Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Identity-Centric Information Systems Architecture for Secure and Scalable Enterprise Platforms

Ishu Anand Jaiswal

Affiliation: University of the Cumberlands, Williamsburg, Kentucky, USA,

ARTICLE INFO

Received: 03 Nov 2022

Revised: 17 Dec 2022

Accepted: 27 Dec 2022

ABSTRACT

The rapid adoption of cloud computing, distributed enterprise applications, Software-as-a-Service platforms, mobile access, remote working, Internet of Things devices, microservices, and multi-cloud infrastructures has fundamentally transformed the architecture of modern enterprise information systems. Traditional enterprise-security architectures were largely constructed around well-defined network boundaries in which users and devices located inside the organizational perimeter were implicitly considered more trustworthy than external entities. However, modern enterprise resources are increasingly distributed across cloud platforms, data centers, remote offices, third-party services, and user devices, making network location an insufficient basis for determining access trust. These developments create significant challenges involving unauthorized access, privilege misuse, identity compromise, credential theft, insider threats, inconsistent authorization, and scalable security-policy enforcement. This study proposes an Identity-Centric Information Systems Architecture for Secure and Scalable Enterprise Platforms (ICISA-ESP) that places verified digital identity, contextual authorization, continuous trust assessment, and fine-grained policy enforcement at the core of enterprise information-system security. The proposed architecture integrates Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Single Sign-On (SSO), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), device identity, contextual risk assessment, least-privilege authorization, policy decision mechanisms, continuous session monitoring, security-event analysis, and identity lifecycle management.

Keywords: Identity-Centric Architecture, Identity and Access Management, Zero Trust Architecture, Enterprise Information Systems, Attribute-Based Access Control.

INTRODUCTION

Enterprise information systems have undergone substantial architectural transformation during the last decade. Traditional organizational applications were commonly hosted inside enterprise-owned data centers and accessed through computers connected to controlled internal networks. Security architectures were consequently designed around clearly identifiable network boundaries, with firewalls, virtual private networks, intrusion-detection systems, authentication servers, and network segmentation separating trusted organizational resources from external networks. The rapid growth of cloud computing, mobile technologies, Software-as-a-Service applications, remote working environments, distributed databases, microservice architectures, Internet of Things devices, and hybrid multi-cloud infrastructures has significantly weakened the assumptions underlying conventional perimeter-oriented security. Enterprise data and applications are no longer located exclusively within organizational networks, while users increasingly access information resources from different geographical locations, devices, networks, and computing environments. As a result, the physical or network location of an entity can no longer serve as a reliable indicator of trust. NIST's Zero Trust Architecture explicitly describes this change by shifting security away from static network perimeters toward users, assets, and individual enterprise resources. It further states that implicit trust should not be granted to a user or device solely because of its location or ownership. This architectural transition creates the need for an identity-centric security model in which verified identity becomes the primary foundation for enterprise access decisions. Identity represents the digital description of an entity interacting with an information system. Depending on the enterprise environment, an identity may correspond to an employee, administrator, customer, contractor, partner, application, service account, workload, virtual machine, device, API, or software process.

Identity management has therefore become a critical component of modern enterprise architecture. As organizations expand their digital ecosystems, the number of identities requiring management grows exponentially, creating challenges related to authentication, authorization, access governance, and regulatory compliance. Traditional identity management approaches, which often rely on isolated authentication systems and static access policies, struggle to accommodate the dynamic nature of contemporary enterprise environments. This limitation increases the risk of unauthorized access, credential misuse, privilege escalation, and security breaches. To address these challenges, enterprises are increasingly adopting Identity-Centric Information Systems Architectures that place identity at the center of security, governance, and operational processes. In such architectures, every access request is evaluated based on the identity of the requesting entity, its assigned privileges, contextual information, and the sensitivity of the requested resource. Technologies such as Identity and Access Management (IAM), Single Sign-On (SSO), Multi-Factor Authentication (MFA), Privileged Access Management (PAM), Identity Governance and Administration (IGA), and Role-Based or Attribute-Based Access Control (RBAC/ABAC) collectively establish a comprehensive framework for securing enterprise resources.

