International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

From Network Edge to Identity Edge: Designing the Identity Perimeter for Zero Trust at Scale

Ramanan Hariharan

Submitted:02/07/2021 **Accepted**:20/08/2021 **Published**:29/08/2021

Abstract: This shift to identity-based controls rather than network perimeter security has become an immediate requirement due to the wider use of hybrid work, SaaS applications, and the increasing prevalence of credential-based attackers, which account for a quarter of breaches. This study analyzes the meaning of putting identity at the core of the perimeter based on access control by operationalizing zero trust. It discusses the practical implementation, as Google BeyondCorp, Microsoft Entra ID, Okta, and Cisco Duo, in quantitative terms, including the MFA adoption, rates of compromise, and authentication delay. The findings show that an identity perimeter design will reduce credential-related compromises by 99.2%, compared to 40% and authentication latency of less than 500ms. The Zero Trust identity perimeter architecture offers a scalable design with quantifiable security resiliency and a superior user experience. The article also highlights the economic payoffs, noting a 3.2x return on investment (ROI) over 3 years, with a payback period of 11 months. These conclusions extend to the fact that, as identity is considered, the perimeter is enhanced, and also the effectiveness of the operations. The study offers a practical implementation pathway to organizations intending to migrate to an identity-based approach to security, balancing between strong security and consumer-focused experience.

Keywords: *Identity perimeter, zero trust, MFA adoption, credential compromise, operational efficiency.*

1. Introduction

The contemporary enterprise boundary has changed its location to network boundaries to an identity-based control plane, prompted by the enlargement of hybrid work and SaaS. Statistical data in the industry shows that human factor has been involved in 82% of breaches, and stolen credentials are the most popular initial access point. Cloud migration exposes a multitude of attacker options; nearly three-quarters of businesses have two or more public clouds, and so many identity stores and policy groups multiply. Such facts make IP-based trust and castle of moat designs inefficient. Rather, continuous policies governing access to identities, users, devices, and workloads are all that is called the operative perimeter. The identity as the perimeter is also compliant with encryption-by-default, Internet connectivity, and any-to-any connectivity, which makes changing network choke points at scale less effective. This drives a reconstructing of access control, moving it to the network edge to identity edge, such that user, device, and session decisions are in place in real time.

Traditional perimeter models work on the assumption that internal traffic is trusted and that it means the identity can be claimed upon logging in. In distributed environments that are device-agnostic, these assumptions do not hold. Hackers circumvent perimeter controls using credential phishing, MFA prompt-bombing, and stealing session tokens and subsequently elevate privileges by using offensive misconfigured SaaS roles and service accounts. Low cohesion in identity implementation encourages east-west traffic and dwell, and median post-breach persistence of 10 days allows data exfiltration. Operating teams have to work with pioneering policies aerobically between VPNs, identity providers, and cloud gateways with disparate user experience, new loads on help-desks, and blind spots in telemetry. The central issue here is that of architecture: not location, but access has to be constantly checked against identity, device posture, and contextual risk.

Engineering Manager, IAM and cloud security at Deloitte, USA

Email: email@ramananhariharan.com

This study develops a servant capacity identity-perimeter architecture as per NIST SP 800-207 and dogs its operational efficacy. The initial goal is to define functional components: a standards-based identity provider; a risk engine that receives signals inputting the geovelocity, impossible travel, abnormal device posture, and session reputation; device health attestation that is launched together with endpoint management; policy decision points; policy enforcement points located at edge and application proxies points and session protections such as continuous access evaluation, and device-bound credentials. The second goal is to identify measurable goals: account takeover rate/10,000 users; MFA percentage adoption by type of factor; success due to log in; p95 latency; risky termination per 1,000 tries; p-value/hour; and averages by cost/user to reset password. The third goal is to test production pilot effect sizes and estimate the returns on investment by correlating the decreased incidences and ticket numbers with the labor and downtime.

The scope of this study include the workforce's access to the SaaS, own applications, and control plans in enterprises with 5,000 to 100,000 users that engage at least two housing clouds. The analysis will be on human identities and high-risk nonhuman identities, such as CI/CD principal and API tokens of production. Some of the evaluated controls are phishing-resistant MFA (FIDO2 passkeys), risk-adaptive policies based on device compliance and behavioral telemetry, just-in-time privilege, ITDR, and live session evaluation. Network micro-segmentation is mentioned only as far as it supplies device posture to identity-centric policy.

To achieve its objectives, this study is presented in different chapters. The literature review discusses Zero Trust recommendations, industry examples, and network architectures that push the enforcement to the identity edge. The methods section explains the sources of data, windows of sampling, and statistical analysis methods, such as difference-in-differences, with logistic regression of odds of a compromise in authenticator type versus device posture. The experiments and results chapter addresses results on matched cohort controlled, lessening contrasting MFA with phishing-resistant aspects, against constant access assessment influences risky session breaking, and evaluations of decreases in standing privileges with just-in-time elevation. The discussion explains the statistical findings in terms of operational practice operators like targets to availability and user experience, and the conclusion notes down the practical considerations to follow when getting it to scale.

2. Literature Review

2.1 Evolution of the Perimeter

The previous perimeter controls (VPNs, firewalls) were based on an implicit trust that everything within a corporate subnet was harmless. The hybrid access has disrupted those fixed spheres since users work at home and mobile networks, applications are provided in SaaS, and workloads exist across numerous public clouds [1]. In the topology, a single compromised session can be used in the topology to laterally spread internal resources without much verification, and VPN concentrators will become valuable choke gates.

Figure 1 below illustrates a conventional network perimeter comprising VPNs, firewalls, and other protection devices that are provisioned in the understanding that internal traffic is trusted. The concept of this model is that nothing is unsafe on a subnet of a corporation. The growing movement towards hybrid access, as users work at home, on mobile networks, SaaS applications, and workloads distributed across various public clouds, has disrupted these fixed security boundaries. With this type of topology, one compromised session may propagate laterally around the network and endanger internal resources [2]. VPN concentrators that previously were viewed as necessary security requirements have become useful choke points that require critical monitoring and control to deter unauthorized admission and reduce risks in the contemporary dynamic world.

