Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Driven Adaptive Zero-Trust Models for U.S. Defense Networks

Md Fahim Ahammed[1]✉ and Md Rasheduzzaman Labu[2]
[1]*Department of Information Assurance and Cybersecurity, Gannon University, Erie, Pennsylvania, USA*
[2]*Department of Information Assurance and Cybersecurity, Gannon University, Erie, Pennsylvania, USA*
Corresponding Author: Md Fahim Ahammed, **E-mail**: mdfahimahammed7773@gmail.com

| ABSTRACT

The dynamically changing cybersecurity landscape in the USA demands a much more robust Identity Access management approach. At the core of this evolution lies the trust mode of security relies on the never-trusted-always-verify principles, turning it into one of the leading ways to plan how access to crucial resources should be secured. This study investigates the use of Artificial Intelligence in improving Identity Access Management through User Behavioral Analytics and adaptive authentication at Zero Trust Architecture. AI-driven User Behavioral Analytics was singled out as one of the transformative tools in the continuous monitoring and analysis of user behavioral patterns. Through the use of ML algorithms, baseline activity metrics are set up: time of login, location, device attribute, and what resource he or she tried to access. It flags deviations from these baselines as potential anomalies, requiring further scrutiny and possible security actions. This proactive approach to anomaly detection greatly strengthens Identity Access Management within a Zero Trust context by allowing an organization in the USA to identify and address such threats in real time.

| KEYWORDS

Zero Trust models; AI-Powered Behavioral Analytics; Identity Access Management; Multi-Factor Authentication; Adaptive Authentication

| ARTICLE INFORMATION

ACCEPTED: 20 May 2025 **PUBLISHED:** 15 June 2025 **DOI:** 10.32996/jcsts.2025.7.6.56

Introduction

As per Joshi et al. (2024), in the recent past, the cybersecurity landscape in America has come to be marked by a rapidly increasing threat environment. From APTs and zero-day vulnerabilities to social engineering, hackers deploy anything that can help them permeate sensitive systems and access critical data. Traditional security models based on perimeter defenses depend on fixed barriers to defend entry into networks, clearly becoming less effective against these evolving challenges. This occurrence has become a defining moment that has driven the need for a radical shift towards a more resilient and adaptive security framework. At the center of this evolving dynamic has been the zero-trust model. According to Chirra (2024), Rooted in one of its guiding principles, "never trust, always verify," the model stresses that no implicit trust shall be allowed in a network, considering any user located anywhere and using any device. Because of this, every access request must undergo strict authentication and authorization with constant monitoring throughout the session. This requires an effective Identity and Access Management strategy that can enforce precise and dynamic access controls to adapt to risk scenarios.

Traditional Identity and Access Management (IAM) solutions provide one layer of security, whereas most fall short of reaching the bar in Zero Trust environments. Essentially, legacy IAM systems are heavily reliant on static rules and depend on pre-defined permissions that are cumbersome and complicated to manage which suffices for the dynamic nature of modern cyber threats. Besides, traditional approaches can barely provide the quota of fine-grained control and real-time threat detection to enforce

the principles of Zero Trust effectively (Weinberg & Cohen, 2024). This research will study the transformative role AI plays in the revolution of IAM in a Zero Trust world. Powering A1 and ML, organizations can adopt access control that is much more adaptive and intelligent. The research focuses on two of the most critical innovation areas for IAM, namely User Behavior Analytics (UBA) and adaptive authentication. AI-driven UBA allows organizations to analyze user behavior patterns more deeply, allowing them to detect and respond to potential security threats in real-time. Additionally, A1 can enhance and customize access control by dynamically adjusting authentication protocols based on user context, risk levels, and the Sensitivity of the resource being accessed. This paper explores the theoretical grounds of AI-Powered UBA and adaptive authentication and evaluates their practical uses in Zero Trust.