The year 2022 marked a significant acceleration in the adoption of identity-centric security frameworks due to the widespread implementation of cloud-native applications, hybrid work models, and Zero Trust security strategies. Organizations increasingly recognized that identities had become the new security perimeter, requiring continuous verification and monitoring throughout the access lifecycle. Modern enterprise platforms must not only authenticate users at the point of entry but also continuously assess risk factors such as device posture, user behavior, geographic location, and access patterns to ensure secure interactions. Furthermore, enterprise platforms are expected to support millions of users, thousands of applications, and highly distributed infrastructures while maintaining performance, reliability, and security. Scalability therefore becomes a fundamental architectural requirement. Identity-centric architectures facilitate scalability through centralized identity repositories, federated identity services, automated provisioning mechanisms, and cloud-based authentication infrastructures. These capabilities enable organizations to efficiently manage growing numbers of identities without compromising security or operational efficiency. In addition to security and scalability benefits, identity-centric architectures contribute to regulatory compliance and governance requirements. Regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and various industry-specific standards require organizations to implement strict controls over access to sensitive information. By providing detailed audit trails, access monitoring, policy enforcement, and identity lifecycle management, identity-centric systems help organizations demonstrate compliance while reducing administrative complexity.

LITERATURE REVIEW

Angin et al. (2010) proposed an entity-centric approach for privacy and identity management in cloud computing. The researchers recognized that users and services must disclose personally identifiable information when authenticating to cloud service providers, creating privacy and security risks when identity information is distributed among multiple providers. Their framework employed privacy-enhancing mechanisms, including active bundles and techniques for protecting identity attributes during service interaction. The study established an important principle for identity-centric enterprise architecture: identity information should remain protected throughout authentication and service-access operations rather than merely securing the communication channel. Celesti et al. (2010) investigated identity management in heterogeneous and federated cloud environments. The researchers proposed an InterCloud Identity Management architecture intended to support authentication between independently administered cloud infrastructures. Their work emphasized the importance of federation when users and enterprise applications access computing resources across multiple providers. The study demonstrated that distributed platforms require interoperable identity mechanisms rather than maintaining completely isolated authentication infrastructures within every cloud environment.

Hamlen et al. (2011) examined developments and future directions in cloud identity management. They identified the management of multiple cloud-user identities in federated environments as a critical security requirement and discussed the relationship between identity technologies and secure cloud computing. Their work highlighted that organizations moving applications and information toward cloud platforms must preserve control over identity verification and access privileges even when resources are distributed outside conventional enterprise boundaries. Hardt (2012) standardized the OAuth 2.0 Authorization Framework through RFC 6749. OAuth introduced a mechanism allowing third-party applications to obtain limited access to HTTP services either on behalf of a resource owner or on their own behalf without requiring applications to possess the user's primary credentials. This separation between authentication credentials and delegated authorization became important for enterprise platforms containing APIs, web applications, mobile services, and cloud resources. Nevertheless, OAuth primarily addresses delegated authorization and therefore normally requires complementary identity mechanisms when strong user authentication and identity assertions are required.

Hu et al. (2014) formalized Attribute-Based Access Control through NIST SP 800-162. ABAC determines whether an operation should be permitted by evaluating attributes associated with subjects, objects, requested operations, and environmental conditions against defined policies. Compared with authorization mechanisms relying exclusively on static roles, ABAC provides substantially greater flexibility for distributed organizations where decisions may depend on department, clearance level, device, resource classification, location, time, or other contextual information. This work provides a major theoretical foundation for fine-grained authorization within the proposed identity-centric architecture. Ward and Beyer (2014) described Google's BeyondCorp approach to enterprise security. Their work challenged the assumption that an internal corporate network should automatically be considered privileged or trustworthy. Rather than controlling access primarily according to network location, BeyondCorp moved corporate applications toward an access model centered on users and devices. The approach showed that enterprise applications could be accessed from untrusted networks when authorization was based on appropriate identity and device information. This represented an important practical transition from perimeter-oriented security toward identity-centric enterprise access.