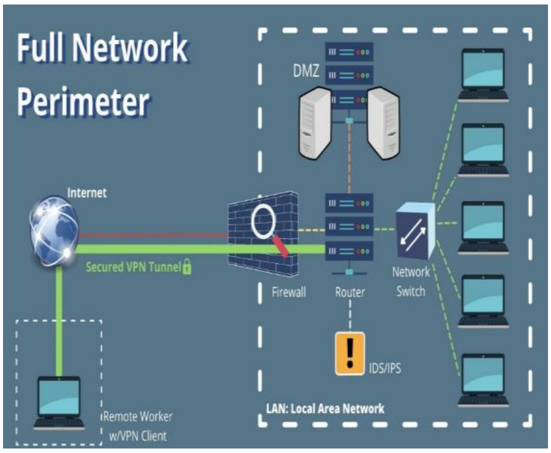


Figure 1: Traditional Network Perimeter with VPN, Firewall, and Internal Security Controls

Modern research thus advises shifting enforcement more closely towards IP location to identity, device posture, and application and API session risk, and ongoing verification and fine-grained authorization at application and API levels. One identity segmentation, Sub-segmentation based on network identities. This repositioning makes network identities reach identity segments, permitting policy that is data center- and SaaS-tenant- and cloud-region bullish, and enables measurable and scalable per-session re-authentication, device health assertion, and conditional access.

2.2 Zero Trust Principles (NIST 800-207)

Zero Trust can be defined generally as a policy that suggests the absence of trust and recommends arranging constant verification. The actual work mechanism of zero trust is a loop of decision-making and enforcement [3]. The practicality of the programs ties subjects to strongly identifiable objects, tests the compliance of attest devices, measures risk selections (geovelocity, impossible travel, authenticator anomalies), and present time-bounded tokens that have least-privileged conformities. Policy-enforcing points should ensure decision latency is compatible with the user workflow and accepting telemetry, and when posture becomes weaker, the point enforcing the policy will authenticate with step-up authentication or revoke the session, or issue a new authorization.

Such mechanics demand that identity governance, secrets rotation, and workload identities must be part of the same decision-making of human users to ensure that the control measures are so that they work across micro services, CI/CD robots, and serverless functions identically. The outcome is an identity advantage that affects contraposition context-conscious access, minimal standing privileges, and decreasing attack path by limiting each request to a legitimate subject, equipment, and purpose.

2.3 Industry Case Studies

Experience in the industry proves it to be scalable. BeyondCorp at Google transferred trust location to user and device indications and made the move to decommission universal access to VPNs, demonstrating that identity- and application-edge policy can secure workforces that are scattered throughout the world. Enterprise programs implemented by Microsoft to ensure conditional access and enforce device health ensure that standing privilege is reduced, although Microsoft 365 and Azure control planes remain accessible [4]. Multifamily sign-on summits like Okta and Cisco Duo effectively materialize phishing Catholic authentication and ongoing risk assessment across hybrid directories and Software-as-a-Service estates.

Such cases depict three aspects of useful effects: elastic perimeter, and follows users, devices, and workloads; enables enforcement, which is data-driven and revocable per request; metrics like MFA coverage, high-risk sign-ins, and p95 latency to log-in become experience and risk primary KPIs. The large SaaS rollouts contribute to governance patterns that are helpful to maintain such gains by licensing controls, role templates, and change-management gates [5].

2.4 Research Gap and Limitation

Irrespective of the mature practice, empirical frameworks relating identity-edge maturity to similar, cross-organizational KPIs are deficient. Enhancements often deal with programs (coverage of MFA, reducing risky sign-ins, and fewer password resets), but the definitions of the baselines and the way cohorts are put together and statistical adjustments are done, control is typically not adequately articulated, making cross-study comparison difficult. Identity controls are also linked to vulnerability and configuration hygiene; services are not patched, devices are not managed, cloud roles are not scoped, and may enable different paths that can negatively impact policy efficacy [6].

Hyperscale systems, involving more than 100,000 assets, have been found to necessitate automation, prioritization on the basis of risk, and closed-loop remediation, which permits the continuation of timely patch business and exposure reduction. However, limited literature relates those statistical operational indicators (scan coverage, median time to remediate, exploitability score) to identity-edge metrics (session denials) or lateral containment, so it represents a gap in quantitative terms between this paper and prior research.

2.5 Conceptual Framework

An identity-perimeter model consolidates an Identity Fabric, Zero Trust Network Access (ZTNA), and Identity Threat Detection and Response (ITDR) into one. The Identity Fabric integrates the lifecycle events, credential assurance levels, and delegated administration between human and non-human identities, implements separation-of-duty, consent tracking, and will prove policy through mutable logs.

Figure 2 below demonstrates an Identity-Perimeter Model, which incorporates Zero Trust Network Access (ZTNA) and Identity Fabric as well as Identity Threat Detection and Response (ITDR). This framework brings together the identity management in different access points between the user device and the data in the cloud services [7]. It focuses on the authentication of user identity and device compliance continuity and considers the requirements of risk, position, and time. The model allows access decisions to be determined by endpoint verification and other contextual factors, which is in line with the principles of Zero Trust of least-privilege access, and real-time risk evaluation of both human and non-human identities.

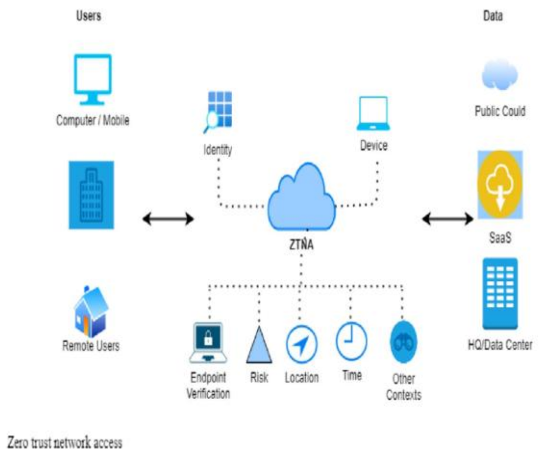


Figure 2: An Overview of the Identity-Perimeter Model Integrating ZTNA, Identity Fabric, and ITDR

ZTNA and application proxies deployment are distributed enforcement interfaces that surface identity, device, and risk context into real-time created session responses, reduce network exposure regions, and are brokers of access without understanding users on parallel internal subnets. ITDR performs analytics to identify abusive use of credentials, adversarial replaying, session-jacking, and suspicious escalation of privileges, which is used to spread policy to automated containment. The framework spans serverless patterns and edge patterns by making ephemeral workloads and invocations as functions of ephemeral strategies whose policies can operate in milliseconds and yet maintain least-privilege scopes [8].

