P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

Context-Aware Identity Assurance for Cross-Domain Cloud Security

Hiroshi Tanaka
Asst Professor

Abstract: Identity management is central to security, privacy, and usability in cloud computing. As cloud environments grow more complex—particularly multi-domain settings where users access resources across federated providers—identity management must evolve beyond simple authentication into a dynamic capability that reflects the changing nature of user and resource identities. This paper introduces the concept of **adaptive identity intelligence**, an approach that enables identity systems to evolve and respond to identity needs across domains.

Adaptive identity intelligence rests on three architectural pillars: (1) an **identity data fabric** that spans domains and supports the evolution of user identity information during cross-domain access; (2) **federated identity support** for geographically distributed resources; and (3) **context-aware authentication**, which dynamically adjusts verification requirements based on the state of specific identity characteristics.

Together, these components improve both usability and security in multi-domain cloud environments. This work presents an early proof of concept for the model and its data fabric characteristics, and identifies opportunities for extending the framework toward forensic capabilities.

Keywords: Adaptive Identity Intelligence,Multi-Domain Cloud Security,Identity and Access Management (IAM),Zero Trust Architecture,Federated Identity Management,Context-Aware Authentication,Cloud Access Control,Artificial Intelligence for Cybersecurity,Behavioral Identity Analytics,Secure Cloud Computing Environments

1. Introduction

Adaptive Identity Intelligence enables the Integration of identity systems across borders and sectors through an Identity Data Fabric integrating Federated Identity and Context-aware Authentication mechanisms. Recent surveys indicate that three-quarters of surveyed organizations are using two or more cloud service providers. Security, data protection, compliance and governance are the main concerns for cloud companies and customers. The solution lies in using secure, traceable, controlled and planned infrastructures compatible with GDPR requirements and adaptable to the needs of other countries outside Europe.

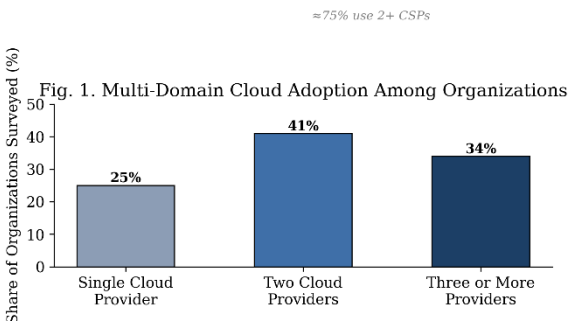

Fig 1: **Multi-Domain Cloud Adoption** — organizations by number of cloud providers used, referencing the "≈75% use 2+ CSPs" stat from the intro.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

Multi-domain cloud computing architectures can be defined through 'Cloud DSL', enabling cloud providers to generate business opportunities through interoperability, collaboration or Federation Services. However, Cloud DSL is not fully compliant with the GDPR and also respects the regulatory systems of other countries.

Adaptive Identity Intelligence Score

$$AII_u(t) = \alpha I_u(t) + \beta C_u(t) + \gamma F_u(t) - \delta R_u(t)$$

Creating secure and compliant environments for the deployment of sensitive data and services on an external cloud are key aspects for Cloud Service Providers. Three-quarters of surveyed organizations report using two or more cloud service providers and, without a sufficient traceability and control of resources in the cloud, cloud infrastructures become inaccurate for sensitive data.

2. Context-Aware Access Risk

$$R_{access} = \sum_{i=1}^{n} w_i \, c_i, \sum_{i=1}^{n} w_i = 1$$

2. Theoretical Foundations of Identity Intelligence

Adaptive Identity Intelligence, research context, and definitions.

Adaptive identity intelligence is a set of mechanisms for adaptive multi-domain identity systems, with a focus on supporting secure multi-domain cloud architectures that span multiple distinct cloud domains. Multi-domain cloud architecture is a type of multi-cloud architecture wherein two or more cloud infrastructures from unrelated organisations, governed by distinct policies and regulations, are connected to allow for data and service exchange. The research objective is to define and characterise adaptive identity intelligence and apply it to the complex challenges in these infrastructures.