Background and Motivation

Yang (2023), posits that the traditional perimeter-based security models are inefficient in guarding digital assets in the ever-changing face of sophisticated cyber threats in information technology and network security. It is this inadequacy that has driven a paradigm shift in security strategies, hence giving birth to the innovative model labeled "Zero Trust.". With the principles of continuous verification, least privilege access, and strict network segmentation, Zero Trust provides a modern framework for protecting digital infrastructures from ever-evolving pervasive security risks. Traditional models are dependent on the implicit trust of an organization's internal network, but this has increasingly become vulnerable as cyber attackers seek to exploit various weaknesses. Shaik et al., (2023), indicated that legacy solutions utilizing firewalls and VPNs have failed against the complexity brought about by cloud computing, a mobile workforce, and an ever-expanding ecosystem of the Internet of Things. Besides this, huge dependence on static perimeters or strategies linked to "castle-and-moat" has turned out to be inefficient in countering advanced threats that easily infiltrate systems and hence go unnoticed. Identity and Access Management represents an overall set of policies, processes, and technologies that manage who has access to which resources within an organization. Essentially, its core part is composed of three main pillars:

- **Authentication**: It normally means the act of proving one's identity based on the provided claims. The usual methods include using usernames and passwords, multi-factor authentication, and biometric verification (Muhammad et al. 2024).
- **Authorization:** This criterion follows immediately after the authentication process. It involves defining what a user is allowed to do. Authorization typically defines what resources are available to a user, the possible actions that can be done, and whether there are any limitations on performing those actions. RBAC is one of the popular authorization models in which permissions are granted according to predefined roles within the Organization (Muhammad et al. 2024).
- **Access Management:** The main goal of this procedure is to ensure centralized control over the whole life cycle, from user account provisioning through to deprovisioning and monitoring regarding the user's activities. This will involve ensuring users are granted access strictly to the resources necessary for their legitimate performance of assigned tasks and that access is promptly revoked upon change due to their role or employment status (Muhammad et al. 2024).

Figure 1 Displays the Identity and Access Management

Problem Statement

With the escalating number of security breaches that are considered serious, in May 2021, the U.S. President signed an executive order that compelled Federal Agencies to implement Zero Trust principles as described in NIST Special Publication 800-207 and

incorporate them as a key element of their Zero Trust security strategies (Weinberg & Cohen, 2024). The standard was the result of extensive coordination and included contributions from a very diverse set of stakeholders, including commercial customers, vendors, and a wide range of government agencies (Weinberg & Cohen, 2024). It has thus been widely adopted as a de facto standard by private organizations to secure enterprise environments. These principles advocate for continuous monitoring and adaptive authentication, as well as leveraging collected data to provide context for access requests and to improve security.

Research Objectives

The chief objective of this research objective is to explore how AI can reinforce the Zero Trust security framework in the face of complex and unique challenges that are imposed on U.S. defense networks. This study intends to develop adaptive models of Zero Trust that would effectively implement AI and ML techniques returning dynamic threat detection, real-time user behavior analytics, and context-aware access control. This research, therefore, seeks cybersecurity resilience through the integration of AI-driven automation and decision-making capability to make access to critical defense resources seamless and safest against sophisticated cyber threats.

Zero Trust Model

Ashfaq et al. (2023), asserted that Zero Trust Architecture is an emerging paradigm in organization cybersecurity, wherein organization cybersecurity is based on zero trust. It primarily prevents data breaches and lateral movement inside the networks. Zero Trust, or ZT, is not a framework per se but a set of guiding principles on how to enable workflows, system design, and operational practices. These enable enhanced security across various classified and sensitive systems. Gudala & Shaik (2023), argued that the concept of ZT is a complete change in security philosophy that works on the maxim "never trust, always verify." Unlike traditional models based on the assumption of everything within the corporate firewall being secure, ZT assumes a breach and validates every request as if it came from an untrusted network. The term "Zero Trust" was first mentioned in 2010 by an analyst from Forrester Research Inc., further interest in implementing this within the tech industry was sparked by Google's ZT security implementation in their network.

The model dismisses the very concept of secure network perimeters by asserting that no boundary is safe by default. Also, all users, whether inside or outside the organizational network, would be stridently authenticated, authorized, and continuously validated. With an understanding of traditional network edges disappearing, ZT meets resources wherever they are situated on-premise, in the cloud, or hybrid (Moresi, 2023). This framework addresses these growing remote workforces, hybrid cloud architectures, and ever-evolving threat landscape by enforcing security policies based on context, employing least-privileged access controls, and requiring rigorous user authentication to maintain a robust security posture. Zero Trust works on several principles that are in close relation to NIST 800-207 stipulations:

- **Continuous Verification:** This is a principle of continuous verification of accesses from any user, irrespective of his or her location to any resource. It ensures that only authorized persons are allowed entry at any particular instance (Moresi, 2023).
- **Decreasing the Blast Radius**: Zero Trust works to contain the consequence of a breach, whether it's an external or internal breach. This is done by segmenting resources and compartmentalizing access thereby reducing what could be compromised in case any security incident occurs (Moresi, 2023).
- **Automated Context Collection and Response:** This means that Zero Trust relies on data-driven decisions and not assumptions. It automatically gathers data on behavior across the entire IT environment, needed for real-time responses to security threats in context (Moresi, 2023).