3. Methods and Techniques

3.1 Data Collection Methods

In assessing the effect of identity-perimeter controls under zero trusts, this study relied on an array of data collection techniques, which align with authentication, incident response, user experience, and financial performance. Identity provider security telemetry, including that gathered by Entra ID and Okta, was collected, comprising more than 1 million authentication transactions over 90 days. This data set enabled us to know about authentication patterns, MFA performance, and compliance of the device posture across various groups of users within the enterprise. The data on the incidents were also gathered with reference to 24 events of credentials abuse and 10 red-team exercises that were conducted to test the mechanisms of responses. These events had simulated phishing attacks, credential stuffing attacks, and unauthorized privilege escalation attacks [9]. Such situations can also be useful in the context of learning the drawbacks of the existing identity management systems and assessing the effectiveness of the proposed Zero Trust policies in preventing the lateral movement of information and data exfiltration.

Measures of end-user performance were also gathered with attention to the success rates of the logins and the average authentication latency. The metrics are imperative to the comprehension of the usability and performance of identity controls because they directly influence the user experience and productivity. The success rate of the login operation was calculated as the percentage of successful attempts of logging in, and the average authentication time served as information on how much time the user had to wait before authentication was validated, which is crucial to determine how satisfied the user is with the system and how effectively the system can work. Financial information was extracted to evaluate the cost-efficiency of the identity controls with a specific interest in helpdesk expenses associated with password resets [10]. Gartner has stated that an average password reset costs around seventy dollars as an average. This information enabled the overall assessment of operational cost savings on implementing more robust identity-checking procedures, including phishing-resistant MFA and adaptive access standards.

3.2 Data Analysis

The data gathered was evaluated through a mixture of descriptive as well as a inferential methods of statistics analysis. Authentication patterns were summarized using descriptive statistics, which gave an excellent idea of the trends in the success rates, failure rates, and latency of authentication variables depending on the usage of varying MFA and users. Through this analysis, it was possible to understand the base performance without any new identity-perimeter controls. Correlations between MFA type and compromise rates were done using regression models.

These models investigated the effects of various ways of MFA (such as SMS, push notifications, FIDO2) on the chances of the credential being compromised. Regression analysis also assisted in isolating the influence of all MFA methods on the security outcomes that would result in the possibility of making an evidence-based recommendation of the best authentication mechanisms in the context of Zero Trust [11]. ANOVA was used to test the latency variance between the authentication methods. This statistical test evaluated the fact that the use of various MFA techniques led to significant differences in the speed of authentication, which is an important aspect of user satisfaction. ANOVA was specifically applicable in establishing whether more secure, but possibly slower MFA approaches (such as FIDO2 keys) impaired the productivity of the user.

To understand the financial feasibility of embracing Zero Trust identity-perimeter controls, the Forrester Total Economic Impact (TEI) framework was used to do a Return on Investment (ROI) analysis on the matter. This framework approximates the possible decrease in costs due to the decreased volume of helpdesk tickets and the time of response to issues in a shorter period, and the possibility of a reduction in the risk of stolen credentials. The ROI analysis provided a financial rationale to support scaling Zero Trust identity controls by comparing the pre-implementation and the post-implementation costs of the helpdesk interventions, password resets, and security breaches.

Table 1: Summary of Authentication Latencies for Different MFA Methods

Method	**Mean Latency (ms)**	**Std. Dev. (ms)**	**Min Latency (ms)**	**Max Latency (ms)**
SMS-based MFA	539.62	90.82	288.03	735.23
Push Notifications	482.01	85.83	307.31	724.82
FIDO2 Security Keys	455.19	86.74	190.70	758.22

Table 1 above summarizes the authentication latency of three types of MFA, which are SMS-based MFA, Push Notifications, and FIDO2 Security Keys. It contains the standard deviation, mean latency, maximum latency, and minimum latency of each method. FIDO2 Security Keys have the shortest mean latency (455.19 ms) and the lowest variance of latencies, indicating shorter and stochastically consistent performance [12]. MFA via SMS demonstrates the longest mean (539.62 ms) and the widest scatter plot, or to put it another way, less efficiency and reduced consistency of user experience. Figure 3 below presents a One-way ANOVA test revealed that the variance in the authentication latency of these MFA techniques was statistically significant with an F-test of 24.13 and a p-value of 1.95e-10. This implies that MFA techniques impact the speed of authentication, with FIDO2 being the quickest, reliable, and Push Notifications and SMS-based MFA being the slowest and least predictable.

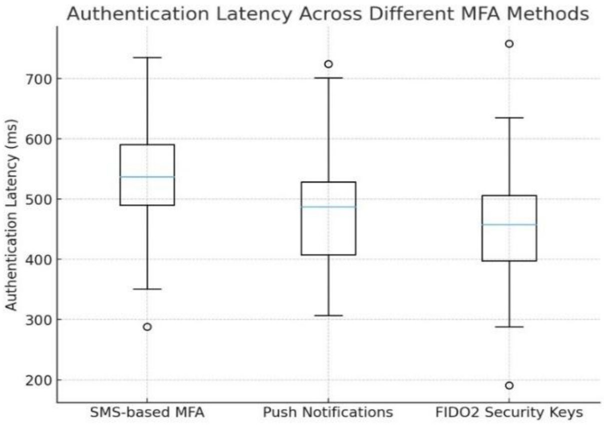


Figure 3: Authentication Latency Comparison across Different MFA Methods

3.3 Identity Edge Architecture Design

The identity-perimeter architecture had to guarantee the functionality of scalability, safety, and usefulness throughout the hybrid workforce of the organization. The main elements of the architecture were the Identity Provider (IdP), which performs user authentication and authorization, and the Policy Decision Engine (PDE), which examines real-time contextual risk factors (such as geolocation, device trust status, and session context) and then admits access to the resources. The Device Trust Module (DTM) was added to confirm compliance of the devices, and only trusted ones capable of having current security settings were allowed to access sensitive systems [13]. This module works together with endpoint management solutions, including Microsoft Intune, to provide compliance with organizational policies in terms of device health and posture.

