International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

Continuous Trust Scoring for Cross-Layer Access Governance in S/4HANA, Fiori, and SAP BTP

Venkata Rao Yadavalli

MYGO Consulting Inc, USA

ABSTRACT: Modern SAP landscapes span multiple technology layers including SAP S/4HANA, SAP Fiori, SAP Business Technology Platform (BTP), cloud identity services, and external enterprise applications. Traditional role-based access control approaches provide limited visibility into evolving access risks across these interconnected environments. This paper proposes a Continuous Trust Scoring framework that dynamically evaluates enterprise access risk using behavioral analytics and cross-platform identity intelligence. The proposed architecture continuously analyzes authentication events, authorization changes, user behavior patterns, application context, segregation-of-duty policies, and cloud identity relationships to generate adaptive trust scores for individual users, service accounts, and business processes. Machine learning algorithms identify anomalous access behavior while graph analytics detect privilege escalation pathways across enterprise systems. The framework supports automated policy enforcement, continuous compliance monitoring, and proactive access governance without relying solely on periodic audit activities. A simulation-based evaluation illustrates improved detection of access anomalies, reduced governance overhead, and enhanced enterprise security posture across hybrid SAP landscapes. The Continuous Trust Scoring model establishes an adaptive governance architecture capable of supporting Zero Trust security principles within complex cloud-enabled ERP ecosystems.

KEYWORDS: Continuous Trust Scoring; Zero Trust Architecture; SAP S/4HANA; SAP Fiori; SAP Business Technology Platform; Identity and Access Management; User and Entity Behavior Analytics; Graph Analytics; Segregation of Duties; Continuous Compliance Monitoring; Adaptive Access Governance

I. INTRODUCTION

Enterprise resource planning landscapes built around SAP S/4HANA have evolved from monolithic, on premise deployments into distributed ecosystems combining S/4HANA business logic, SAP Fiori, SAP Business Technology Platform (BTP), cloud identity providers, and third party applications connected through APIs. Each layer introduces its own authentication mechanism, authorization model, and audit trail, while access governance has historically treated these domains separately.

Traditional governance relies on role based access control (RBAC), segregation of duties (SoD) rules, and periodic access certification through SAP Governance, Risk, and Compliance (GRC) tooling (Sandhu et al., 1996; Little & Best, 2003). These controls remain necessary, but they are largely point in time. A role assignment may be checked when granted or during periodic recertification, while changes in user behavior, device context, and cross system entitlements can occur between reviews. In a landscape spanning S/4HANA, Fiori, BTP, and federated identity, effective access risk depends on signals distributed across all layers.

Zero Trust principles address this limitation by replacing implicit trust with continuous verification of identity, device, and behavioral context (Rose et al., 2020; Kindervag, 2010). UEBA, adaptive authentication, and conditional access operationalize these principles in general enterprise IT (Shashanka et al., 2016; Chandola et al., 2009). In SAP, however, GRC Access Control, BTP authorization through XSUAA, and cloud identity services largely operate as separate control planes.

This paper proposes a Continuous Trust Scoring (CTS) framework for cross-layer access governance across SAP S/4HANA, SAP Fiori, and SAP BTP. CTS treats trust as a continuously recomputed, bounded score derived from behavioral analytics, graph-based privilege escalation analysis, and SoD and compliance evaluation. The score is used to support adaptive policy enforcement while complementing existing SAP authorization and governance controls.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

II. RELATED WORK

Relevant research spans access control models, behavioral and graph-based anomaly detection, Zero Trust architecture, and SAP specific governance. RBAC provides the foundation for SAP authorization, while ABAC adds dynamic attributes to static role structures (Sandhu et al., 1996; Ferraiolo et al., 2001; Hu et al., 2014, 2017). Hybrid RBAC and ABAC models demonstrate the feasibility of layering contextual evaluation on existing roles (Kuhn et al., 2010).

Anomaly detection research has progressed from traditional intrusion detection to machine learning methods suitable for enterprise behavior analytics (Denning, 1987; Chandola et al., 2009; Buczak & Guven, 2016). Isolation Forest and autoencoder based reconstruction error provide complementary approaches for tabular and sequential behavior (Liu et al., 2008; Sakurada & Yairi, 2014). graph-based methods analyze anomalous structures and attack paths, providing a basis for modeling relationships among identities, roles, scopes, and critical privileges (Noble & Cook, 2003; Eberle & Holder, 2009; Akoglu et al., 2015; Homer et al., 2013).

