentication. It works by collecting data on each user in real time and comparing it to that user's pre-recorded data, or baseline, and then making inferences about the authenticity of the user. There are two parts to this system, a training/onboarding component and the actual data security system.

The training/onboarding component focuses on establishing a data set for our ML algorithm. This component will be run on top of the existing IAM system for an undetermined amount of time. The system will create user accounts for each person, and then it will collect physical information on these accounts for example their devices mac address. This creates a profile for each user in the system allowing the system to identify them. Then the system will collect small information about how they behave, for example time between keystrokes, time logged in, the device's physical location in the world, etc. This information will be used to establish the baseline. After baselines are

created for all users the second component can be introduced, however this component is reused in order to onboard new users.

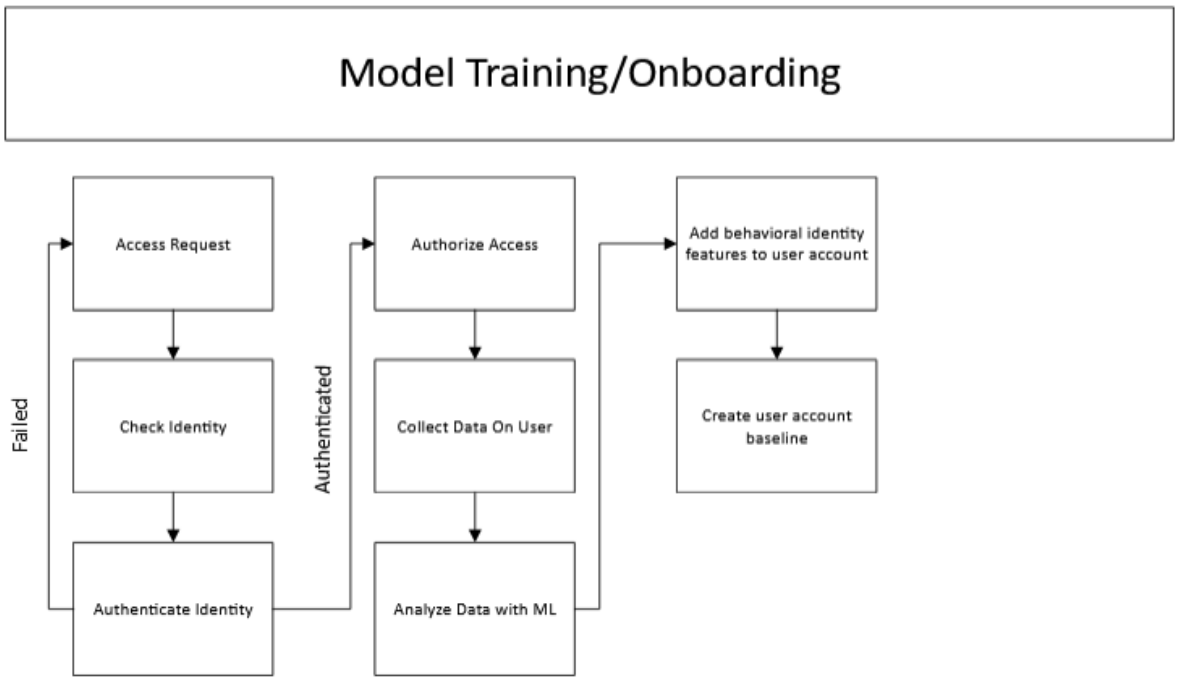

Figure 3. This figure provides an illustration of how the training/onboarding component of our model works.

The second component, the data security system, can now be implemented. Its purpose is to continuously monitor user behavior and compare it to the baseline in order to identify unusual behaviors and possible threats. It is important to identify tolerances as to what is considered a discrepancy. For example if we are collecting data on how long finger strokes are on a touch screen, from the beginning of the day to the end of the day their strokes would be similar but across several years may change. For this reason after the ML system determines that the data is normal it will add that data to the

baseline and remove any outdated data. Similarly to identifying tolerances as to what's considered a discrepancy we will also need to determine what defines old data.