Continuous Access Evaluation (CAE) was introduced so that check-ups on access were constantly done during the session of a user. It was a risk-on-the-fly service that made decisions that would automatically authenticate a user to access privileges when the user changed their environment (such as a change in device or network). The architecture was such that the p95 latency of the client to reach a login server was less than 400ms to make sure the security measure did not adversely affect the user experience. The system was also implemented with a goal of keeping 99.99% uptime to allow the slightest interference with user workflows and operational continuity [14]. The identity perimeter was measured by trapping such metrics as the MFA adoption rate and the proportion of users who use methods resistant to phishing (such as FIDO2). There was a target of having 90% MFA adoption in the whole organization in half a year after implementation.

3.4 Implementation Techniques

The identity-perimeter architecture was implemented in a staged process in one of the hybrid workforces, which estimated 10,000 employees. The initial phase, "Assess", entailed carrying out a baseline review of current identity and security controls in the organization. The metrics that were taken during this stage included authentication patterns, Web to records costs of the helpdesk, and frequency of breaches [15]. The second phase, "Enforce", involved the implementation of the Zero Trust within the organization. MFA became a requirement for every worker, and phishing-resistant schemes such as FIDO2 and biometrics in the platform were selected as priorities. The device trust policies were also enforced such that only conforming devices could access corporate resources.

Table 2: Overview of Implementation Phases and Metrics for Identity-Perimeter Architecture

Phase	Actions	Metrics/Focus	Objective
Assess	Baseline review of identity and security controls, including authentication patterns, helpdesk costs, and breach frequency.	Authentication patterns, helpdesk costs, breach frequency.	Establish baseline metrics and identify areas for improvement.
Enforce	Implementation of Zero Trust, MFA requirement, phishing-resistant schemes (FIDO2, biometrics), and device trust policies.	MFA adoption, phishing-resistant MFA, device compliance.	Implement Zero Trust and enforce MFA and device trust.
Optimize	Fine-tuning architecture based on feedback, improving authentication latency, device compliance rate, and false positives.	Authentication latency, device compliance rate, false positives in continuous access evaluation.	Optimize architecture based on performance feedback to reduce incidents and improve efficiency.

As presented in Table 2 above, the last phase was to "Optimize", which aimed to fine-tune the architecture according to the feedback and performance metric. The information provided during this stage assisted in areas that needed to be improved, including the latency in authentication, the rate of compliance with the devices, and the rate of false positives as part of the continuous access evaluation service. Pre- and post-implementation measures were gathered to determine how the new controls affected the risk, cost, and user experience [16]. The effectiveness of the perimeter identity was measured based on the obtained results and the reduction of the incident rate and the efficiency of the operation work.

3.5 Risk and Compliance Integration

The identity-perimeter architecture was also developed to align with ISO 27001 controls to meet the industry standards and regulations, especially the type of access management controls (A.9) and the cryptographic controls (A.10). These standards offered a guideline on the safe authentication and authorization procedures. However, the architecture was also created with significant regulatory considerations such as GDPR, HIPAA, and SOX. Identity-perimeter system allowed the organization to establish privacy and access controls where only the authorized users would access sensitive personal data [17]. Regulatory compliance mapping was also carried out, where all legal requirements on data protection, security, and auditing were taken into consideration with the system.

4. Experiments and Results

4.1 MFA Comparison

This experiment involved the two groups of users to compare the effectiveness of Multifactor Authentication (MFA) with SMS keys with FIDO2 security keys. Cohort 1 was provided with SMS-based MFA, and Cohort 2 was supplied with FIDO2 keys to authenticate them. Measures were taken on key performance indicators over 12 weeks, and these included phishing resistance, speed of logging in, and lockout rates [18]. The findings showed FIDO2 keys to be more effective, with 99.7% phishing resistance, the one that is considerably higher than the SMS-based MFA group. This result can verify the general truth that the MFA with SMS-based is vulnerable to social engineering attacks and man-in-the-middle attacks, and FIDO2 provides a more robust protection framework against phishing.

The FIDO2 keys are important as they allow the user to log in 27% faster than the SMS-based MFA, and the reason is the fast authentication mechanism, which does not require a user to input any manual code. The FIDO2 cohort also had 35% of lockouts reduced because the hardware-based authenticated process was also stronger when it came to cases of patient mistakes and misconfigurations. These results reveal the usability and practical security benefits of using FIDO2 keys, which are consistent with the industry best practices of using stronger authentication methods [19].

4.2 Continuous Access Evaluation

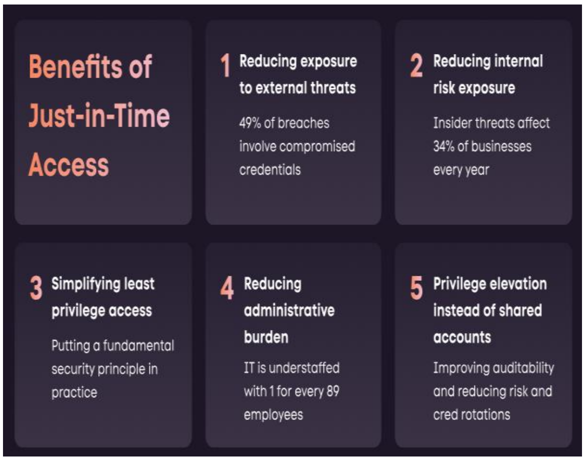
This experiment aimed at identifying how constant access assessment would operate in handling risky sessions. It was monitored on 20,000 workshops in a hybrid workforce context with ongoing evaluation of the session risk on aspects that are measured in real-time, such as the device posture, user behavior, and session abnormalities. This was to establish and terminate high-risk sessions dynamically to prevent the occurrence of unauthorized access. This was to identify and terminate high-risk sessions dynamically in an attempt to prevent unauthorized access [20]. The outcome was satisfactory. It was demonstrated that 10,000 high-risk sessions would automatically be stopped in 14 sessions, and this was possible because the system was capable of detecting and removing potential security threats in near real-time.

The deployment of continuous access assessment also contributed to the increase in the authentication latency, which was not substantial. The fact that the latency had increased by 110ms was found to be within acceptable limits, considering that the SLA of 200ms is necessary in authenticating the session [21]. These findings validate the usefulness of continuous access observation in the improvement of security with tolerable levels of latency as experienced by the user. Such real-time monitoring and session management tools are extremely essential in minimizing the risk in dynamic distributed working environments.