Zero Trust was formalized by NIST as continuous, identity centered verification rather than implicit trust (Rose et al., 2020; Kerman et al., 2020). SAP and ERP governance research, in contrast, has focused strongly on SoD and role based controls, with SAP documentation describing security mechanisms within individual layers (Little & Best, 2003; SAP SE, 2020, 2021, 2022). Cloud IAM research identifies federated identity and continuous risk evaluation as continuing challenges in hybrid environments (Indu et al., 2018). Collectively, these streams establish the technical foundations but do not provide a unified trust measure across S/4HANA, Fiori, and BTP.

Research Stream	Representative Work	Core Contribution	Gap Relative to Cross-Layer SAP Governance
RBAC / ABAC	Sandhu et al. (1996); Hu et al. (2014, 2017)	Static and attribute-driven access decision models	Evaluates access at grant/request time, not continuously; no cross-platform identity fusion
Behavioral analytics (UEBA)	Chandola et al. (2009); Shashanka et al. (2016); Liu et al. (2008)	Statistical/ML baselining of user behavior	Not integrated with SAP-specific authorization semantics or SoD rules
Graph-based anomaly detection	Noble & Cook (2003); Akoglu et al. (2015); Homer et al. (2013)	Structural analysis of relationship graphs for anomalies/attack paths	Applied mainly to network vulnerabilities, not identity entitlement graphs
Zero Trust Architecture	Kindervag (2010); Rose et al. (2020); Kerman et al. (2020)	Architecture-agnostic continuous verification principles	Silent on how to fuse ABAP-core, BTP, and federated-identity risk signals
SAP / ERP SoD research	Simon & Zurko (1997); Little & Best (2003)	Formal SoD conflict definitions applied to SAP	Rule-based and largely periodic; not behavior-adaptive or cross-layer
Cloud IAM surveys	Indu et al. (2018)	Identification of cross-domain IAM challenges	Diagnostic rather than prescriptive; no scoring architecture proposed

Table.1. Related Work Comparison

III. RESEARCH GAP

Three gaps motivate CTS. First, SAP access governance commonly evaluates role and SoD risk at assignment time or during periodic review, leaving behavioral drift between reviews insufficiently visible (Little & Best, 2003; SAP SE, 2022). Second, behavioral and graph analytics are mature in general cybersecurity but have not been jointly adapted to the heterogeneous telemetry and authorization semantics of S/4HANA, Fiori, and BTP (Chandola et al., 2009; Liu et al., 2008; Akoglu et al., 2015). Third, Zero Trust reference architectures are deliberately platform agnostic and do not specify a concrete identity correlation and trust scoring mechanism for the SAP ecosystem (Rose et al., 2020; Kerman et al., 2020).

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

CTS addresses these gaps by correlating cross platform identities, combining behavioral, graph, and SoD signals, and translating the resulting trust score into graduated governance actions. The framework is designed as an additive control layer rather than a replacement for SAP GRC, existing authorization models, or BTP authorization services.

IV. PROPOSED CONTINUOUS TRUST SCORING FRAMEWORK

The CTS framework is organized as a four layer pipeline, illustrated in Figure 1: cross-layer telemetry sources, an identity correlation and feature fabric, a trust scoring and analytics engine, and trust score fusion with adaptive policy enforcement. The identity layer resolves a canonical identity across S/4HANA user IDs, Fiori sessions, BTP identities, and federated identity provider subjects while preserving native telemetry formats.

The analytics engine runs three components in parallel: behavioral analytics, graph analytics for privilege escalation, and an SoD and compliance reasoner. Layer 4 fuses these component scores into a single trust value and maps trust transitions to enforcement actions, with GRC and SIEM integration supporting auditability and model feedback.