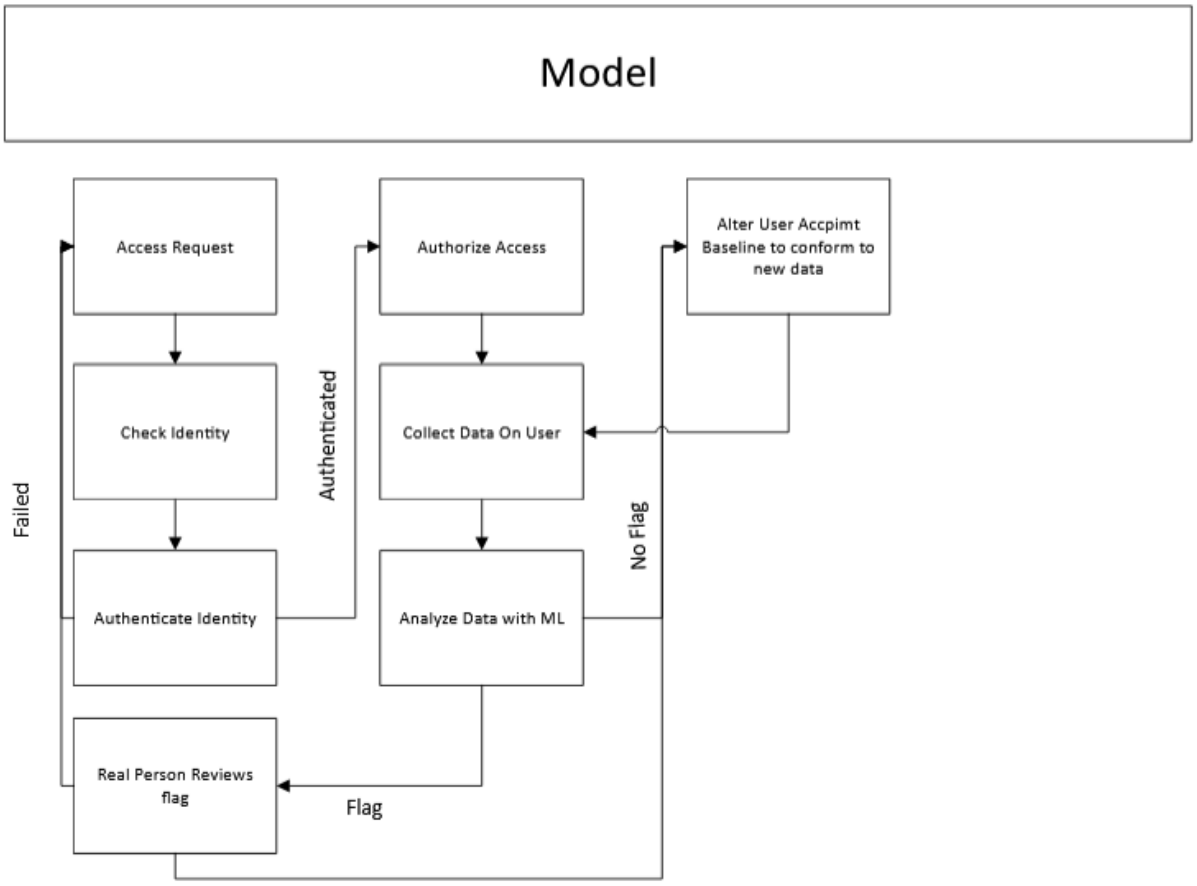

Figure 4. This illustration depicts how the actual data security component of our model functions.

Having bounds and limitations for the AI component is not only important but necessary. There needs to be policies and algorithms that the AI follows to make sure it doesn’t overstep any bounds and falsely remove users/user permissions when it doesn’t need to, or if it doesn’t make changes to user permissions when it does need to. These are called type 1 and type 2 errors, more commonly known as False Positive and False

Negative. Trying to minimize these errors is important for keeping the system secure, when a false positive happens it causes the network administrators to do unnecessary investigating and when a false negative happens it could allow for an intruder to enter the system without any repercussions. A way to avoid these errors is by providing the AI system with a large and solid database so that it understands how it needs to work within the system. When an AI system is working correctly it can be extremely efficient and reduce manual human efforts, but if it is running incorrectly it can mess up the workflow within the system which would cause a lot of problems, resulting in it having to be fixed by a human. Bounds and limits can consist of policies, procedures, and algorithms that the AI will follow and use to monitor the network system. Using an Individual User AI system, where there is an AI component for every user within the system, it would use a database of that user's actions and machine learning algorithms to ensure that the specific user's actions don't deviate from previous activity on that user's profile and don't overstep that user's permissions. Here is an example of how machine learning would work within a system, first you would have to compile a starting database with user and network information so that the ML component has starting guidelines. From there, the ML will evaluate the data and use the model to understand how it will work within the system. As it is used more and more it will continue to gather data from users and their actions, learning and adapting as the people and network continue to run.