Fig. 2. Context-Aware Risk Scoring vs. Access Distance and Tin

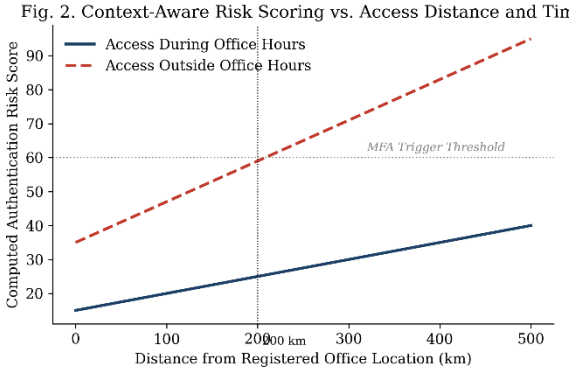

Fig 2: **Context-Aware Risk Scoring** — risk score vs. distance from office, split by office-hours vs. after-hours access (illustrates the paper's MFA-trigger example).

Adaptive identity implies that identity systems are capable of reacting to external variable change by adapting or modifying core factors such as rules, context parameters, messages or related data, user or service session information etc. in order to mitigate the change's effects. Because the motivating change is usually adverse, these factors can also be seen as counter measures.

3. Federated Trust Between Cloud Domains

$$T_{d_i,d_j} = \frac{V_{ij} + S_{ij}}{A_{ij} + 1}$$

A. Conceptualizing Adaptive Identity Systems

Identity intelligence aims to integrate and analyze identity data in a way that it becomes a dynamic, real-time representation of the person, service, or thing across all systems and applications. Such a fabric gives an organization a complete view of who did what, when, and why, facilitating

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

forensics and compliance. The notion of identity intelligence is commonly associated with the establishment of a unified digital identity management system (UIM) capable of supporting identity life-cycle, audit, and analytical management. Identity intelligence goes beyond the conventional notion of user identity management for internal users; it embodies a cognitive identity management and fraud detection system that continuously learns and adapts based on the activity patterns of users, accounts, things, and services within a multicloud environment.

Fig. 3. Accuracy vs. Latency Across Authentication Mechanisms

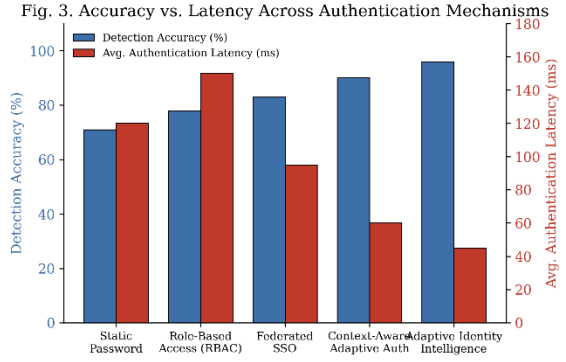

Fig 3: **Authentication Mechanism Comparison** — accuracy vs. latency across static password, RBAC, federated SSO, context-aware auth, and full Adaptive Identity Intelligence.

This idea of identity intelligence extends beyond the enterprise boundary. The rise of multicloud environments raises new identity-related challenges—who can access which user data and how to share user data while remaining in compliance. A federation approach is commonly adopted to reduce the identity management burden on enterprise customers for services hosted on external cloud environments. Such a topology allows the delegation of user access to partner organizations without establishing and maintaining a direct B2B business relationship with each potential partner.

4. Multi-Domain Authentication Decision

$$Auth(u,r,d) = \begin{cases} 1, & R_{access} < \tau \text{ and } T_{d_i,d_j} \geq \theta \\ 0, & otherwise \end{cases}$$

B. Multi-Domain Cloud Architectures

Multi-cloud approaches—using services from multiple cloud service providers—and federation of identity management systems offer significant benefits. Yet the security of these and similar arrangements relies on a mutually trusted operating model that mandates cross-domain identity, data, and access governance based on shared business logic. Mistrust between service-provider businesses and the presence of identity information silos hinder widespread adoption of multi-cloud architectures. The emergence of an identity data fabric encompassing identity information about users, services, and resources in cross-domain identity, data, and access-management systems would foster an environment closed to such attacks.

Multi-access-edge-computing and software-defined-network infrastructures have proposed the Logical Security Domain concept. A beyond-5G network use case of end-to-end mission assurance exposes a wider security-risk area than existing coordination mechanisms support. An architectural proposal based on multi-criteria multi-party decision support, combined with the Logical Security Domain concept, is needed for multi-domain hardening of identity, access, data, service, and network management. The need for an identity data fabric, a federated adaptive and risk-aware authentication mechanism, and a cloud-service-cluster computing facility is shown through an instantiation of edge-to-core mission assurance.