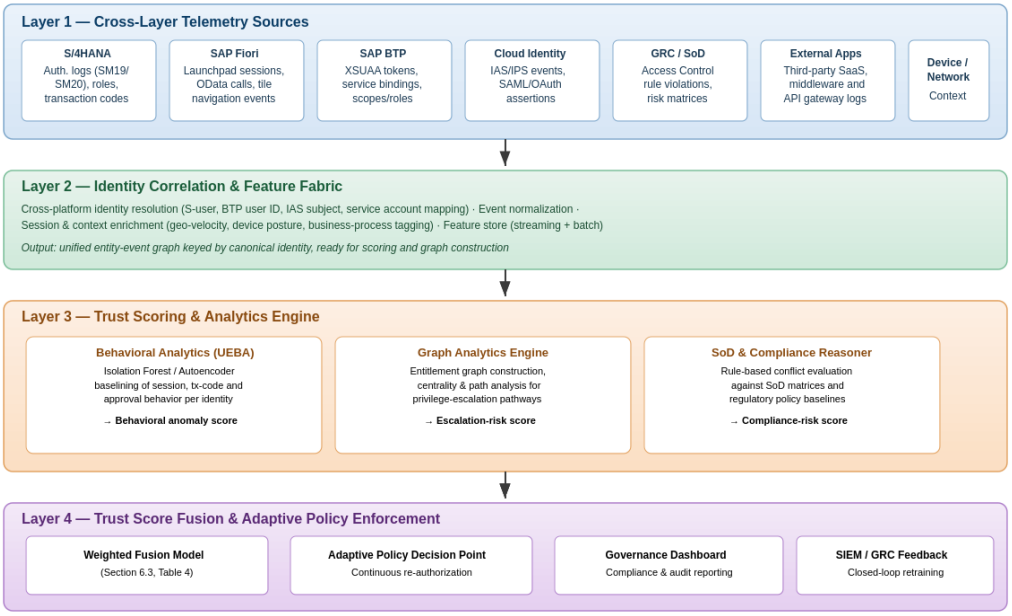


Figure.1. Layered architecture of the proposed Continuous Trust Scoring framework spanning telemetry, identity correlation, analytics, and enforcement

V. CROSS-LAYER ACCESS GOVERNANCE ARCHITECTURE

Figure 2 presents the governance model from a complementary perspective, emphasizing the relationship among an identity core and platform, application, and ecosystem layers. The identity core represents the canonical cross platform identity. The platform layer captures S/4HANA and BTP authorization state, the application layer captures Fiori session and navigation context, and the ecosystem layer captures federated identity relationships and external application access.

Five principles apply across the architecture: no implicit trust, identity as the control plane, continuous rescoring, cross-layer correlation, and evidence based compliance. A signal originating in one layer can therefore influence enforcement in another, while governance remains grounded in the existing SAP control environment.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

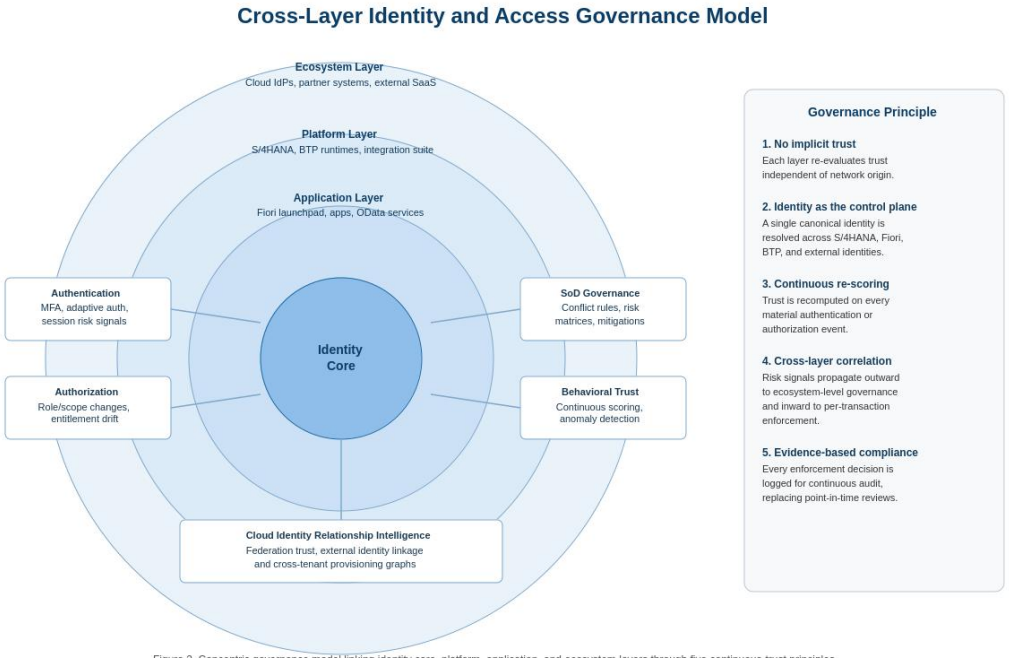


Figure.2. Concentric governance model linking identity core, platform, application, and ecosystem layers through five continuous trust principles.