Of importance in the Zero Trust Model is the context collection and response. In this regard, real-time contextual information about a user or system behavior should be gathered, including real-time device details, user attributes, and network conditions. Context is really important in ZTM as it facilitates decision-making. A simple example would be that when an endpoint tries to access financial data, context will determine whether the request is from a valid employee or a threat. The device's location, user identity, and data being accessed provide substantial context. What is missed, though, is whether the employee should have access to that particular data from that device or location (Ghasemshirazi et al., 2023). That's the missing piece: context. Without context, a risk assessment will not be complete, and different teams might interpret and respond to it differently. Another important development in Zero Trust security is the publication by the U.S. Cybersecurity and Infrastructure Security Agency of the Zero Trust Maturity Model, or ZTMM. It offers a structured method for the evaluation and development of an organization's Zero Trust capabilities (Moresi, 2023). The ZTMM encompasses five major pillars, each dealing with a particular core aspect of the implementation of Zero Trust:

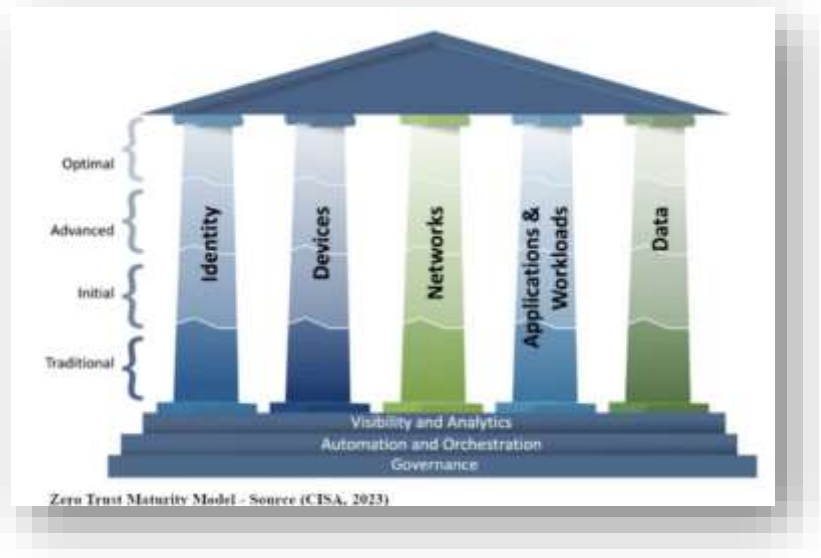

Figure 2: Exhibits the Five Pillars of the Zero Trust Model

By referring to Figure 2 above about the five pillars of the Zero Trust Maturity Model, identity describes attributes that uniquely identify an agency user or entity, including non-person entities. Device describes the set of assets Capable of network connection (hardware, software, and firmware) Network is an open communications medium including internal networks, wireless networks, and the Internet. Applications and workloads refer to systems, programs, and services executed across different environments. Data include structured and unstructured files that reside in systems, devices, networks, and backups. Each pillar also supports Visibility and Analytics, Automation and Orchestration, and Governance (Munir et al., 2023). Visibility and Analytics refer to the observable artifacts resulting from enterprise-wide events and cyber-related data analytics. Automation and Orchestration is the utilization of automated tools and workflows for security response capabilities while ensuring oversight and security. Governance enforces the policies and processes of cybersecurity across pillars to mitigate risks. The levels of maturity are categorized into four: Traditional is about manually configured lifecycles, static security policies, and Manual response and mitigation. First is the initiation of automation of attribute assignment, configuration of life cycles, policy decisions, and enforcement with initial cross-pillar solutions (Munir et al., 2023). Advanced is applied to Automating the controls, including lifecycle and configuration assignment, with cross-pillar coordination. Optimal refers to From fully manual to full automation, just-in-time life cycles, and attribute assignments based on automated or observed triggers.