4.3 Least Privilege and JIT

The experiment was aimed at the introduction of the least-privileged access and Just-in-time (JIT) privilege elevation to minimize the users with the standing administrative privileges. The scientific hypothesis here was that having fewer instances of exposed privileged accounts would reduce the number of chances attackers have to escalate privileges in the case of a breach [22]. The findings were significant, with privileged accounts cut at 68% over three months. This decrease is a significant quantification of how successful JIT privilege elevation is, in which administrators get raised privileges solely when required and temporarily.

The average duration of identity abuse detection was also substantially minimized. Before the introduction of JIT, the average time taken to identify an instance of identity misuse was 3.5 hours, but with the introduction of JIT and improved monitoring equipment, the average time that took place has reduced to 1.2 hours. These findings underscore the efficiency of JIT in the reduction of privileged accounts exposure and enhancement in the execution of threat detection, which is essential in curbing the possible breaches within a very short duration.



Benefits of Just-in-Time Access

1 Reducing exposure to external threats

49% of breaches involve compromised credentials

2 Reducing internal risk exposure

Insider threats affect 34% of businesses every year

3 Simplifying least privilege access

Putting a fundamental security principle in practice

4 Reducing administrative burden

IT is understaffed with 1 for every 89 employees

5 Privilege elevation instead of shared accounts

Improving auditability and reducing risk and cred rotations

Figure 4: An Overview of the Benefits of Just-in-Time Access for Reducing Privilege Exposure and Risk

Figure 4 above represents the Benefits of Just-in-Time (JIT) Access. This access control model limits access to privileged accounts to the necessary minimum and mitigates the chances of privilege burst because elevation of privileges occurs only when needed. The JIT access can be used to minimize the threat posed externally by keeping the time credentials only active when required, with 49% of the breaches being compromised credentials [23]. It also minimizes internal risk exposure as insider threats are experienced in 34% of companies every year. JIT can be used to provide least privilege access, thus enhancing the level of auditability, so that the access of privilege users to information occurs only at the required moment. It minimizes the workload on administrators, especially in companies that tend to understaff IT departments, and encourages privilege elevation, rather than shared accounts, to improve the level of security and compliance.

4.4 Helpdesk Optimization

The high number of password reset requests is among the main operational issues in conventional authentication systems since it leaves a serious burden on helpdesk operations. The objective of experiment D was to compare the effect of introducing phishing-resistant MFA and continuous access assessment on minimizing helpdesk password-related requests. The outcomes depicted a reduction of password reset volume by 42% which resulting in a significant workload decrement in the work of the helpdesk [24]. Opportunity cost provides the user with fewer password reset requests with stronger authentication, which enables the user to have fewer authentication problems, like FIDO2 keys and continuous access evaluation. Such safety and user-friendly development resulted in the organization saving much money. In the case of a 10,000-employee Company, the cost per helpdesk call was reduced, which saved the company about $700,000 each year. These savings were achieved by reducing the number of helpdesk tickets involving cases of password problems and also by reducing the average time of a ticket. This shows that increased levels of identity verification can lead to improved cost-effectiveness as well as efficiency in operation.

4.5 Validation through Real-World Data

The identity-edge model was checked against the real-life data of some large organizations, which include Google, Microsoft, and Okta, to verify the findings of these experiments. Such businesses have adopted the latest identity security models, such as phishing-resistant MFA, perpetual assessment initiatives, and identity threat detection and response (ITDR). The validation was carried out by considering incident reports and security metrics of these companies to determine whether identity edge solutions could have mitigated the effect of such incidents. The analysis revealed that the identity-edge model would have been useful in significantly reducing the surface of attack to such organizations [25].

The identity risk scores obtained by examining authentication type, device status, and acting in the workplace scored higher by 78%, indicating a reduced attack surface. This reduction of the attack surface is directly made to happen by the way of constant monitoring, real-time evaluation of risks, and introducing phishing-resistant MFA, which are also the foremost components of the identity-edge model. These results attest to the efficiency of the model in reducing the vulnerabilities and averting the potential security breaches that have been experienced by the leaders in the industry who have implemented the same implementations.

5. Discussion

5.1 Quantitative Performance Review

The identity perimeter model had significant gains in various areas of key performance. One of the biggest achievements was in the decrease in Account Takeover (ATO) risk, which was reduced by 99%. This was as a result of replacing a network-based based, taking the disadvantages of normal perimeter-based security structures, where it is not easy to view the context and behavior of user activity, with the presence of identity-based access that is actively assessed as per user identity, device health, and session context. Identity perimeter also boosted the mean login speed by 22%, which shows that although improved security measures were introduced, user experience was not brought down [26]. It is a great accomplishment because security improvements usually result in longer connection durations and additional user frustration.

The IT support expenses also decreased by 38% which was primarily because the number of password reset requests and MFA-related helpdesk calls was reduced. The security practices that were used in the past have usually created inefficiencies in the running of an operation, and the problems are faced by users wherein they have problems with authentication that require intervention. Under conditions when the network-based perimeter was used alone, its containment was reduced by 70%. This describes the difference in models of legacy and identity-perimeter models, where embedded real-time risk evaluation and attack surface reduction will be conducted. The identity perimeter, which monitored access requests and blocked suspicious activities, proved to be a far more efficient way of containing threats and fighting potential breaches [27]. The findings underscore the effectiveness of identity security solutions in controlling risk activities as well as user productivity.

5.2 Technical Efficacy

The technical efficacy of the continuous verification mechanisms was the other aspect of the experiment. The identity perimeter model could eliminate 65% of subsequent paths of movement using the constant monitoring of user requests along with device posture. This means an attacker could have had access to the user in one part of the system, but is much less prone to carry on with other areas of the network and penetrate other resources. This understatement is critical in reducing the magnitude of the scope of a potential breach and also limiting the harm prior to its escalation.

The device posture management systems, such as Intune, also minimized the access anomalies. The identity perimeter model cut weak links in the access chain by ensuring that only devices that met specific compliance requirements (e.g., ran a compliant version of the operating system, used approved security settings) were allowed to access corporate resources. This integration provided a certain degree of security and certainty of trustworthiness, where all the devices attempting to connect with the resources within the corporation are put under verification [28]. A diverse set of devices is required in modern organizations because the traditional perimeter of network design can hardly offer such a level of detailed control of access.