Layer	Source System	Native Identifier	Correlation Mechanism
Core ERP	SAP S/4HANA (ABAP stack)	S-user / SU01 user ID	Directly mapped to canonical identity via user master synchronization
Application	SAP Fiori Launchpad / Gateway	Fiori/Gateway session user	Inherits ABAP-stack user ID via single sign-on session token
Platform	SAP BTP (Cloud Foundry / Kleros runtimes)	XSUAA subject (JWT sub claim)	Mapped via identity-provider federation attribute matching S-user
Identity	SAP Cloud Identity Services (IAS/IPS)	SAML NameID / OIDC subject	Serves as the federation anchor linking on-premise and cloud identifiers
Governance	SAP GRC Access Control	Risk analysis user/role key	Joined to canonical identity for SoD and role-risk enrichment
Ecosystem	External SaaS / API gateway	OAuth client or delegated user token	Linked opportunistically via service-account registry and token introspection

Table.2. cross-layer Identity Sources

VI. METHODOLOGY

This research follows a design science methodology based on conceptual framework development informed by published literature and SAP platform documentation. Requirements were derived from the research gaps and cross checked against documented S/4HANA security mechanisms and BTP XSUAA authorization. The architecture, entitlement graph, and trust fusion model were then designed to satisfy the research objectives while remaining additive to existing controls.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

Representative feature sets, weights, and enforcement thresholds were specified as illustrative defaults requiring organizational calibration. Because production SAP telemetry was not available, evaluation uses a synthetic identity population and event stream to illustrate expected detection behavior. The results are therefore explicitly simulation based and are not presented as empirical validation.

VII. MACHINE LEARNING AND GRAPH ANALYTICS MODELS

The behavioral component establishes a per identity baseline over session and transaction features. Isolation Forest is applied to session level features because it supports high dimensional mixed type data without requiring a labeled anomaly set (Liu et al., 2008), while an autoencoder reconstruction error model captures anomalous sequence behavior (Sakurada & Yairi, 2014). Features include login time deviation, geo velocity, device changes, transaction or Fiori app sequences, entitlement changes, and federation context.

The graph component constructs a directed entitlement graph in which nodes represent identities, roles, role collections, scopes, and critical transactions or authorization objects. Edges represent assignment, inheritance, or delegation. For each identity, shortest path distance and centrality to tagged critical nodes are computed using approaches adapted from attack graph aggregation and graph anomaly detection (Noble & Cook, 2003; Homer et al., 2013; Akoglu et al., 2015). The escalation risk is expressed as a sensitivity weighted, distance discounted sum, allowing short paths to critical privileges to receive greater risk.

The feature schema combines behavioral, entitlement, structural, and compliance signals. SoD evaluation remains rule based, while federation anomalies are assessed through rule based and anomaly scoring.