Sakimura et al. (2014) introduced OpenID Connect 1.0 as an identity layer built on top of OAuth 2.0. OpenID Connect enables applications to verify the identity of an end user based on authentication performed by an authorization server and to obtain standardized claims describing the authenticated user. The specification provided an interoperable mechanism for authentication and identity federation across web and cloud applications. Its separation of identity providers from relying applications is particularly relevant for scalable enterprise architectures where numerous applications require centralized or federated identity verification. Schaffer (2015) investigated continuous authentication using mobile devices. The study observed that traditional authentication generally verifies the user only at a particular point in time, while subsequent session activity may continue without further identity validation. Mobile devices containing multiple sensors create opportunities for continuous authentication through behavioral and contextual signals. The work highlighted the transition from one-time identity verification toward persistent confidence assessment, which is important for enterprise sessions involving sensitive applications or long-duration access.

Dos Santos et al. (2016) proposed a framework for risk-based access control in cloud computing. The researchers argued that traditional access-control policies are often too rigid for dynamic and heterogeneous cloud environments. Their framework extended XACML with risk assessment and supported combinations of conventional RBAC or ABAC mechanisms with dynamically calculated access risk. The study demonstrated that contextual risk can be incorporated directly into authorization decisions, enabling flexible handling of exceptional access requests while maintaining policy enforcement. This provides a significant basis for the proposed architecture's contextual trust and risk-assessment components. Osborn et al. (2016) described the design and deployment of BeyondCorp within Google. The architecture based access decisions on information concerning a device, its security state, and the associated user rather than whether the request originated from an internal network. BeyondCorp implemented dynamic tiers of access and treated both internal and external networks as untrusted. This operational deployment demonstrated that identity- and device-aware access control could be implemented at enterprise scale without requiring a traditional privileged intranet model.

Grassi et al. (2017) published the NIST Digital Identity Guidelines, providing structured requirements for digital identity proofing, enrollment, authentication, authenticator management, federation, and assertions. The guidelines distinguish multiple components of the digital identity lifecycle rather than treating authentication as a single password-verification event. Their framework reinforces the importance of connecting identity proofing, authentication assurance, lifecycle management, and federation when designing enterprise identity architectures. Werner et al. (2017) presented a comprehensive survey of privacy strategies for cloud identity management. The researchers observed that cloud systems involve large numbers of users, applications, identity providers, and service providers exchanging sensitive information. They identified continuing challenges involving identity-data privacy, federated identity, trust relationships, fine-grained dissemination control, policy enforcement, and dynamic cloud environments. The study demonstrated that scalable identity management must protect not only application resources but also the identity attributes used during authentication and authorization.

Shahzad and Singh (2017) investigated continuous authentication and authorization in Internet of Things environments. They argued that one-time authentication is insufficient in dynamic settings because users may not retain continuous control of devices throughout an active session. The researchers emphasized continuous verification and authorization as mechanisms for maintaining security as conditions change. Although focused on IoT, the principle is directly relevant to distributed enterprise platforms containing mobile endpoints, intelligent devices, service identities, and dynamically changing sessions. Sartoli and Siami Namin (2019) proposed an adaptive access-control policy model using Answer Set Programming. Their work addressed limitations of conventional static policies when contextual conditions change at runtime. The model differentiated default, context-dependent, and

exception policies and allowed policy decisions to adapt when previously unavailable information or exceptional circumstances appeared. The study demonstrated that enterprise authorization policies may require runtime reasoning rather than permanently fixed rules, especially in context-aware environments.

Nespoli et al. (2019) developed PALOT, a framework for context-aware continuous authentication and authorization using Internet of Things information. Their architecture combined an ontology-based information model with behavioral-pattern analysis and a confidence-management component capable of interpreting interactions among users and heterogeneous devices. Experimental analysis demonstrated the feasibility and scalability of continuous, non-intrusive authentication. This work supports the use of behavioral and contextual evidence in determining whether a previously authenticated identity should continue receiving enterprise privileges. Rose et al. (2020) formalized Zero Trust Architecture in NIST SP 800-207. The publication explicitly rejected implicit trust based solely on physical or network location or enterprise ownership. It established that authentication and authorization of subjects and devices should occur before sessions to enterprise resources are established and shifted the security focus from protecting network segments toward protecting individual resources. The document also defined logical components and deployment approaches for enterprise zero-trust systems. This work represents a central foundation for identity-centric enterprise architecture because identity, device state, policy, and resource context become primary inputs to access decisions.