User Behavior Analytic

Paul (2023), indicated that User Behavior Analytics- represents a security practice that includes the process of continuous monitoring and analysis of the pattern of activity by users. UBA employs machine learning algorithms to establish baselines for normal user behavior based on a multitude of factors. These factors can include login times, geographic location, device characteristics, applications accessed, data files opened, and network resources utilized. By analyzing historical data of user activity, ML algorithms can learn the typical patterns associated with each user's account. This established Baseline serves as a benchmark for identifying potential anomalies that deviate from the user's customary behavior. These baselines can then be used to highlight deviations that may reflect potential security incidents that require Ku-ther investigation. For example, a login from an unusual geographic location at an unrecognized time of day may trigger an alert for potential unauthorized access. Similarly, a significant increase in the number of files accessed, and the volume of data transferred/downloaded by a user account may suggest the existence of a malicious actor. Trying to exfiltrate sensitive information. UBA allows organizations to detect and mitigate threats in real-time, well before they become major security incidents. This proactive approach towards security significantly empowers Identity Access Management in zero-trust environments (Munir et al., 2023).

Adaptive Authentication

Talukder et al., (2023), reported that Adaptive authentication is a form of access control where the level of authentication adapts depending on the estimated risk score related to the specific access attempt. This approach customizes security to contextual requests. This could mean that logging in from an unknown location or device automatically initiates a stronger factor of authentication, such as multi-factor authentication, whereas access through a trusted device on the corporate network would

only require a simple username and password combination. In this way, a risk-based approach enhances security when the risk is high while not making everyday access more complicated.

Existing Studies on A1-powered Identity and Access Management & Zero Trust

In 2010, Kindervag, an analyst at Forrester Research, came up with the concept of Zero Trust Network Architecture, or ZTNA, and spelled out ways for its implementation in real environments. Paul (2022), provided an overview of the existing foundational ZTA models and suggested key logical components for its framework. This work focused, largely, on the practical implementation of Zero Trust and how to apply it in the real world. Zero Trust is, at the heart of it, a paradigm shift in cybersecurity strategy strategizing based on location to a more data-centric approach. This allows more hard-core enforcement of security for users, systems, data, and assets that are dynamic by nature.

AI-driven Identity and Access Management represents one of the fastest-developing areas of research within Zero Trust security. Many have considered how AI could benefit IAM by discussing some perceived advantages that might arise from AI for IAM functionality. Shaik et al. (2023), for example, described a use case of machine learning to identify anomalies in user behavior. These findings suggest that suspicious activity can be identified with the help of machine learning algorithms, thereby enhancing the accuracy of threat detection in Zero Trust environments. Another recent work by Ashfaq et al. (2023) has focused on AI for adaptive authentication in cloud computing environments. It shows how AI will adapt authentication protocols according to user context and risk profiles to enhance security without compromising user convenience. On the other hand, embedding AI into IAM systems also triggers a series of challenges.

Meanwhile, Muhammad et al. (2022), underscored the need to take into consideration the biases of each AI model in the process of analyzing user behavior. Furthermore, private and secure protection of users' data is considered to be handled via AI algorithms. This research extends the literature in that the theoretical underpinnings and the practical implication of A1-powered UBA and adaptive authentication within the Zero Trust security framework are shown to provide detailed insights on potential benefits and challenges.

AI in Identity and Access Management (IAM):

The core principles of implementing Zero Trust Architecture (ZTA) revolve around authentication and access control. These mechanisms verify a user's identity and determine their permissions for performing specific actions on protected resources. The purpose of this process is to transition a user from an unidentified to an identified state. In the dynamic world of cloud computing, IAM systems that are robust are highly sought after with the rise in cybersecurity threats and intricacies associated with managing digital identities (Munir et al., 2023). Organizations are thus integrating state-of-the-art technologies that factor into IAM strategies, given the frequency of data breaches or complex cyber-attacks. Of the lot, AI is emerging as a game-changing force, enabling machines to learn, adapt, and generate insights. AI in the IAM space is going to be particularly critical in cloud environments, further shaping the building and deployment of models involved in generative AI. These capabilities will automate policy creation, improve many other security measures, and redefine the IAM landscape. The complexities of network interaction then become obvious, hence allowing IT departments to introduce sagacious administrative measures and make better-informed decisions concerning user licenses. IAM is based on four cornerstones: Authentication, Authorization, Administration, and Audit. Each cornerstone plays a very important role in the creation of a secure and effective access management system (Joshi., 2024).