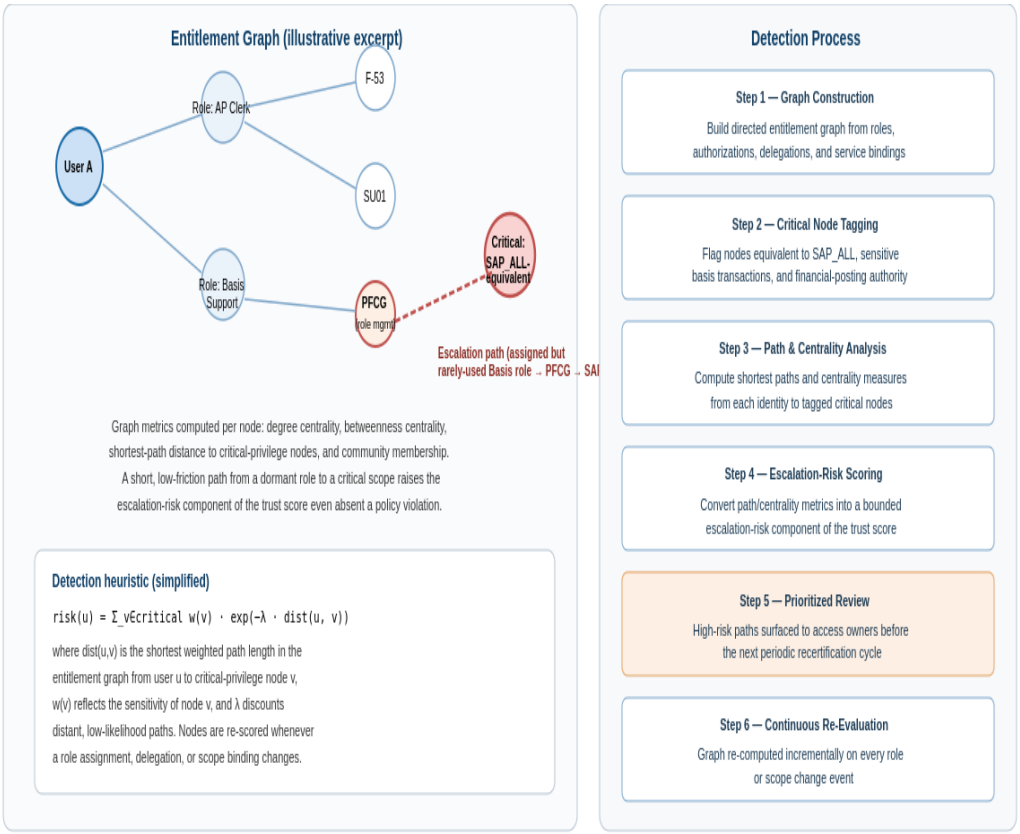


Figure .4.End to end machine learning and graph analytics pipeline underlying the Continuous Trust Scoring engine

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

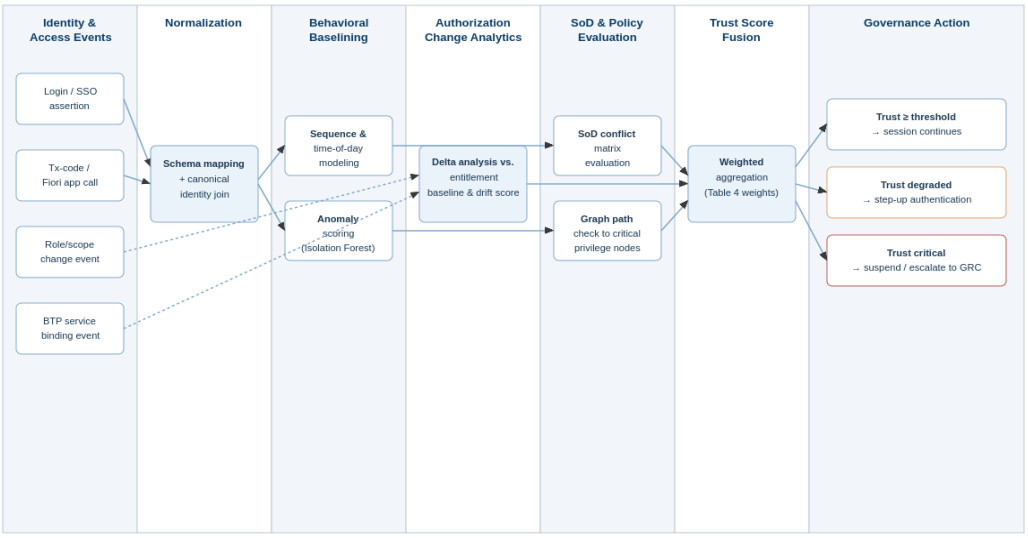


Figure.5. Illustrative entitlement graph and process for detecting privilege escalation pathways ahead of periodic access review.