Teerakanok et al. (2021) examined migration from traditional perimeter-oriented networks toward Zero Trust Architecture. The authors emphasized that zero trust cannot be implemented simply by purchasing or replacing a particular security product; migration requires consideration of security requirements, threats, organizational processes, existing infrastructure, and implementation stages. Their analysis highlighted the practical difficulty of transforming legacy enterprise environments while maintaining system operation. The study is particularly relevant to this research because an identity-centric architecture must support gradual integration with existing IAM, applications, networks, and access-control infrastructure. He et al. (2022) provided a detailed survey of Zero Trust Architecture and identified identity authentication, access control, and trust assessment as three fundamental technical areas. The authors emphasized continuous dynamic security access control, minimum privileges, device and user authentication, continuous monitoring, and dynamic adjustment of access rights according to current trust status. They also concluded that zero-trust implementation remained relatively immature and identified further research needs relating to architecture, authentication, access control, and trust-evaluation algorithms.

Arshad et al. (2022) reviewed Semantic Attribute-Based Access Control and examined limitations of conventional ABAC in heterogeneous and distributed environments. They observed that attributes describing subjects, objects, actions, and environments may be semantically equivalent but represented using syntactically different terms across systems. Semantic ABAC integrates semantic technologies with attribute-based authorization to improve interoperability and policy expressiveness. This challenge is highly relevant to enterprise platforms where identity attributes are frequently obtained from different directories, cloud services, business applications, and organizational domains. Nahar and Gill (2022) proposed an integrated identity and access management metamodel and pattern system for secure enterprise architecture. Their work developed a technology- and business-domain-agnostic IAM metamodel integrating identity management with access management. Using Design Science Research, they produced an ontology-based model and eight IAM patterns addressing recurring architectural problems. The study concluded that integrated IAM modelling could assist enterprise and information-systems architects in designing situation-specific identity architectures while maintaining a common conceptual foundation. This work is particularly close to the present research because it connects IAM directly with enterprise architecture rather than treating identity management as an isolated security service.

METHODOLOGY

This study adopts a Systematic Literature Review (SLR) combined with a Conceptual Experimental Framework to investigate the design of an identity-centric information systems architecture for secure and scalable enterprise platforms. The methodological structure follows the uploaded reference paper, which combines systematic review, conceptual framework development, mathematical representation, algorithmic processing, and performance evaluation.

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

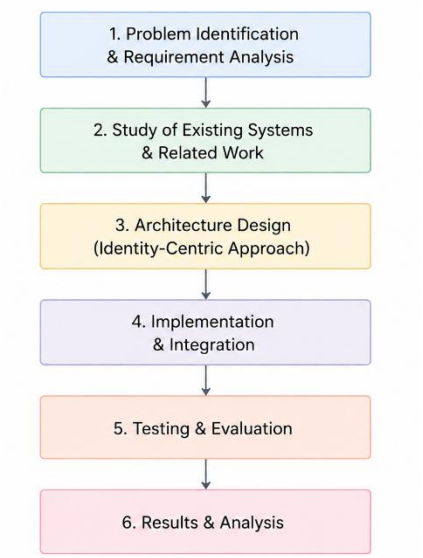

Figure 1: Methodology for Identity-Centric Information Systems Architecture for Secure and Scalable Enterprise Platforms

Figure 1 illustrates the research methodology adopted for developing an identity-centric information systems architecture. The process begins with problem identification and requirement analysis to understand security and scalability challenges in enterprise environments. A comprehensive review of existing systems and related literature is then conducted to identify research gaps and best practices. Based on these findings, an identity-centric architecture is designed, followed by its implementation and integration within the enterprise framework. The developed system is subsequently tested and evaluated to assess its security, performance, and scalability. Finally, the results are analyzed to determine the effectiveness of the proposed architecture in enhancing secure access management and supporting scalable enterprise operations.

Proposed Algorithm

Step 1: Identity and Access Request Acquisition

The system receives an access request from a human user, application, API, service account, workload, or enterprise device.