User authentication

Authentication focuses on verifying user identities, and ensuring that only authorized individuals can access the system.

Adaptive and Continuous User Authentication

According to Yang et al. (2023), this protocol involves the tracking of users' behavior during a session and requests for re-authentication in the case of observation of an anomaly. A process that begins with the modeling of a user's behavior concerning interaction with devices over a predefined period. Then, data pre-processing takes place, stored in a dataset containing information regarding a user's behavioral pattern. This procedure simply selects a few distinctive features in multidimensional space, including sensor activities, application usage, communication patterns of the phone, and screen gestures toward formulating a correct profile. Lastly, the current usage is matched with the established behavioral profile in its dataset storage. AI-powered adaptive and continuous user authentication integrates behavioral biometrics, anomaly detection, and UEBA (Munir et al., 2023). Figure 3 brings out the steps in AI-driven adaptive and continuous user authentication.

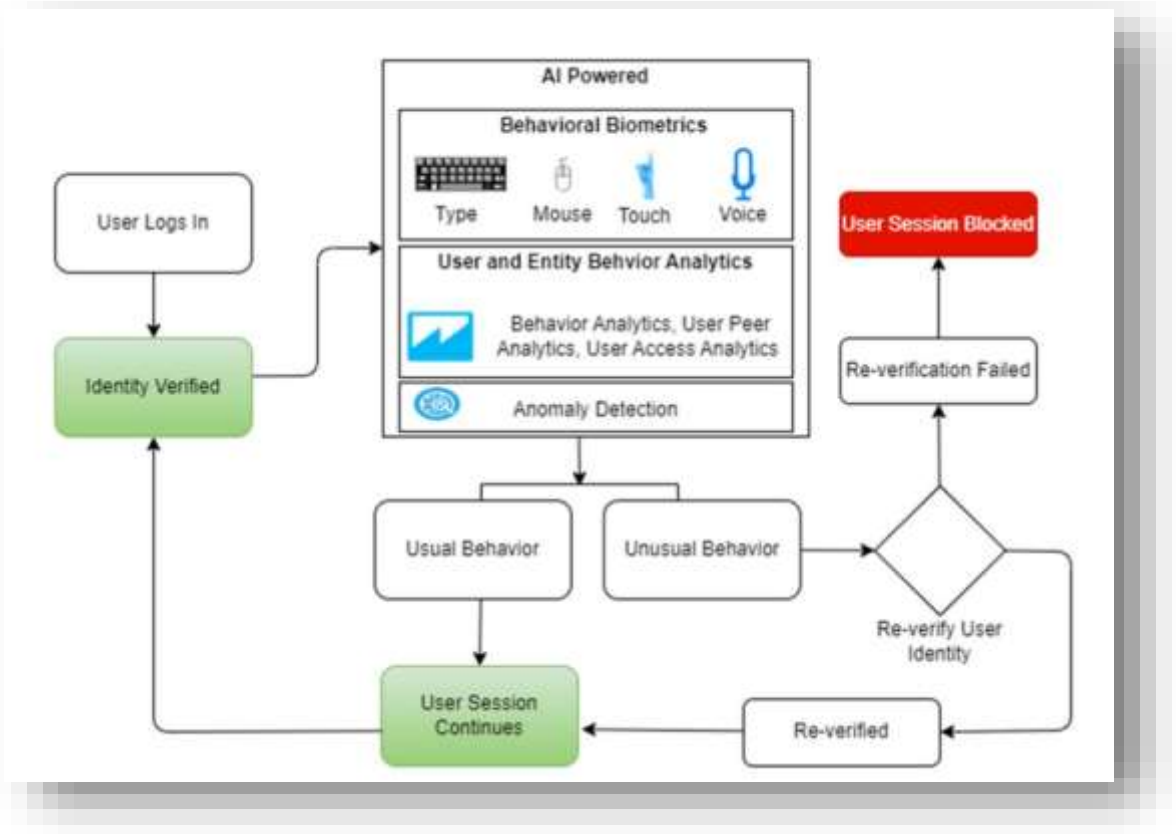

Figure 3: Depicts the Adaptive Continuous User Authentication

Fig. 3 displays Adaptive and continuous user authentication. The AI-powered system verifies the identity of users upon login and then continuously tracks the behavioral anomalies during the session. Behavioral biometrics would identify small differences in activities such as the way a user types, moves the mouse, holds the phone, or interacts with touchscreens. User and Entity Behavior Analytics (UEBA) aggregates data from a wide range of enterprise sources, including firewalls, routers, virtual private networks (VPNs), identity access management systems, antivirus and anti-malware tools, endpoint detection and response (EDR) solutions, security information and event management (SIEM) systems, active directory logs, and threat intelligence feeds. If the anomaly detection system recognizes a major violation of its predefined behavior baselines in real-time, then it will require the user to re-establish their identity. If the re-establishment of identity fails to verify, then the session shall be terminated and the access blocked.

Voice and Speech Recognition

Voice authentication relies on biometric technology for its backbone, which authenticates users based on distinctive features of their voice. A1 can learn the voice patterns of individual users, creating a model that improves accuracy in voice-based authentication and provides better resistance against spoofing. A1 and ML can process big datasets and thereby increase efficiency by autonomously learning and adapting to changes in the environment (Yang et al., 2023). It can be trained to differentiate between different accents, dialects, contexts, and emotions. They can also better deal with complex and multi-dimensional data, which is necessary for tasks related to data mining and machine learning.

Facial Recognition