Feature Category	Representative Features	Analytic Method	Primary Layer Source
Session behavior	Login time-of-day deviation, geo-velocity, device fingerprint change	Isolation Forest (Liu et al., 2008)	S/4HANA, Fiori, Cloud Identity
Transaction sequence	Tx-code / Fiori-app n-gram sequence, sequence entropy	Autoencoder reconstruction error (Sakurada & Yairi, 2014)	S/4HANA, Fiori
Entitlement change	Role/scope grant frequency, dormant-role activation	Statistical drift scoring vs. rolling baseline	S/4HANA GRC, BTP XSUAA
Entitlement structure	Shortest-path distance to critical node, betweenness centrality	Graph analytics (Noble & Cook, 2003; Homer et al., 2013)	SAP GRC entitlement export, BTP role collections
SoD / compliance	Active SoD rule violations, mitigation control coverage	Rule-based conflict evaluation	SAP GRC Access Control
Federation context	Cross-tenant provisioning anomalies, IdP assertion risk	Rule-based + anomaly scoring	SAP Cloud Identity Services

Table.3. Machine Learning and Graph Analytics Features

VIII. TRUST SCORING ENGINE

The trust scoring engine fuses behavioral anomaly B(u), graph-based escalation risk G(u), and SoD and compliance risk C(u) into a bounded trust value T(u) in [0,1]: $T(u) = 1 - (wB \cdot B(u) + wG \cdot G(u) + wC \cdot C(u))$, where the weights sum to one and are illustrative defaults subject to organizational calibration. A linear fusion function is used so that each component's contribution remains auditable when a score changes.

Trust scores are recomputed on an event triggered basis. Authentication events, authorization changes, or newly detected SoD violations invalidate the previous score and trigger recomputation, consistent with continuous verification principles (Rose et al., 2020).

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

Component	Description	Default Weight	Calibration Note
Behavioral anomaly, B(u)	Isolation Forest / autoencoder anomaly score, normalized to [0,1]	0.40	Increase for identities with rich historical session data; decrease for new hires
Escalation risk, G(u)	Graph-based distance/centrality score to critical entitlement nodes	0.35	Increase in landscapes with flat, broadly scoped BTP role collections
Compliance risk, C(u)	Active SoD violations and mitigation control coverage	0.25	Increase where regulatory scope (e.g., SOX) is broad
Fusion output, T(u)	Bounded trust score in [0,1] driving policy enforcement	n/a	Thresholds in Table 6 require organization-specific tuning before production use

Table.4. Trust Scoring Factors and Weights (Illustrative Defaults)

IX. POLICY ENFORCEMENT FRAMEWORK

Policy enforcement is graduated rather than binary. A normal trust band permits the session to continue, a degraded band triggers step up authentication or supplementary logging, and a critical band triggers session suspension and escalation to a human reviewer through GRC and SIEM integration. Figures 3 and 6 show the resulting workflow and dashboard representation.

Every enforcement action and its supporting trust components are logged for continuous compliance evidence and for model recalibration. This preserves an auditable link between the observed signal, the trust decision, and the resulting governance action, consistent with continuous auditing research (Alles et al., 2008).