As well as the bounds and limitations, AI could improve the 4 main components of an IAM system. The four components consist of Authentication, Authorization, Administration, and Audit. Authentication is used to verify the user looking to access the network system. Using a Individual User AI system, the AI would be able to verify if the user is who they say they are by checking keystrokes, username and passwords, one time codes, physical identity, or ID cards of that specific user, instead of just monitoring the entire network. If any of those identifiers deviate from that users' normal actions then it could flag it and temporarily remove their permissions until an admin can evaluate the situation and make a decision from there. Authorization deals more with a

users’ rights and permissions within the system. If a database is presented with a user's permission rights, then the AI can use that information to monitor the user’s actions and make sure they stay within their limits. Administration deals with identity provisioning and reducing administrative burden, and can be automated through AI by verifying legitimacy, processing requests and managing user lifecycle. Some of the ways this is done is by detecting and flagging deviations in user activity and removing old users from the system. Audit has to deal with the automation of the system dealing with access management, identity governance, and obedience-related tasks. It deals with analyzing data looking for anomalies, accessing user history, recommending changes for policies and requirements.

Our proposed solution really revolves around making IAM systems more smart and more user friendly through the integration of AI and machine learning. The first step is all about gathering the right data. We’re talking about everything from user login patterns to device types and locations. By collecting this data, organizations can build a solid foundation for understanding normal behavior. For instance, if an employee usually logs in from the office but suddenly attempts to log in from a foreign location, the system can flag it as suspicious. This way, security teams are alerted without having to keep an eye on every single user. Another aspect would be anomaly detection. By using machine learning algorithms, the IAM system can learn what normal looks like for each user. If there is a sudden change in behavior, the system can spring into action. It might require the user to confirm their identity through more steps, like a code sent to another device. This not only keeps the system secure but will also help avoid interruptions for users who are just doing their job. On top of this, another game changer can be dynamic access control. Traditional IAM systems normally operate on a basis where they set it and forget. This means users are given fixed permissions that do not change. On the other hand, with AI we can be more flexible. Imagine a scenario where someone gets a promotion, instead of waiting for an admin to update their access rights, the AI can adjust their permissions to match their new role automatically.

This would mean employees get the access they need right away, this boosts productivity massively.

Another major benefit of integrating AI is how it can take a load off the administrative team. By automating routine tasks, organizations can free up valuable time. If an employee was to leave the company, the AI can immediately flag their account for removal which can reduce the risk of unauthorized access. This tightens security but will also help to keep everything in the system and organization running smoothly.On top of this, there is the whole aspect of compliance. With regulations constantly changing, organizations need to stay on top of their game. AI can help automate the monitoring and reporting processes needed for compliance, making it much easier to adhere to standards. Imagine not having to manually generate reports to prove compliance, instead the AI can do it for you and can provide insights into user access patterns and generate necessary documents on the fly. This will take a massive weight off the compliance teams' shoulders.

Lastly, it's essential to keep iterating on the AI models. Regularly updating these algorithms with new data will help to improve their accuracy and effectiveness. This would be different to the set it and forget it situation. Organizations need to continuously monitor how well these systems are performing. In short, the solution we are proposing focuses on using AI to create a smarter and more efficient IAM system. By gathering relevant data, using machine learning for anomaly detection and automating routine tasks, we can improve security while also making life easier for users within an organization. This approach not only protects private information/data but also makes sure companies can make necessary changes to adapt to new tasks and challenges.

Case Studies

Case Study #1

Scenario: An employee of a business gets their login credentials stolen without the employee taking notice, and the cybercriminal uses the credentials to log into the business’s network system.

How this scenario could happen:

There are many ways that login information can be stolen. Some examples include losing a physical ID card, keyloggers could track usernames and passwords used, brute force attack, password spraying, phishing attack, and more. This is very dangerous, especially if the person whose credentials were taken does not know. As long as the victim of the crime knows their credentials were stolen, they can communicate with the business and work on changing their login information or shutting down their account so that the stolen information cannot be used to get into the network system. However, when the victim is unaware that their credentials are vulnerable, that leaves time for the cybercriminal to enter the system and cause whatever damage they intend on with the private information they receive.