Each request is represented as:

$$AR_i = \{I, D_i, D, V_i, R, E, S_i ACT_i LOC_i T_i CTX_i\}$$

where:

ID_i= Requesting identity
DV_i= Device or workload identity
RES_i= Requested enterprise resource
ACT_i= Requested operation
LOC_i= Access location
T_i= Request timestamp
CTX_i= Additional contextual information

The system retrieves the corresponding identity profile:

$$IP_i = \{R, o, l, e_i, Dept_i Clearance_i Status_i Privilege_i\}$$

If the identity does not exist, is suspended, or has been revoked, the request is terminated.

$$Status_i \neq Active \Rightarrow Deny$$

This step ensures that only currently valid enterprise identities proceed to authentication.

Step 2: Authentication Verification

The identity is authenticated using one or more available authentication mechanisms.

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Authentication factors may include:

Password
One-Time Password
Security token
Smart card
Digital certificate
Biometric characteristic
Federated identity assertion
Device certificate

The authentication status is represented as:

$$AS_i = f(C, R_i, M, F, A_i CERT_i BIO_i FED_i)$$

where:

CR_i= Credential verification
MFA_i= Multi-factor verification
$CERT_i$= Certificate verification
BIO_i= Biometric verification
FED_i= Federated identity verification

If authentication fails:

$$AS_i = 0 \Rightarrow Deny$$

If authentication succeeds:

$$AS_i = 1 \Rightarrow Continue$$

The framework may require stronger authentication when the requested resource is highly sensitive.

Step 3: Device and Endpoint Trust Verification

The requesting device or workload is evaluated before access is authorized.

The Device Trust Score is calculated as:

$$DTS_i = w_1 OS_i + w_2 PATCH_i + w_3 ENC_i + w_4 EDR_i + w_5 COMP_i$$

where:

OS_i= Operating-system integrity
$PATCH_i$= Patch status
ENC_i= Encryption status
EDR_i= Endpoint protection status
$COMP_i$= Enterprise compliance status

The device can be categorized conceptually as:

$$DeviceState \in \{T, r, ustedConditionalUntrusted\}$$

A managed and compliant enterprise device receives greater trust than an unknown, outdated, or non-compliant endpoint. If the device is classified as untrusted and the requested operation is highly sensitive, the request can be denied or challenged with additional verification.

Step 4: Context and Behavioral Risk Assessment

The framework evaluates the current request context and compares it with historical identity behavior.

Relevant contextual characteristics include:

Access location
Login time
Network type
Device change
Resource sensitivity
Previous authentication failures
Unusual data-transfer activity

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Behavioral deviation
Threat intelligence indicators

The Behavioral Deviation Score is:

$$BDS_i = d(B_{current}, B_{historical})$$

where:

$B_{current}$= Current behavior
$B_{historical}$= Historical identity behavior

A larger value indicates stronger deviation from expected activity.

The Identity Risk Score is then calculated:

$$IRS_i = v_1 AF_i + v_2 DR_i + v_3 BDS_i + v_4 RR_i + v_5 TI_i$$

where:

AF_i= Authentication-failure risk
DR_i= Device risk
BDS_i= Behavioral deviation
RR_i= Resource-related risk
TI_i= Threat-intelligence indicator

Conceptually:

$$IRS_i \in \{L, o, w, ModerateHighCritical\}$$

A critical risk level may immediately terminate the request.

Step 5: Dynamic Trust Score Calculation

Authentication success alone does not automatically produce full enterprise trust.

The framework calculates a dynamic trust score using:

$$TS_i = \alpha AC_i + \beta DTS_i + \gamma BC_i + \delta LC_i - \epsilon IRS_i$$

where:

AC_i= Authentication confidence
DTS_i= Device trust
BC_i= Behavioral confidence
LC_i= Location/context confidence
IRS_i= Identity risk

Higher values indicate stronger trust. The exact weights are organizational or experimental parameters and should not be treated as universal constants.

The conceptual trust levels are:

Trust Level	Interpretation
High	Strong identity and contextual confidence
Moderate	Access may be allowed with restrictions
Low	Additional verification required
Critical Risk	Access should be denied

Trust is evaluated against the sensitivity of the requested resource.

$$RequiredTrust_i = f(ResourceSensitivity_i)$$

Therefore, more sensitive resources require stronger trust.