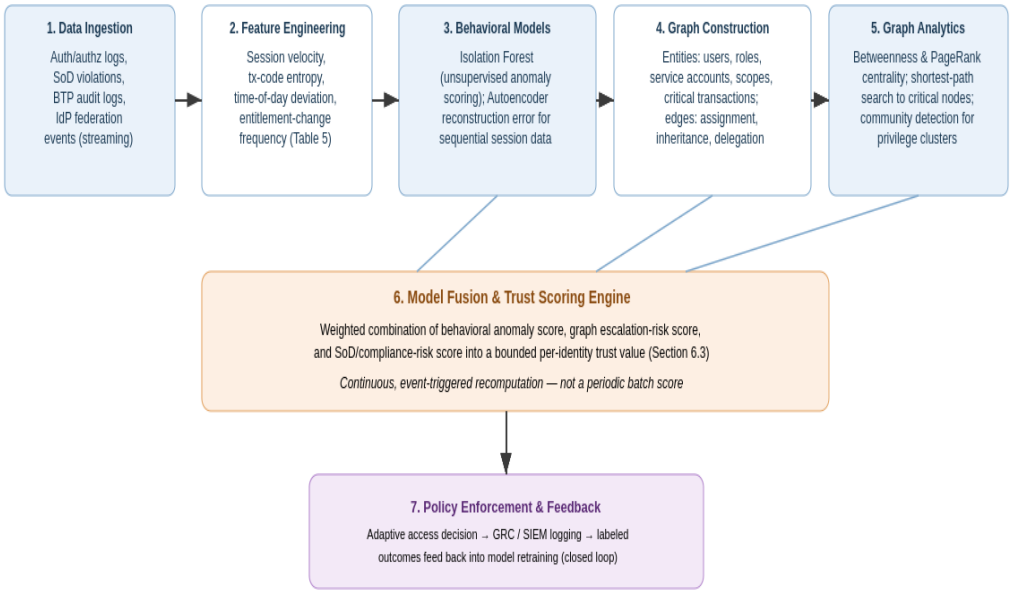


Figure.3. End to end analytics workflow from raw authentication and authorization events to graduated governance actions

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

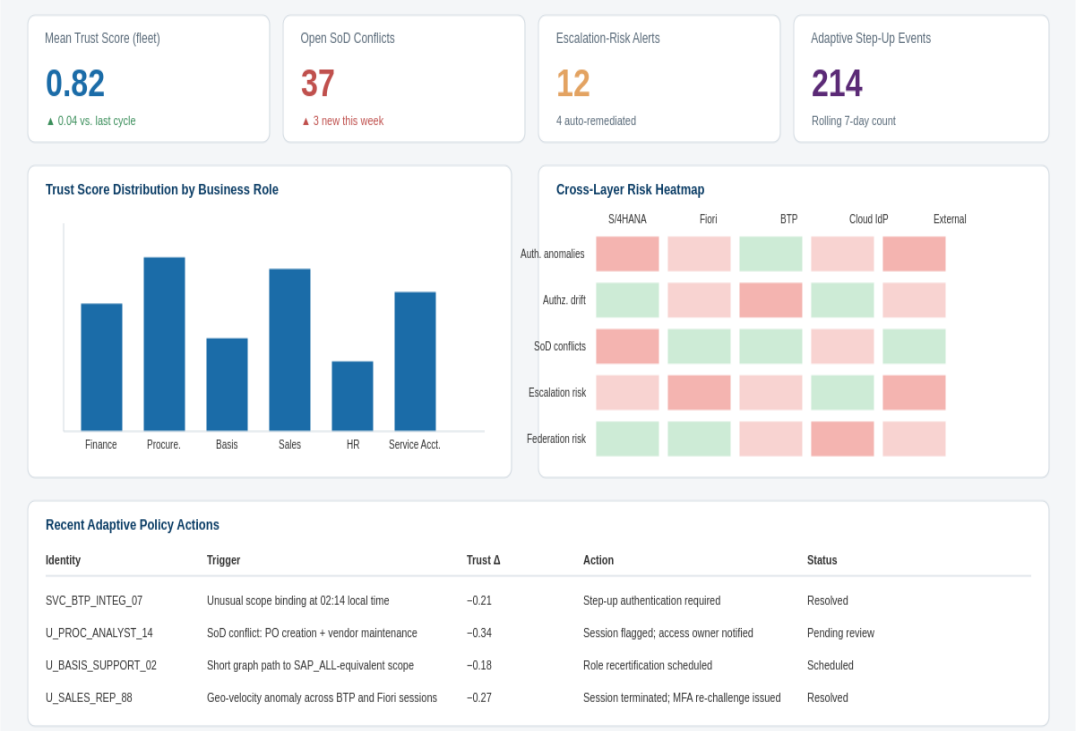


Figure.6. Illustrative governance dashboard combining trust score analytics, cross-layer risk heatmapping, and adaptive enforcement actions.

X. EVALUATION METHODOLOGY

Because CTS had not been deployed against production SAP telemetry at the time of writing, evaluation uses an illustrative simulation. A synthetic population of 5,000 identities, including business users, technical support roles, and service accounts, was generated with entitlement structures informed by documented SAP role patterns and SoD conflicts (Little & Best, 2003). A synthetic event stream combined normal behavior with injected anomalous sequences representing SoD conflicting transactions, dormant role activation, and short path privilege escalation.