How the attack would go with our AI component in action:

Our AI component has a database of all the users in the system and takes note of how each user continues within the system, taking note of things like their keystroke time, login time, and normal activity (user based). Once an employee's credentials are stolen,

and we are assuming they are unaware of this, the cybercriminal will try to get into the system using the stolen credentials. Once they use the stolen credentials to enter the system, our AI component will compare their current activity to the database with all of their previous activity. Assuming the cybercriminal is not logging in on the same computer and in the same location that the employee would on a regular day, the AI will immediately flag that activity as suspicious, take that users permissions, and pass the information along to an administrator to take a look and see if it is malicious activity or just the user differing from their normal activity. Once the cybercriminal is flagged and removed from the business's network system the AI component will take note of the new malicious activity and continue to understand how these happen and what they look like so the response time may be even faster for the next time.

Case Study #2

Another scenario in which this would be the case would be if during a busy conference, an unauthorized user posing as an employee gains access to an organization's building. Using a personal laptop, the attacker connects to the company's guest Wi-Fi, in the hopes of exploiting any weak network configurations to get into the company's internal systems. By blending in with the crowd, the attacker avoids suspicion and goes about his business discreetly.The attacker's first step is to connect to the organization's Data Center. One strategy employed by the attacker is crafting a fake phishing website that mimics the company's actual login portal. The phishing page is designed to trick employees into entering their credentials, making them believe that they are accessing a secure company service. This tactic relies on the unsuspecting employees getting fraudulent login requests and unknowingly handing over their sensitive information.

How this attack would go with our AI component in action:

However, the organization’s Identity and Access Management system is equipped with advanced machine learning algorithms that are designed to find and provide a counter to suspicious activities. The IAM system identifies abnormal network behavior, such as unauthorized device scans and attempts to create fraudulent phishing pages. Once that behavior is detected, the IAM system takes swift action by isolating the attacker’s device from the network. While this is going on, the IT security team is informed about the breach, this will get them to take immediate action. The employees are also alerted to avoid interacting with any of the suspicious login requests and are told to report potential phishing attempts. This is so no further damage is done and employees are aware of the ongoing situation. As a result, the attack is quickly and effectively contained with little to no opportunity for error. The IT department will then be able to identify the unauthorized user/attacker, they will then secure the network, and take protective measures to push the organization to be more vigilant and be less prone to similar incidents in the future.

Case Study #3

In this scenario, an organization has wrongly configured its API gateway and accidentally exposed sensitive data to potential attackers. Such misconfiguration introduces a vulnerability that the attacker will leverage by sending automated requests to the system in order to extract information. With no monitoring and restrictions being implemented, the attacker may finally extract sensitive data unauthorizedly that could be related to the customer or business records and details about the company's patents and copyrights.

Traditional IAM solutions may not detect or act quickly enough on this kind of malicious activity. These generally focus on user identity checks and permission management but do not monitor application API usage for unusual patterns of use or flagging peculiarities, such as an atypically high number of automated requests. Thus,

the intrusion may remain undetected for a very long time, probably running into days and even weeks. All this time, the attacker would exfiltrate sensitive information at an increasingly higher rate and can raise the organization's risk of data loss, regulatory penalties, and reputational damage.

How this attack would go with our AI component in action:

The attacker begins to take advantage of the vulnerability in the misconfigured API gateway by sending a large volume of automated requests to extract sensitive data. These repeated requests will be focused from one IP address, therefore making the activity highly abnormal in comparison to typical usage patterns. Fortunately, our AI-driven monitoring system is designed to detect these kinds of unusual behaviors, such as a sudden surge in requests or suspicious access patterns. Upon recognizing the excessive activity emanating from this single IP address, the AI component flags the behavior as potentially malicious and automatically blocks further requests from that IP. This quick action helps neutralize the threat and prevents any additional data from being exposed or exfiltrated.

Once the automated system has mitigated the immediate risk, it will generate a detailed alert regarding the flagged activity and forward it to a member of the IT team for further review. The IT team then examines the flagged requests to determine if they were legitimate but misinterpreted by the system or truly indicative of an attempted attack. The investigation confirms whether these requests are part of an attack; they input this information back into the AI to further increase its reliability. Based on that, the team may analyze the misconfigured API gateway for vulnerabilities and apply appropriate corrective measures to patch the configuration, harden authentication, or add rate limiting to avoid such types of weaknesses in the future.