As per Yang et al., (2023), facial identification is a technology-based process for identifying people by mapping face features from images and videos. It works by comparing the mapped facial characteristics against images in a database to establish a match. Facial recognition finds wide applications across a wide spectrum of industries: in airports, on smartphones, in classrooms, on social media platforms, and in businesses. Some organizations have even swapped traditional security badges for a facial recognition system. AI plays a huge role in improving the facial recognition technique by facilitating the development of higher-order systems that generate and analyze facial data to identify and authenticate users accurately based on unique facial features.

AI-Driven Anomaly Detection

According to Shaik et al., (2023), AI-powered anomaly detection depends on the role of artificial intelligence and machine learning algorithms in detecting abnormalities in data that differ from predetermined patterns. Machine learning-based anomaly detection considers the normal behavior patterns in unlabeled data. The anomaly identification is done through k-means clustering, isolation forests, and one-class SVM that flag the deviations as potential threats. Within the online security arena, AI-powered models are employed to identify and resolve threats in a much more proactive manner. Such systems provide for the real-time monitoring of user behavior and detect unusual patterns that could signal a security risk or account compromise.

AI in Multi-Factor Authentication.

Multi-factor authentication boosts security by adding more verification layers. In addition to a basic form of authentication, like a password, MFA entails sending a one-time, password, also referred to as an OTP, is forwarded to the email or mobile phone of the user. Since this OTP uses a time factor in its creation, it would ensure that at least two factors in authentication have indeed been correctly verified (Yang et al., 2023). MFA is the various authentication principles applied in the login considerations to a system through multiple devices by gathering enough evidence to verify that a user is who they claim to be.

Adaptive Multi-Factor Authentication (AMFA)

As per Yang et al., (2023), AMFA is a technique for deducing, with the help of contextual information and business rules, which determines which of the authentication factors to use with a particular user in any given circumstance. Adaptive Authentication is often used in conjunction with MFA and single sign-on (SSO solutions). AMFA solutions, powered by A1, monitor the activities that users perform over a period to identify the pattern, create baseline profiles of users, and detect anomalous behavior. Adaptive authentication considers the following factors:

Profile Device- It assesses the system from which the request originates.

- **Location awareness**: This involves assessing the request's source, including whether it comes from an IP address range associated with risk or from a potentially risky country.
- **User behavior**: Understanding the intention of the user's server, application, or data access. AMFA assigns risk scores to suspect events and adjusts authenticating factors in real time based on administratively defined policies.
- **Low-risk behavior:** Users can log in by using their username and password only.
- **Medium-risk behavior**: Users require an additional code via SMS for verification purposes.
- **High-risk behavior Users**: Must provide further information to complete Authentication and then proceed to authorization.