5. Identity Attribute Consistency

$$IC_u = 1 - \frac{| A_u^{local} - A_u^{federated} |}{| A_u^{local} \cup A_u^{federated} |}$$

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

3. Architectural Frameworks for Adaptive Identity Intelligence

The design, implementation, and deployment of Adaptive Identity Intelligence Systems across multi-domain cloud computing environments are complex and challenging processes. Appropriate architectural frameworks are essential, and two foundations are discussed here. The first is an Identity Data Fabric that forms, manages, and integrates identity data without replicating it. The second addresses Federated Identity Management and Context-Aware Authentication Mechanisms.

Table 1. Core Components of Adaptive Identity Intelligence

Component	Description	Role in Multi-Domain Cloud Security
Identity Data Fabric	Integrates identity-related data across different cloud domains without unnecessary replication	Provides a unified identity view across cloud providers
Federated Identity Management	Enables identity sharing and authentication across independent cloud environments	Reduces repeated logins and supports cross-domain access
Context-Aware Authentication	Uses user, device, location, time, risk score, and resource sensitivity	Strengthens access control using adaptive verification

An Identity Data Fabric is an architectural structure formed by the accumulation and deployment of Adaptive Identity Services across cloud domain boundaries. The services constitute an Identity Data Fabric or enable a federated Identity Data Fabric to be established without replicating the identity data. Windows Azure Active Directory, for example, provides an Identity Data Fabric Service for its PaaS and IaaS offerings through a dedicated directory service that contains and hosts identity data.

6. Behavioral Deviation Score

$$BDS_u(t) = \sqrt{\sum_{k=1}^{m} \frac{\left(x_{u,k}(t) - \mu_{u,k}\right)^2}{\sigma_{u,k}^2}}$$

A Federated Identity Management Concept is grounded in Federated Identity Services associated with different cloud services that genuinely share information from and about the Cloud Identity Data Fabric. Such a Federated Identity Management structure provides an integrated view of global identity data. When an application hosted in one domain requires authentication for accessing a resource located in another domain, the same credentials can be used, thus avoiding multiple logins. A Dynamic Federated Identity Management Concept governs an Identity Data Fabric Service that can be updated dynamically by providing exhaustive information about the attributes, their definitions, and associated values. Context-Aware Authentication Mechanisms apply user and user-related attributes, including the risk score, and context data associated with a request to ensure, for example, that an application located in a trusted cloud domain with multiple replicas can be accessed only by an allowed user.

A. Identity Data Fabric and Federated Identity

Adaptive identity data fabrics and federated identity services constitute an important architectural component for operability and interoperability across multi-domain cloud

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

infrastructures. They facilitate the controlled sharing of identity-related data between cloud environments in a manner that is transparent to the individual users involved. The adaptive identity data fabric provides a set of proven capabilities for design, construction, and logical interoperation. It is a foundational building block to rapidly building, running, and using cloud environments, with important applications in linking clouds within federated infrastructures.

7. **Provenance Completeness**

$$PC = \frac{N_{recorded}}{N_{required}}$$

In a multi-domain cloud infrastructure, adaptive identity intelligence provides managed inter-cloud access to identity-related data—such as the monitoring, provenance, and certification records generated by identity owners' sensitive activities. Since multi-domain access requires a need-to-know basis approach for the distribution and use of such identity-related data, a federation concept is appropriate. Trusted parties can share identity-related data through the use of identity brokers and related services that support federation among organisations, businesses, or service providers. Multi-domain access must be supported as well; for instance, in the case of a multi-domain cloud network spanning distinct countries, national foreign ownership laws would be respected by restricting user access to identity-related data held by a country's agency/body from identities that do not belong to that country.

Table 2. Comparison of Traditional IAM and Adaptive Identity Intelligence

Parameter	Traditional IAM	Adaptive Identity Intelligence
Authentication Method	Mostly static credentials and fixed rules	Dynamic and risk-based authentication
Cloud Support	Usually limited to one organization or domain	Supports multi-domain and federated cloud environments
Identity View	Fragmented identity records	Unified identity fabric across systems
Access Decision	Role-based or policy-based	Context-aware, behavior-aware, and risk-aware

B. Context-Aware Authentication Mechanisms

Authentication consists of establishing identity or verifying whether an entity is what or who it claims to be. Context-aware authentication mechanisms assess identity claims based on user, environment, application, and resource attributes, thus enabling continuous and adaptive authentication. Context-aware mechanisms mitigate authentication attacks while minimizing user burden and halting threats as soon as possible. For example, organizations should analyse time of day, location, and distance from the physical object before authorising data or system access. User identity is granted based on an algorithm sensitive to these attributes; for example, if access is attempted outside office hours and the user is more than 200 km from the office, a second factor of authentication via SMS could be triggered. More sensitive resources could require authentication via multiple channels.