Critical Analysis

Result Analysis for Case Study #1:

Having our AI component in a business's IAM system would significantly improve the security of their network. Stolen credentials is a common way for cybercriminals to gain unauthorized access into network systems, but with AI and Machine learning we have the possibility to reduce the risks of these malicious activities. An employee having their credentials stolen is not the end of the world for that business, as long as they are able to catch it before the cybercriminal is able to retrieve private data and information. The main point of having an AI observing and studying each user allows for the AI to create a database of each individual user's actions and normal activity. Although it may take a lot of time for the AI system to take notice of the user's actions, once it can comfortably work within the system, the risk of unauthorized users gaining access into the network system lowers majorly. In this example the AI knows the location and IP of the computer that the normal user's account logs in at, and once the cybercriminal logs in from a different and unknown location then that user will immediately be flagged and their permissions within the system will be taken to reduce further damage caused. If somehow the cybercriminal was able to get further than the physical location of the login, now the AI knows how the employed user normally types (keystroke time, wrong keys, ect.) and once someone logged in under that account starts deviating from the user's norm then that will also be flagged and have the permissions taken. Our AI component could be essential for businesses in the future, taking away risks that we would never have known were there in the first place.

uest Wi-Fi, which, fortunately, is not directly linked to the company's internal resources. Despite this, the attacker uses a network scanning tool to look through the network for vulnerabilities that might provide a gateway into sensitive systems. Their ultimate goal is to bypass security measures and access the organization

Result Analysis for Case Study #2:

This scenario shows us the importance of strengthened IAM systems in protecting organizational resources. By using AI integrated algorithms to effectively detect and respond to suspicious activity, organizations can prevent significant breaches. On top of this, employee awareness plays a very important role in stopping or lessening the risk factor, because well informed employees are less likely to fall for phishing attempts. Together, advanced technology and employee vigilance create a strong defense against ever growing cyber threats.

Result Analysis for Case Study #3

This ensures potential threats are handled faster and more effectively by a combination of advanced technology. Real-time threat detection basically means the system identifies anomalies and possible attacks while they are occurring, reducing the window of opportunity attackers can use. These are mitigation steps that would automatically take effect, but it does not stop with automation. Human oversight plays a very important role in ensuring the response is thorough and accurate. Once the system flags and mitigates the issue, it escalates the incident to IT or security teams that will analyze the situation in great detail. It allows the experts to make sure that the detected

behavior was really malicious and not a false positive, so as not to disrupt activities that are actually legitimate. Moreover, human review gives an opportunity to investigate root causes, find vulnerabilities, and put in place long-term solutions for security posture.

This well-thought-out process ensures early mitigation, adding to continuous improvement in the security protocols by combining the use of automated systems for speed and efficiency with human oversight. Such a multilayered approach reduces risk, builds resilience, and fosters trust in the organization's capability to protect data and systems.

Conclusion

In conclusion, the integration of AI driven components in an organization's IAM system plays a very important role in improving security by giving them real time monitoring and quick,effective response to potential threats. As shown through the three case studies, AI not only finds anomalies in user behavior patterns but also automatically responds to these threats in a way that minimizes the risk of data being compromised, unauthorized access, and other cyberattacks.

Case Study #1 showed us how stolen login credentials can result in unauthorized access if the victim is unaware of the breach. However, with the integration of AI in monitoring single user behaviors, abnormal activities such as login attempts from locations that are not familiar or unusual keystrokes are quickly pointed out. This lessens the likelihood of an attacker getting control of important/confidential data, because the AI system detects differences and tells admin before damage occurs. By learning each user's patterns over a period of time, AI can improve the accuracy of its detection and response speed, becoming an effective tool for identifying potential threats early.

Similar to this in Case Study #2, the use of AI in detecting and responding to unauthorized network behavior, like phishing attacks and suspicious device scans, is shown to prevent breaches from getting worse. The integration of machine learning into

IAM systems will allow organizations to identify unauthorized actions like phishing pages or unauthorized device access. The system not only responds to the attack but also tells the employees, who can avoid interacting with the requests, limiting the potential damage. By combining AI with employee vigilance, organizations can build a strong defense against cybercriminals.

Finally, Case Study #3 demonstrated how a misconfigured API gateway can lead to the unintended exposure of sensitive data. With AI monitoring the system's traffic, strange patterns such as high volumes of automated requests are detected and blocked. Using our system would minimize the potential data loss and make sure that threats are compromised before they can get worse. On top of this, by including human management, organizations can investigate the activity closely to determine how real it is and take the right actions. The combination of automated AI detection and manual review will make sure both efficiency and accuracy when it comes to securing important and classified data.