Figure 4 illustrates the steps involved in AMFA. AMFA performs the fundamental role of enterprise security enhancement by allowing business access to only authorized users.

Applications and data. Importantly, it minimizes challenges for the users who show expected Behavior patterns.

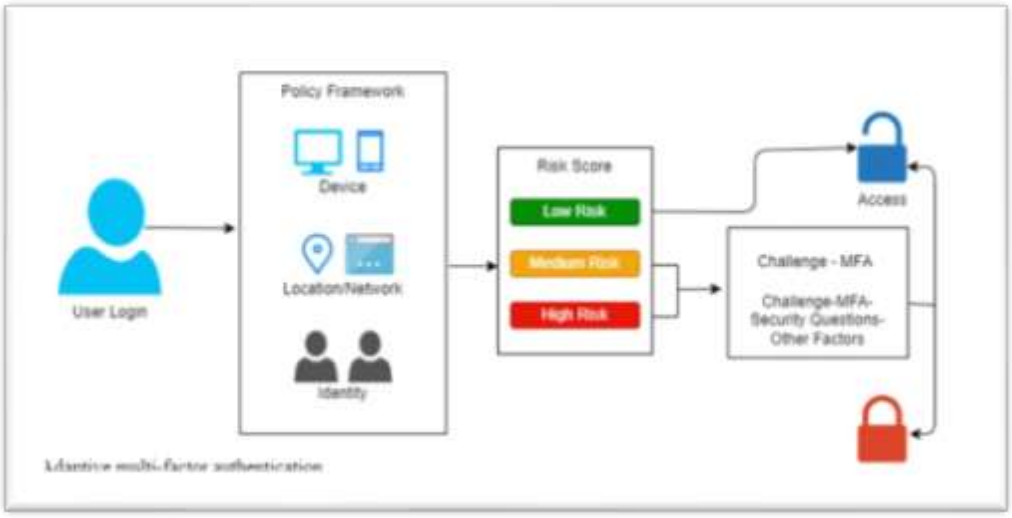

Figure 4: Portrays Adaptive Multi-Factor Authentication

Fig 4 depicts Adaptive multifactor authentication. During a login event, the system looks at the device from which it would extract information such as the origin of the request, the location of the request, the IP address for the request, and the intent of the request. It compares this information with the user's base profile and returns risk scores. In case it's a low-risk behavior, then it lets him log in with only a username and password. In the case of medium-risk behavior, the system asks for additional authentication through the means of an SMS code. If it identifies high-risk behavior, seek additional information. The user logged on with low-risk behavior, medium-risk behavior, and attempted with High-risk behavior. The user did not provide more detailed information, and access was blocked.

AMFA reinforces the ZT model to:

- **Contextual verification**: This protocol monitors device profiles, location awareness,

and user behavior. ZT assumes that there are attackers both inside the network and outside the network perimeter. AMFA prevents unauthorized access even when valid

credentials are compromised. Through constant verification of identities, it reduces the impact of Compromised Accounts(Yang et al., 2023).

- **Risk-based Authentication:** Dynamically adjusts authentication based on risk scores

requirements.

- **Biometric and token authentication**: These factors enhance identity validation (Yang et al., 2023).
- **Location-agnostic access**: From any location and irrespective of the network of origin, AMFA ensures secure access to services (Yang et al., 2023).
- **Scalability and cloud readiness:** AMFA scales consistently across different endpoints,

including cloud-based machines, software-as-a-service applications and

Personal devices.

Benefits of Integrating AI-Powered Behavioral Analytic

Improved Threat Detection. AI-powered User Behavioral Analytics can detect minor anomalies in users' behavior, which may have been altogether ignored by traditional-based security systems. This proactive approach to security equips the organization with the ability to identify and mitigate threats before they escalate into major security incidents (Talukder et al., 2023).

Real-Time Threat Response. AI can analyze user behavior in real-time, allowing

organizations to respond to potential threats quicker and more effectively. This minimizes the potential damage a security breach can cause (Talukder et al., 2023).

Reduced False Positives: With the power of advanced ML algorithms, A1 can

distinguish between normal user behavior and that which is hilly anomalous. This leads to a significant reduction in false positives as compared to conventional signature-based detection methods.

Improved Security Posture: Through proactive identification and mitigation of threats, AI-powered User Behavioral Analytics strengthens an organization's overall security posture. This translates toward a more secure environment for users and the protection of data (Talukder et al., 2023).