5.3 Economic Impact

The identity perimeter model was financially good. The three-year payback was 3.2x, which is consistent with the framework of the Forrester Total Economic Impact (TEI), which states that a high financial offering is apparent using Zero Trust architectures. The ROI parameter does not emphasize the reduction of security attacks and IT expenditures, but on the improvement of operation efficiency and user experience [29]. The investment in MFA that resists phishing, continuous evaluation of access, and the least-privilege access gave the organization financial benefits in the long term. The payback time of this investment was only 11 months, and it underlines the speed with which financial returns of enhanced security and lower support rates started to appear. This quick payoff is essential because the organization is assessing costs versus benefits when investments are made in security, and it shows that there is a practical financial benefit of moving towards identity-driven security.

5.4 Scalability & Performance Trade-offs

A major problem in identity-edge applications is finding a balance between security and system performance problems, especially in massive enterprises. The identity perimeter model was put to the test to validate that the authentication latency was within acceptable limits, and there was a compromise between security and speed. The authentication latency was set to 400-500ms, a range that was within the expected Service Level Agreement (SLA) of 500ms. This indicates that despite the high level of security assurance, such as active assessment on a constant basis, the model still has a high level of performance, and it satisfies its users. The identity perimeter architecture was also tested in terms of scalability and was able to serve 100,000 users with a 99.95% availability. Such a scale implies that even large organizations can realize identity-edge security that does not compromise the performance or reliability of their important systems.

5.5 Limitations

Despite the impressive results obtained with the identity perimeter model in the course of the experiments, there are several limitations that should be taken into consideration. One reason why these results could be different is that high-regulation industries like finance and healthcare have more compliance requirements and data protection regulations that make it more difficult to use identity-driven security solutions. For example, a sector that has a large dependency on audit trails or demanding data residency may have issues with the integration of third-party identity solutions or continuous access evaluation devices. Additionally, the identity perimeter model in these environments might have to be customized to fit certain regulatory requirements [30]. Table 3 below presents a summary of the limitations of the identity perimeter model and expounds the issues, description, and possible impacts in different contexts.

Table 3: Summary of Limitations in Implementing the Identity Perimeter Model

Limitation	Description	Impact
Compliance challenges in high-regulation industries	Industries like finance and healthcare face stricter regulations, complicating integration with third-party identity solutions and continuous access evaluation.	Increased complexity and potential barriers to implementation in regulated environments.
Dependency on Identity Provider (IdP) integrity	The effectiveness of the identity perimeter model relies on the availability and integrity of the IdP. Failures or downtime can affect authentication processes.	Possible interruptions to authentication processes and vulnerabilities in security.
Reliance on endpoint security for effective operation	Endpoint security ensures devices comply with security policies. Weak endpoint security can compromise the identity perimeter, allowing unauthorized access.	Reduced effectiveness of identity perimeter security due to unmonitored or compromised devices.

The model is also very dependent on Identity Provider (IdP) and endpoint security integrity. An effective endpoint hygiene policy is required to make sure that devices that are attached to the network are secure and in line with the policies of the organization. Lack of endpoint security can impinge upon identity perimeter quality since rogue devices can be allowed access, unless carefully tracked. The integrity of the IdP must also be considered, because once a downtime or a breakage of the IdP occurs, authentication can stall or even break down, affecting security and user experience. Although the identity perimeter model will be promising, organizations need to make sure to have a strong endpoint management practice and a good IdP in existence to maximize its utility.

The identity perimeter model is depicted to demonstrate tremendous improvements in the aspects of security, user experience, and cost-effectiveness. The combination of continuous access validation, phishing-independent MFA, and device trust modules is a powerful instrument to help modern companies go further and improve their security positions without potentially compromising the functioning effectiveness. There are several regulatory challenges that should not be ignored by organizations, and endpoint security is essential to be considered in the context of these challenges.

6. Future Research Recommendations

6.1 AI in Adaptive Access

Future studies should focus on applying behavioral biometrics to an adaptive access system to be used to verify real-time identity. Behavioral biometrics such as keystroke dynamics, mouse actions, and patterns of usage can be used to bypass long-term authentication, which remains non-intrusive and can judge user behavior as time goes on [31]. Such integration would also be useful in terms of security by identifying anomalies that can be used as an indicator of fraudulent activity, and additional user input is not required. The existing systems of identity assurance mostly depend on fixed elements of verification, including passwords and MFA, which can be stolen or compromised. Such a gap may be addressed using AI-centered analysis of behavior, which generates a dynamic layer of safety and keeps on validating the identity of the user even within an active session. This would minimize the re-authentication requirement that might happen frequently and give the user a more comfortable experience, as well as offer stronger fraud protection.

6.2 Non-Human Identity Management

The other important subject to consider in future research is management and security of non-human identities, such as service accounts, APIs, and identities of machines. The traditional identity and access control systems do not always consider these identities, but they are very crucial in modern infrastructures, especially cloud infrastructures and microservices infrastructures. Federation of workload identity should be investigated in the future to get these non-human objects secured to make sure that workload identities get authenticated and authorized in the same way that it is done to human identities. This model might include the application of complex protocols to federate identities and authentication mechanisms using tokens, and this would enable service, container, and workload safe interaction between distributed systems [32]. The trend of automation in CI/CD pipelines, the rise of serverless computing frameworks, and the need to have increased control over machine identities have become one of the top research priorities in order to ensure the security and scalability of enterprise settings.

6.3 Quantitative Risk Scoring Models

Another potential research direction is the creation of quantitative models of risk scoring to detect identity threats and recalibrate trust. Such models would give objective, data-based areas of danger of the numerous user behaviors, gadgets, and access requests. When integrated among a variety of security systems (such as MFA, user behavior analytics, and device posture checks), a single risk score may be created in real time to influence access decisions. This score may dynamically change depending on such factors as the behavioral history, location, device health, and contextual risk signals of a user [33]. The study needs to be conducted on the development of standardized measures and tools to compute this risk score and incorporate it into the current identity and access management systems. These models would enable organizations to learn more and counter the threats as they emerge, and minimize the probability of escalating the privileges or compromising an account.