8. **Compliance Alignment Score**

$$CAS = \lambda_1 PC + \lambda_2 IC_u + \lambda_3 T_{d_i,d_j} - \lambda_4 R_{access}$$

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

As private networks have expanded beyond physical boundaries to incorporate third-party and outside contingents, the risk from insider attacks has exponentially increased. Although organisations invest heavily in perimeter security, such as firewalls and network access control, the design of Wi-Fi networks is poorly considered. Extensive background work by organisations is generally required for the analysis of an employee's behaviour, which could happen over a period of years. Therefore, patterns should be examined and deviations from the patterns should trigger an alert in order to identify the insecure behaviour of trusted users quickly. This could help detect an insider or a compromised account, even when a trusted user accesses information that their role does not require.

Table 3. Context-Aware Authentication Factors

Authentication Factor	Example Input	Security Purpose
Time of Access	Office hours or non-office hours	Detects unusual access timing
User Location	Country, city, GPS region, network zone	Identifies abnormal login locations
Device Trust	Managed device, unknown device, jailbroken device	Evaluates endpoint reliability
Distance from Office	More than 200 km from expected workplace	Triggers additional verification
Resource Sensitivity	Public file, internal system, critical database	Adjusts authentication level

4. Data Governance and Compliance in Cross-Domain Environments

Cloud services have revolutionized software deployment, operation, and management, enabling agile startup processes for Web 2.0 businesses. Cloud vendors, such as Amazon and Salesforce, sell services supporting users' business functions, benefiting from economies of scale. Cloud providers frequently deploy cloud computing services, including Infrastructure-as-a-Service, Data-as-a-Service, Software-as-a-Service, and Platform-as-a-Service (PaaS), within their administrative domains. Emerging multi-domain cloud architectures combine cloud services from multiple providers' administrative domains. Some technologies enable service sharing across strict administrative boundaries, and specialized identity and privacy certification authorities ensure compliance with data governance and privacy laws for sensitive domain data.

Governance of data in cross-domain services, where sensitive data from various countries or customers are stored in the cloud, presents challenges. Data provenance, traced from origin to use, enables effect assessment and supports regulatory compliance by revealing who used sensitive data and when. For compliance, provenance must include a complete privacy expert certification authority chain, allowing domain compliance authorities to assess whether sensitive data use violates privacy policies. Cloud services can be combined to form complex solutions with required performance, availability, security, and privacy properties by leveraging a cloud fabric that supports Blueprint-based inter-domain cloud service composition.

9. **Adaptive MFA Trigger**

$$MFA(u) = \begin{cases} 1, & R_{access} \geq \tau_r \text{ or } BDS_u \geq \tau_b \\ 0, & otherwise \end{cases}$$

A. Data Provenance, Lineage, and stewardship

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

The provenance and lineage of data provide information about data sources and context, including the ownership and auditing of data-related tasks verified through data control. In a multi-domain environment with redundant data resources, particularly in a delay-tolerant environment where data redundancy is significant, data security, relevance, and quality control are crucial. Users require reliable provenance for data retrieval and thereby demand trustworthy models for their management, often centered around ownership. Data ownership is, therefore, one of the most important and sensitive issues in big data applications across distributed or multiple administrative domains.

Table 4. Multi-Domain Cloud Identity Security Challenges and Solutions

Challenge	Security Risk	Proposed Solution
Identity silos across cloud providers	Inconsistent access control and poor visibility	Identity Data Fabric
Multiple cloud service providers	Increased identity complexity	Federated Identity Management
Cross-border data access	Legal and regulatory violations	Policy-aware identity governance
Insider threats	Unauthorized access by trusted users	Behavioral monitoring and anomaly detection
Sensitive data movement	Weak traceability and audit gaps	Data provenance and lineage tracking
Static authentication	Inability to respond to changing risk	Context-aware adaptive authentication

One effective approach to solving the data ownership problem is the combination of data provenance and data stewardship, where a steward is a user or entity with rights to access, manage, and publish data. Stewardship of data similar to stewardship of biological species can involve collections of contributors, custodians, and users responsible for managing and providing quality data and information products useful for advancing scientific knowledge. A more precise definition of users is thus needed, one that identifies a root user or group of users with capabilities beyond other users.