RESULTS AND FINDINGS

Identity Verification Performance

Table 1. Comparative Authentication Capability

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Authentication Mechanism	Identity Assurance	Credential-Theft Resistance	User Convenience	Enterprise Suitability
Password Only	Low	Low	High	Moderate
Password + OTP	High	High	Moderate	High
Certificate-Based	Very High	Very High	Moderate	Very High
Biometric Authentication	Very High	High	High	High
Federated SSO	High	High	Very High	Very High
Adaptive MFA	Very High	Very High	High	Very High

Analysis

Table 1 demonstrates that password-only authentication provides relatively weak protection because credentials may be stolen, reused, or exposed through phishing. Multi-Factor Authentication improves assurance by requiring independent authentication factors. Certificate-based authentication offers strong identity and device verification but introduces certificate lifecycle-management requirements. Federated Single Sign-On improves usability and enterprise scalability by reducing the need for separate application credentials. Adaptive MFA provides additional flexibility because stronger verification can be triggered only when contextual risk justifies it. Therefore, the proposed framework combines federated authentication and adaptive MFA rather than depending upon one authentication mechanism.

Access Control Capability

Table 2. Comparison of Enterprise Authorization Models

Access Model	Role Awareness	Context Awareness	Fine-Grained Control	Dynamic Adaptability
ACL	Low	Very Low	Moderate	Very Low
RBAC	Very High	Low	Moderate	Low
ABAC	High	Very High	Very High	High
Risk-Based Access	Moderate	Very High	High	Very High
Proposed Hybrid Model	Very High	Very High	Very High	Very High

Analysis

Table 2 indicates that no single conventional authorization mechanism satisfies all enterprise requirements. Access Control Lists provide direct permissions but become difficult to administer across large numbers of identities and resources. RBAC simplifies enterprise administration by grouping permissions according to organizational roles, but it provides limited support for dynamic context. ABAC offers stronger fine-grained control through subject, object, action, and environmental attributes. Risk-based authorization improves adaptability by considering current security conditions. The proposed architecture combines role, attribute, contextual, resource, and risk information to support more flexible access decisions.

Identity and Context Evaluation

Table 3. Trust Evaluation Factors

Trust Factor	Security Importance
Authentication Confidence	Very High
Device Compliance	Very High
Historical User Behavior	High

Access Location	High
Resource Sensitivity	Very High
Authentication Failure History	High
Threat Intelligence	Very High
Current Session Behavior	Very High

Analysis

Table 3 demonstrates that trust cannot be accurately determined using identity credentials alone. Authentication verifies who the requester is, but contextual indicators determine whether the current request is consistent with expected behavior. A legitimate identity using a compromised device may still present substantial security risk. Similarly, a valid identity exhibiting unusual access behavior may require additional verification. Therefore, identity assurance and contextual trust should operate together.

CONCLUSION AND DISCUSSION

The present study investigated Identity-Centric Information Systems Architecture for Secure and Scalable Enterprise Platforms through a systematic examination of identity-management, authentication, authorization, continuous-access, and zero-trust research published from 2010 through 2022 and through the development of the proposed Identity-Centric Information Systems Architecture for Secure and Scalable Enterprise Platforms (ICISA-ESP). Following the structure of the reference study, the discussion integrates the major findings of the review with the architectural and algorithmic framework developed in the methodology rather than treating the conclusion as a brief summary alone. The central finding of the study is that conventional perimeter-oriented security is increasingly inadequate for modern distributed enterprise platforms. Traditional enterprise architectures frequently assume that entities operating inside an organizational network are more trustworthy than entities accessing resources externally. This assumption becomes difficult to maintain when users, applications, cloud workloads, devices, APIs, and enterprise resources are distributed among internal data centers, public cloud environments, SaaS applications, remote working locations, and third-party infrastructures. NIST SP 800-207 formalized this shift by defining zero trust around users, assets, and resources and explicitly rejecting implicit trust based solely on network location or asset ownership. The proposed architecture therefore places digital identity at the center of enterprise access control. Every human user, application, workload, service, and relevant device must possess a verifiable identity that can be associated with credentials, roles, attributes, devices, organizational relationships, and security context. This approach transforms identity management from a supporting authentication service into a principal architectural component that governs how enterprise resources are accessed. Earlier cloud research already demonstrated the importance of managing identities across distributed service environments. Angin et al. proposed an entity-centric identity approach intended to protect personally identifiable information while supporting cloud services, whereas Celesti et al. addressed authentication across federated cloud environments. Hamlen et al. subsequently identified identity management as a major cloud-security requirement because users may maintain multiple identities across federated systems. These studies established an early foundation for the identity-centric approach developed in ICISA-ESP. A second major conclusion is that authentication should be considered a continuous assurance process rather than a single login event. Password-only authentication cannot provide sufficient confidence for sensitive enterprise systems because credentials can be stolen, reused, shared, or compromised. The proposed architecture therefore incorporates Multi-Factor Authentication, certificates, federated authentication, device verification, and additional contextual information.