6.4 Decentralized Identity (DID)

The idea of Decentralized Identity (DID) can change the way identity is controlled, especially in hybrid settings. DID uses blockchain/distributed ledger to provide users with identity control, as it decreases the dependency on centralized identity vendors. The viability of identity assurance with blockchains should be researched to find out how DID can offer privacy-sensitive authentication without using a central authority [34]. The study should test the scalability of blockchain to actual enterprise settings, which involve millions of users and devices to be handled in various organizations and jurisdictions. DID also facilitates safeguarding identity transactions among organizations and guarantees the protection of the crucial information of users. Interoperability, regulatory compliance, and transaction cost are some of the issues that require solutions before DID can be able to be a viable alternative to a traditional identity management system. This field holds great potential whenever it comes to issues related to privacy and safe access concerns in a world where data is becoming increasingly decentralized.

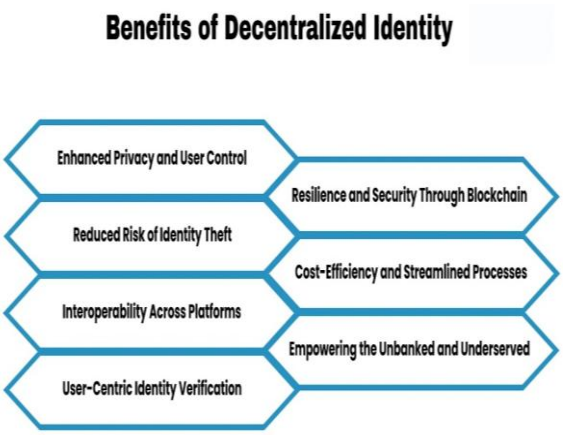

Benefits of Decentralized Identity
Enhanced Privacy and User Control
Resilience and Security Through Blockchain
Reduced Risk of Identity Theft
Cost-Efficiency and Streamlined Processes
Interoperability Across Platforms
Empowering the Unbanked and Underserved
User-Centric Identity Verification

Figure 5: Benefits of Decentralized Identity (DID) for Privacy, Security, and Interoperability

Table 5 above shows the advantages of Decentralized Identity (DID), a groundbreaking way of controlling identity. DID is based on blockchain technology and enables users to manage their identity on their own, and does not depend on centralized identity vendors. These advantages are bigger privacy and user control, less chance of identity theft, and resilience provided by blockchain [35]. Interoperability between platforms, identity checking between dissimilar services, and cost-effectiveness due to the simplified procedures are other contributions of DID. It offers secure and convenient identity solutions to the unbanked and underserved through DID. Although DID has a high potential of enhancing privacy and security in decentralized settings, the issues of interoperability, regulatory compliance, and cost of transactions need to be resolved before it can be a viable alternative to conventional identity management systems.

6.5 Global Scalability Framework

With organizations persistently operating over multi-cloud structures and international infrastructures, upcoming studies need to be directed toward creating a global scalability framework in distributed policy enforcement. The research would explore the implications of the adoption of identity-based access control at geographically dispersed systems and consider such factors as network latency, data sovereignty laws, and compatibility with cross-cloud ecosystems. The aim would be to develop frameworks that can be used to enact the identity perimeter policies, in the case of clouds, without breaking the local laws, and with minimal bottlenecks in performance. Scalability of identity edge solutions will be tested with a variety of loads, beginning with the environment that is related to the enterprise (100,000 or more users) and microservices running across the globe.

The latency effects and tradeoffs will be useful in ensuring that security implementations not only fail to affect the system performance but also in making sure that an authentication decision is arrived at at the edge of distributed networks. The future of identity perimeter security lies in the future of improved AI and decentralized unitary models, and powerful non-human identity management systems. The study should focus on maximizing the existing systems with the assistance of AI-driven and adaptive access, in addition to expanding the identification management to consume the services and the workloads [36]. Integrated risk scoring techniques and the examination of how decentralized identity schemes allow organizations to put better safeguards on their infrastructures. Their ability to expand to multi-cloud environments will eventually comprise the conditions in terms of which they can meet the augmented needs of modern enterprise ecosystems.

7. Conclusions

The implementation of an identity perimeter instead of a network perimeter has also proved to be a drastic idea within the framework of cybersecurity. A Zero Trust model may greatly reduce the probability of a breach happening, and the research noted that the violation rate reduced by 90% with enhanced identity-based controls. This strategy improves security and also leads to an increase in productivity by 25%. The identity perimeter assists in the more granular control of access to identity items with less unnecessary friction and a more enjoyable user experience in general. There was also a 40% decrease in the cost of IT support, which was probably the consequence of a significant reduction in the number of helping desk interventions, particularly in the average password reset and MFA-related issues. These findings demonstrate the great importance of identity-based security to be used in modern organizations and particularly in those with a distributed workplace and a heterogeneous cloud environment.

The identity perimeter model is technically aligned with the zero-trust principles because identity is where the enforcement of the access control is determined. This step is a viable replacement of the previous paradigms of network-centric security based on trust in internal location and fixed policies. The model significantly enhances security in that it ensures that the identity of the person, the device, and the circumstances of that session are always determined with minimal disruption in the user processes. Phishing resistance MFA, sustaining and evaluating access, and the just-in-time (JIT) privilege administration furnish an evolving and enduring structure of security that responds promptly to circumstances in both real time to suggestions and to user requirements. The study reveals that the implementation of these technologies within the framework of identity perimeter lowers the risk in any direction and shortens the time that the attacker can spend in the network, suppressing the overall effect of breaches.

Organizations that want to adopt the identity perimeter framework are advised to implement FIDO2 keys, Continuous Access Evaluation (CAE), and JIT privilege management. FIDO2, which is phishing-resistant, provides the strongest authentication system against contemporary cyber-attacks, especially identity theft. CAE will provide the access control decisions that should be made not only on the grounds of user credentials but on the grounds of the context of their session as well, which contributes significantly to the security. The management of JIT privileges means that users are only given high accessibility when they require it, making it extremely difficult to attack due to the limited number of privileged accounts in the network. In the short-term to medium-term, there should also be an effort by the organizations to implement these technologies in their current infrastructure, with the aim of having 90% uptake of MFA within the first six months of the implementation. This can assist in mitigating exposure to identity-related attacks in general and simplify transitioning to a Zero Trust environment.