10. **Secure Access Utility**

$$SAU = \eta_1 Security + \eta_2 Usability - \eta_3 Latency - \eta_4 Risk$$

5. Conclusion

Despite the proven advantages of cloud computing, the deployment of sensitive applications or services across multiple domains or regions still exhibits multiple risks, especially in the fields of identity and access management (IAM), data privacy, and service production. Identity systems migrating to the cloud must be designed considering the security and privacy concerns of cloud environments. In this context, multi-domain IAM systems need to be defined with a dedicated security point of view; the identity data management processes must be made compliant with the General Data Protection Regulation (GDPR) regulation, and it must be possible to define breed services that, by their characteristics, do not require data tracing functionality,

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

potentially allowing for the final reduction of data storage already at the design phase.

This study defines the concept of Adaptive Identity Intelligence and identifies the elements required to create an Adaptive Identity Framework composed of several interconnected Logical Sub-Systems able to control Identity Services and their operation. The concept of Federated Identity is expressed in a more general form called Federated Identity Intelligence, which is further articulated into Federated Identity Control Plane and Federated Identity Data Plane. Examples of Logical Sub-Systems belonging to the Adaptive Identity Intelligence Logical Architecture are presented, as well as some possible applications in the context of Multi-Domain Cloud Computing, GDPR compliance, and service design.

Acknowledgment

Research results presented form part of a project conducted by the Research Institute for the Defence of the Republic of Poland and Almost Anything Cloud Systems under Cloud and Network Infrastructure in Defence project, supported by the National Centre for Research and Development within Strategic Research Programme.

Realising the Cloud Computing Security Requirements Failure to design and implement security controls that address the security requirements identified during cloud risk assessments has led to serious breaches and data loss incidents. The exposure and loss of large quantities of confidential personal, government, and commercial data has focused attention on Cloud Service Providers (CSP) and the security controls they put in place to protect customers data. Customers may use third-party tools to assess cloud security, to provide them with independent assurance that the CSP is taking the necessary steps to protect their data; however such tools provide generic cloud security advice and do not reflect the actual controls applied by any one CSP. This paper discusses the research and development of a cloud security controls requirement specification tool that provides guidelines to Cloud Security Accreditation Commissions by determining what security controls a CSP has in place. The proposed cloud security controls specification tool is mapped to the widely-cited Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. The tool extracts details either from three benchmark datasets or directly from the CSP, providing customers with the information they need to make informed decisions about their choice of cloud provider.

Reference

1. He, H., Zheng, L., Li, P., Deng, L., Huang, L., & Chen, X. (2020). An efficient attribute-based hierarchical data access control scheme in cloud computing. Human-Centric Computing and Information Sciences, 10, Article 49.
2. Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, M. S., Watters, P. A., Ng, A., Hammoudeh, M., Badsha, S., & Kumara, I. (2020). A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. Sensors, 20(9), Article 2464.
3. Sriram, H. K., Adusupalli, B., Singreddy, S., & Malempati, M. (2021). Revolutionizing risk assessment and financial ecosystems with smart automation, secure digital solutions, and advanced analytical frameworks. Murali, Revolutionizing Risk Assessment and

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

Financial Ecosystems with Smart Automation, Secure Digital Solutions, and Advanced Analytical Frameworks (December 27, 2021).