REFERENCES:

[1] Angin, P., Bhargava, B., Ranchal, R., Singh, N., Ben Othmane, L., Lilien, L., & Linderman, M. (2010). An entity-centric approach for privacy and identity management in cloud computing. *29th IEEE Symposium on Reliable Distributed Systems*. DOI: 10.1109/SRDS.2010.28.

[2] Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010). Three-phase cross-cloud federation model: The cloud SSO authentication. *2010 International Conference on Advances in Future Internet*. DOI: 10.1109/AFIN.2010.23.

[3] Hamlen, K. W., Liu, P., Kantarcioglu, M., Thuraisingham, B., & Yu, T. (2011). Identity management for cloud computing: Developments and directions. *7th Annual Cyber Security and Information Intelligence Research Workshop*. DOI: 10.1145/2179298.2179333.

[4] Hardt, D. (2012). *The OAuth 2.0 Authorization Framework*. RFC 6749. Internet Engineering Task Force. DOI: 10.17487/RFC6749.

[5] Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. NIST Special Publication 800-162. DOI: 10.6028/NIST.SP.800-162.

[6] Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *;login:, 39*(6), 6–11.

[7] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). *OpenID Connect Core 1.0*. OpenID Foundation.

[8] Jaiswal, I. A. (2022). Identity-centric information systems architecture for secure and scalable enterprise platforms. Journal of Information Systems Engineering and Management.

[9] Dos Santos, D. R., Marinho, R., Schmitt, G. R., Westphall, C. M., & Westphall, C. B. (2016). A framework and risk assessment approaches for risk-based access control in the cloud. *Journal of Network and Computer Applications, 74*, 86–97. DOI: 10.1016/j.jnca.2016.08.013.

[10] Osborn, B., McWilliams, J., Beyer, B., & Saltonstall, M. (2016). BeyondCorp: Design to deployment at Google. *;login:, 41*(1), 28–34.

[11] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital Identity Guidelines*. NIST Special Publication 800-63-3. DOI: 10.6028/NIST.SP.800-63-3.

[12] Werner, J., Westphall, C. M., & Westphall, C. B. (2017). Cloud identity management: A survey on privacy strategies. *Computer Networks, 122*, 29–42. DOI: 10.1016/j.comnet.2017.04.030.

[13] Shahzad, M., & Singh, M. P. (2017). Continuous authentication and authorization for the Internet of Things. *IEEE Internet Computing, 21*(2), 86–90. DOI: 10.1109/MIC.2017.33.

[14] Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security, 2022(11). https://doi.org/10.52710/cfs.836.

[15] Nespoli, P., Zago, M., Huertas Celdrán, A., Gil Pérez, M., Gómez Mármol, F., & García Clemente, F. J. (2019). PALOT: Profiling and authenticating users leveraging Internet of Things. *Sensors, 19*(12), 2832. DOI: 10.3390/s19122832.

[16] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207. DOI: 10.6028/NIST.SP.800-207.

[17] Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and challenges. *Security and Communication Networks, 2021*, 9947347. DOI: 10.1155/2021/9947347.

[18] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on Zero Trust Architecture: Challenges and future trends. *Wireless Communications and Mobile Computing, 2022*, 6476274. DOI: 10.1155/2022/6476274.

[19] Arshad, H., Johansen, C., & Owe, O. (2022). Semantic Attribute-Based Access Control: A review on current status and future perspectives. *Journal of Systems Architecture, 129*, 102625. DOI: 10.1016/j.sysarc.2022.102625.

[20] Nahar, K., & Gill, A. Q. (2022). Integrated identity and access management metamodel and pattern system for secure enterprise architecture. *Data & Knowledge Engineering, 140*, 102038. DOI: 10.1016/j.datak.2022.102038.