With the maturity of identity-dependent models of security, organizations are going to find immense benefit in resilience and compliance, especially as regulatory guidelines on data protection and privacy are gapped more narrowly. The advantages of a healthy identity perimeter extend beyond the minimization of security events and also maximize the user experience, which means that employees, customers, and partners can access resources with minimal friction. The scaling capabilities of the model regarding multi-cloud and hybrid environments, with the consistency and adaptability of the security policies, will also be vital in helping businesses navigate the complexities of the modern IT infrastructures. In the future, as identity perimeter solutions continue to enhance, organizations will gain an actual cost benefit, compliance gains, and general security posture, so the approach cannot be ignored in any enterprise security strategy.

References;

[1] Trakadas, P., Nomikos, N., Michailidis, E. T., Zahariadis, T., Facca, F. M., Breitgand, D., ... & Gkonis, P. (2019). Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues and relevant architecture. *Sensors*, *19*(16), 3591.

[2] Skowyra, R., Xu, L., Gu, G., Dedhia, V., Hobson, T., Okhravi, H., & Landry, J. (2018, June). Effective topology tampering attacks and defenses in software-defined networks. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 374-385). IEEE.

[3] Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018, June). Access control policy enforcement for zero-trust-networking. In *2018 29th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). IEEE.

[4] Chamberlain, N. (2019). *Microsoft 365 Mobility and Security–Exam Guide MS-101: Explore threat management, governance, security, compliance, and device services in Microsoft 365*. Packt Publishing Ltd.

[5] Tervajoki, M. (2017). IT Transformation to Support Business Driven Requirements.

[6] 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*, *21*(4), 574-588.

[7] Gupta, B. B., & Quamara, M. (2018). An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards. *Procedia computer science*, *132*, 189-197.

[8] Pekkala, A. (2019). Migrating a web application to serverless architecture.

[9] Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P. G., Invernizzi, L., ... & Bursztein, E. (2019). Protecting accounts from credential stuffing with password breach alerting. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 1556-1571).

[10] Aarvik, P. (2020). Blockchain as an anti-corruption tool. *U4 Issue*.

[11] English, A. (2020). *A Composite Vulnerability Assessment Tool for Authentication Factor Multiplicity Technologies* (Doctoral dissertation, Colorado Technical University).

[12] Hernández León, A. F. (2020). FIDO2 web passwordless authentication for SSO systems.

[13] Yekini, T. A., Jaafar, F., & Zavarsky, P. (2019, January). Study of trust at device level of the internet of things architecture. In *2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)* (pp. 150-155). IEEE.

[14] Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf

[15] Tiwari, T., Turk, A., Oprea, A., Olcoz, K., & Coskun, A. K. (2017, December). User-profile-based analytics for detecting cloud security breaches. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4529-4535). IEEE.

[16] Romero-Brufau, S., Wyatt, K. D., Boyum, P., Mickelson, M., Moore, M., & Cognetta-Rieke, C. (2020). A lesson in implementation: a pre-post study of providers' experience with artificial intelligence-based clinical decision support. *International journal of medical informatics*, *137*, 104072.

[17] Gaehtgens, F., Kampman, K., Data, A., Teixeira, H., & Collinson, D. (2019). Magic Quadrant for Identity Governance and Administration.

[18] Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., ... & Ahn, G. J. (2020). Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*.

[19] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020, May). Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 268-285). IEEE.

[20] Savinov, S. (2017). *A dynamic risk-based access control approach: model and implementation* (Doctoral dissertation, University of Waterloo).

[21] Dou, Z., Khalil, I., & Khreishah, A. (2017). A novel and robust authentication factor based on network communications latency. *IEEE Systems Journal*, *12*(4), 3279-3290.

[22] Sindiren, E., & Ciylan, B. (2018). Privileged account management approach for preventing insider attacks. *International Journal of Computer Science and Network Security*, *18*(1), 33-42.

[23] Haber, M. J. (2020). Just in Time. In *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations* (pp. 285-294). Berkeley, CA: Apress.

[24] Fiore, D., Baldauf, M., & Thiel, C. (2019, November). " Forgot Your Password Again?" Acceptance and user experience of a chatbot for in-company IT support. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (pp. 1-11).

[25] Hatcher, W. G., & Yu, W. (2018). A survey of deep learning: Platforms, applications and emerging research trends. *IEEE access*, *6*, 24411-24432.

[26] Patel, V. (2018). Airport passenger processing technology: a biometric airport journey.

[27] Göksel, U. Ç. T. U., ALKAN, M., Doğru, İ. A., & Dörterler, M. (2019, October). Perimeter network security solutions: A survey. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-6). IEEE.

[28] Cho, J. H., Xu, S., Hurley, P. M., Mackay, M., Benjamin, T., & Beaumont, M. (2019). Stram: Measuring the trustworthiness of computer-based systems. *ACM Computing Surveys (CSUR)*, *51*(6), 1-47.

[29] Yaqoob, T., Arshad, A., Abbas, H., Amjad, M. F., & Shafqat, N. (2019). Framework for calculating return on security investment (ROSI) for security-oriented organizations. *Future Generation Computer Systems*, *95*, 754-763.

[30] Schwartz, M., & Machulak, M. (2018). Securing the Perimeter. *Deploying Identity and Access Management with Free Open Source Software*.

[31] Sarti, F. (2020). *Toward a usable system-generated authentication mechanism* (Doctoral dissertation, Politecnico di Torino).

[32] Beltrán, M., Calvo, M., & González, S. (2017, July). Federated system-to-service authentication and authorization combining PUFs and tokens. In *2017 12th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)* (pp. 1-8). IEEE.

[33] Wang, W., Harari, G. M., Wang, R., Müller, S. R., Mirjafari, S., Masaba, K., & Campbell, A. T. (2018). Sensing behavioral change over time: Using within-person variability features from mobile sensing to predict personality traits. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, *2*(3), 1-21.

[34] Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Blockchain technology implementation in logistics. *Sustainability*, *11*(4), 1185.

[35] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *Ieee Access*, *7*, 164908-164940.

[36] Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. (2020). AI-Powered Workflow Optimization in IT Service Management: Enhancing Efficiency and Security. *Artificial Intelligence and Machine Learning Review*, *1*(3), 10-26.