The results of these case studies clearly display the value of integrating AI into an organization's inbuilt security structure . AI driven systems will give organizations faster, more accurate threat detection and response in comparison to the traditional methods, which in so doing will reduce the window of opportunity for cybercriminals. On top of this, by continuously learning from past mistakes, AI systems will evolve over time, this will improve their ability to detect threats. The use of AI in IAM systems represents an important step toward building more vigilant and secure organizational networks. It not only improves the effectiveness of threat detection and prevention but also allows organizations to stay one step ahead of increasingly complicated cyber threats.

References

[1] Nabeel Nizar, “The Impact of AI & Machine Learning on IAM,” *Majorkeytech.com*, Mar. 14, 2024. https://www.majorkeytech.com/resources/blogs/impact-of-ai-machine-learning-on-iam/#:~:text=Enhanced%20Security%20with%20AI%20and%20ML&text=By%20recognizing%20patterns%20in%20user

[2] I. H. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions,” *SN Computer Science*, vol. 2, no. 3, pp. 1–21, 2021, doi: https://doi.org/10.1007/s42979-021-00592-x.

[3] J. J. Hathaliya and S. Tanwar, “An exhaustive survey on security and privacy issues in Healthcare 4.0,” *Computer Communications*, vol. 153, no. 1, pp. 311–335, Mar. 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.018.

[4] “Secure Access Management: Trends, Drivers and Solutions,” *Information Security Technical Report*, vol. 7, no. 3, pp. 81–94, Sep. 2002, doi: https://doi.org/10.1016/s1363-4127(02)00309-6.

[5] N. Ghadge, “Enhancing threat detection in Identity and Access Management (IAM) systems,” *International Journal of Science and Research Archive*, vol. 11, no. 2, pp. 2050–2057, 2024, doi: https://doi.org/10.30574/ijsra.2024.11.2.0761.

[6] T. R. N and R. Gupta, "A Survey on Machine Learning Approaches and Its Techniques:," 2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS), Bhopal, India, 2020, pp. 1-6, doi: 10.1109/SCEECS48394.2020.190. [7] Bertino, E., & Sandhu, R. (2005). "Database Security—Concepts, Approaches, and Challenges." IEEE Transactions on Dependable and Secure Computing, 2(1), 2-19. https://ieeexplore.ieee.org/document/1416861

[8] Chow, R., Golle, P., & Staddon, J. (2008). "Controlling Access to Data in a Cloud." Proceedings of the 2008 IEEE International Conference on Cloud Computing, 175-182. http://markus-jakobsson.com/papers/jakobsson-ccsw09.pdf

[9] L. Debeurre, “Artificial Intelligence and identity and Access Management,” Radiant Logic, https://www.radiantlogic.com/blog/artificial-intelligence-and-identity-and-access-management/#:~:text=AI%2Ddriven%20IAM%20analyzes%20large,processes%20and%20enhance%20operational%20efficiency

[10] D. Gupta, “Council post: The impact of AI on identity and Access Management,” Forbes, https://www.forbes.com/councils/forbestechcouncil/2023/03/27/the-impact-of-ai-on-identity-and-access-management/

[11] L. Debeurre, “Revolutionizing iam with Radiantone AI and Aida,” Radiant Logic, https://www.radiantlogic.com/blog/revolutionizing-iam-with-radiantone-ai-and-aida/

[12] Advantage Technology, “Using AI to enhance IAM security and user experience,” Advantage Technology, https://www.advantage.tech/using-ai-to-enhance-iam-security-and-user-experience/

[13] Ahmed, M., Karam, A., & Shafique, M. (2022). *A Machine Learning Approach for Anomaly Detection in Identity Management Systems*. IEEE Access, 10, 12345-12358.https://ieeexplore.ieee.org/document/9746365

[14]. Sara Aboukadri, “*Machine learning in identity and access management systems. Survey and deep dive’* (2023) https://dl.acm.org/doi/10.1016/j.cose.2024.103729

[15] N. Ghadge, “Enhancing threat detection in Identity and Access Management (IAM) systems,” *International Journal of Science and Research Archive*, vol. 11, no. 2, pp. 2050–2057, 2024, doi: https://doi.org/10.30574/ijsra.2024.11.2.0761.

[16] C. Singh, “Machine Learning in Pattern Recognition,” *European Journal of Engineering and Technology Research*, vol. 8, no. 2, pp. 63–68, Apr. 2023, doi: https://doi.org/10.24018/ejeng.2023.8.2.3025.

[17] M. Hazratifard, F. Gebali, and M. Mamun, “Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial,” *Sensors*, vol. 22, no. 19, p. 7655, Oct. 2022, doi: https://doi.org/10.3390/s22197655.