4. Kayes, A. S. M., Rahayu, W., Watters, P., Alazab, M., Dillon, T., & Chang, E. (2020). Achieving security scalability and flexibility using fog-based context-aware access control. Future Generation Computer Systems, 107, 307–323.
5. Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, 166, Article 102731.
6. Mashetty, S. (2022). Enhancing Financial Data Security And Business Resiliency In Housing Finance: Implementing AI-Powered Data Analytics, Deep Learning, And Cloud-Based Neural Networks For Cybersecurity And Risk Management. Migration Letters, 19(6), 1302-1818.
7. Pöhn, D., & Hommel, W. (2020). An overview of limitations and approaches in identity management. Proceedings of the 15th International Conference on Availability, Reliability and Security, Article 90, 1–10.
8. Raja, S., Kumar, B. A., & Venkatesan, G. K. D. (2020). A security-attribute-based access control along with user revocation for shared data in multi-owner cloud system. Information Security Journal: A Global Perspective, 30(6), 309–324.
9. Choi, E.-B. (2020). An entity attribute-based access control model in cloud environment. Journal of Convergence for Information Technology, 10(10), 32–39.
10. Wang, J., et al. (2020). A fully distributed hierarchical attribute-based encryption scheme. Theoretical Computer Science, 815, 25–46.
11. Recharla, M. (2020). Targeted Gene Therapy for Spinal Muscular Atrophy: Advances in Delivery Mechanisms and Clinical Outcomes. International Journal of Science and Research (IJSR), 9(12), 1921-1934.
12. Li, H., Deng, L., Yang, C., & Liu, J. (2020). An enhanced media ciphertext-policy attribute-based encryption algorithm on media cloud. Mobile Information Systems, 2020, Article 8420186.
13. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alazab, M., & Watters, P. (2020). ABC-RuleMiner: User behavioral rule-based machine learning method for context-aware intelligent services. Journal of Network and Computer Applications, 154, Article 102480.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

14. McIntosh, T., Watters, P., Kayes, A. S. M., Ng, A., & Chen, Y. P. P. (2021). Enforcing situation-aware access control to build malware-resilient file systems. Future Generation Computer Systems, 115, 568–582.
15. Paleti, S. (2021). Cognitive core banking: A data-engineered, AI-infused architecture for proactive risk compliance management. AI-Infused Architecture for Proactive Risk Compliance Management (December 21, 2021).
16. Xie, M., Ruan, Y., Hong, H., & Shao, J. (2021). A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices. Future Generation Computer Systems, 121, 114–122.
17. Paul, N. R. R., & Raj, D. P. (2021). Enhanced trust based access control for multi-cloud environment. Computers, Materials & Continua, 69(3), 3079–3093.
18. Mamdouh, M., Awad, A. I., Khalaf, A. A. M., & Hamed, H. F. A. (2021). Authentication and identity management of IoHT devices: Achievements, challenges, and future directions. Computers & Security, 111, Article 102491.
19. Barreto, L., Fraga, J., & Siqueira, F. (2021). An intrusion tolerant identity provider with user attributes confidentiality. Journal of Information Security and Applications, 63, Article 103045.
20. Mukesh, A., & Aitha, A. R. (2021). Insurance Risk Assessment Using Predictive Modeling Techniques. International Journal of Emerging Research in Engineering and Technology, 2(4), 68-79.
21. Psarra, E., Verginadis, Y., Patiniotakis, I., Apostolou, D., & Mentzas, G. (2021). Accessing electronic health records in critical incidents using context-aware attribute-based access control. Intelligent Decision Technologies, 15(4), 667–679.
22. Zhong, H., Zhou, Y., Zhang, Q., Xu, Y., & Cui, J. (2021). An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. Future Generation Computer Systems, 115, 486–496.
23. Akinyele, J. A., et al. (2021). A multi-factor authentication-based framework for identity management in cloud applications. Computers, Materials & Continua, 71(2), 3193–3209.
24. Zhang, Y., et al. (2021). How to implement secure cloud file sharing using optimized attribute-based access control with small policy matrix and minimized

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 01 ISSUE: 01
RECEIVED: OCTOBER 03 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 08 PUBLISHED: NOVEMBER 17

cumulative errors. Computers & Security, 107, Article 102318.

25. Mostafa, A. M., Rushdy, E., Medhat, R., & Hanafy, A. (2022). Security and privacy in cloud computing: Technical review. Future Internet, 14(1), Article 11.
26. Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and risk aware access control for zero trust systems. Security and Communication Networks, 2022, Article 7026779.
27. Botlagunta, P. N., & Sheelam, G. K. (2020). Data-Driven Design and Validation Techniques in Advanced Chip Engineering. Global Research Development (GRD) ISSN, 2455-5703.
28. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143–57179.
29. Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. Sustainability, 14(18), Article 11213.
30. Aghili, S. F., Sedaghat, M., Singelée, D., & Gupta, M. (2022). MLS-ABAC: Efficient multi-level security attribute-based access control scheme. Future Generation Computer Systems, 131, 75–90.
31. Inala, R. Designing Scalable Technology Architectures for Customer Data in Group Insurance and Investment Platforms.
32. Liao, C.-H., Guan, X.-Q., Cheng, J.-H., & Yuan, S.-M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. Future Generation Computer Systems, 135, 450–466.