Strategies of Implementation:

Following are the ways organizations can use different strategies in choosing their AI-powered Identity Access Management (IAM) solution:

- ✓ **Proof of Concept (POC):** Initiate a POC to understand the feasibility of AI-powered IAM and its effectiveness in your environment. This helps in pinning possible challenges and fine-tuning the implementation strategy before a full-scale deployment is undertaken.
- ✓ **Phased Approach:** Identity Access Management with AI capabilities should be brought in a bit piecemeal manner, targeting a specific use case like User Behavioral Analytics. This endeavor makes the adoption and troubleshooting easier whenever there is an issue.
- ✓ **Integration with Existing Systems:** Each solution selected should integrate easily with the current IAM and security infrastructure to avoid disruption and ensure a non-disruptive implementation process.

- ✓ **Focus on User Experience:** Any deployment should balance increased security with user convenience. Tailor AI-driven access controls to align with specific risk profiles, maintaining a positive user experience.

Conclusion

Retrospectively, the most fundamental change in Identity Access Management involves the integration of zero-trust security principles with artificial intelligence. This research has deeply explored how AI-powered Identity Access Management can improve security, facilitate efficient access control processes, and further the cause of security posture for organizations. Key functionalities researched in-depth include User Behavior Analytics to finetune anomaly detection, adaptive authentication to empower dynamic, risk-based access control, and user provisioning and access lifecycle automation. AI-powered systems can tell what is legitimate user behavior and what may be a threat with increasing accuracy by taking user context data, machine learning algorithms, and continuous learning into consideration. Further, adaptive authentication dynamically adjusts the impediments to access by checking risk, therefore hedging a more balanced position between security and user experience. Automation increases efficiency because it minimizes human error and eases administrative tasks associated with the management of users.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Ashfaq, S., Patil, S. A., Borde, S., Chandre, P., Shafi, P. M., & Jadhav, A. (2023). Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis. *Journal of Electrical Systems*, *19*(2).
[2] Chirra, D. R. (2024). AI-Augmented Zero Trust Architectures: Enhancing Cybersecurity in Dynamic Enterprise Environments. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *15*(1), 643-669.
[3] Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, Challenges, and Opportunities. *arXiv preprint arXiv:2309.03582*.
[4] Gudala, L., & Shaik, M. (2023). Leveraging Artificial Intelligence for Enhanced Verification: A Multi-Faceted Case Study Analysis of Best Practices and Challenges in Implementing AI-driven Zero Trust Security Models. *Journal of AI-Assisted Scientific Discovery*, *3*(2), 62-84.
[5] Joshi, Hrishikesh. "Emerging Technologies Driving Zero Trust Maturity Across Industries." (2024).
[6] Moresi, G. (2023). *Zero Trust Network & Zero Internet: Defense Strategies Against the Zero Day Kill Chain*. Gianclaudio Moresi.
[7] Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), 99-135.
[8] Munir, M. S., Proddatoori, S., Muralidhara, M., Saad, W., Han, Z., & Shetty, S. (2024). A Zero Trust Framework for Realization and Defense Against Generative AI Attacks in Power Grid. *arXiv preprint arXiv:2403.06388*.
[9] Paul, F. (2022). The Role of Artificial Intelligence in Enhancing Zero Trust Security.
[10] Shaik, M., Gudala, L., & Sadhu, A. K. R. (2023). Leveraging Artificial Intelligence for Enhanced Identity and Access Management within Zero Trust Security Architectures: A Focus on User Behavior Analytics and Adaptive Authentication. *Australian Journal of Machine Learning Research & Applications*, *3*(2), 1-31.
[11] Talukder, S., Alam, S., & Bhowmik, P. K. (2023). *Developing an AI-Powered Zero-Trust Cybersecurity Framework for Malware Prevention in Nuclear Power Plants* (No. INL/CON-23-75326-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (United States).
[12] Weinberg, A. I., & Cohen, K. (2024). Zero Trust Implementation in the Emerging Technologies Era: Survey. *arXiv preprint arXiv:2401.09575*.
[13] Yang, L., El Rajab, M., Shami, A., & Muhaidat, S. (2023). Diving Into Zero-Touch Network Security: Use-Case Driven Analysis. *Authorea Preprints*.