The CTS pipeline was applied to this event stream and compared with a periodic review baseline that flags identities with explicit SoD violations on a simulated quarterly cadence. Evaluation considered precision, recall, F1, AUC, mean time to detect, governance review effort, and false positive rate. All numerical results are illustrative outputs of the synthetic evaluation.

XI. RESULTS

The simulation produced a higher separation between injected anomalous and normal identities for the fused CTS model than for the behavioral only and periodic SoD review baselines. The main relative improvement was in detection time: the periodic baseline can miss anomalies that do not correspond to an explicit SoD violation until its next review, whereas event triggered CTS identifies corresponding synthetic sessions within the same simulated session window.

The simulation also reduced governance review effort by risk ranking alerts rather than presenting an undifferentiated list. Table 5 reports illustrative precision of 0.87, recall of 0.90, and F1 of 0.88 for CTS, compared with 0.58, 0.41, and 0.48 for the periodic baseline. Mean time to detect was approximately 90 days for the simulated quarterly baseline and less than one session window for CTS. These values demonstrate the intended behavior of the framework and should not be interpreted as production performance guarantees.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

Figure 7 summarizes the simulated detection and efficiency comparison.



Figure.7. Illustrative, simulation based detection and efficiency comparisons between the proposed CTS model and a periodic review baseline

Metric	Periodic-Review Baseline	Continuous Trust Scoring (Simulated)	Direction
Precision	0.58 (simulated)	0.87 (simulated)	Higher is better
Recall	0.41 (simulated)	0.90 (simulated)	Higher is better
F1-score	0.48 (simulated)	0.88 (simulated)	Higher is better
Mean time-to-detect	~90 days (quarterly cycle, simulated)	< 1 session window (simulated)	Lower is better
Governance review effort	High, undifferentiated (simulated)	Reduced via risk-ranked prioritization (simulated)	Lower is better
False positive rate	Low but slow (simulated)	Moderate, tunable via threshold (simulated)	Lower is better

Table.5. Comparative Performance Analysis (Illustrative Simulation)

XII. DISCUSSION

The results are consistent with the framework's design intent. Fusing behavioral, graph structural, and rule based compliance signals should detect a broader range of access risk because each component addresses a different failure mode: statistical deviation, structural escalation opportunity, and explicit policy violation. The magnitude of improvement should not be over interpreted because the synthetic anomaly injection was designed by the same authors who designed the model and is therefore likely to be more favorable than real adversarial behavior.

Auditability is another central design consideration. The linear weighted fusion function was selected over a more opaque learned combiner so that trust score changes remain explainable within financial and access governance controls. CTS is also additive rather than substitutive: it consumes outputs from SAP GRC, S/4HANA authorization, and BTP authorization instead of replacing them.

XIII. LIMITATIONS

The evaluation is simulation based and does not use production SAP telemetry. The synthetic population and injected anomalies cannot fully capture real enterprise behavior or adaptive adversaries. Cross platform identity correlation may also be incomplete where provisioning practices are inconsistent or local BTP accounts are unmanaged, which could reduce trust score accuracy.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

The weights and thresholds require organization specific calibration, while graph analysis depends on accurate and current tagging of critical nodes. Documentation and historical data quality may also affect behavioral analytics. Finally, adaptive enforcement introduces operational risk if false positives are excessive, which is why the framework uses graduated and auditable actions rather than automatic hard blocking.

XIV. FUTURE WORK

Future research should validate CTS against anonymized production SAP telemetry under appropriate data protection safeguards and replace simulation results with empirical measurements. Comparative evaluation of linear fusion against nonlinear or learned fusion methods could quantify the tradeoff between predictive performance and interpretability.

The entitlement graph could be extended with temporal analysis to capture how privilege escalation pathways change as roles and scopes evolve. Future work should also examine adversarial robustness, including slow privilege acquisition designed to remain below anomaly thresholds, a concern established in general intrusion detection research (Sommer & Paxson, 2010).

XV. CONCLUSION

This paper proposed a Continuous Trust Scoring framework for cross-layer access governance across SAP S/4HANA, SAP Fiori, and SAP BTP. The framework addresses the gap between periodic, platform specific access controls and Zero Trust principles by fusing behavioral analytics, entitlement graph analysis, and SoD and compliance evaluation into a continuously recomputed, auditable trust score that drives graduated policy enforcement.

An illustrative simulation suggests that the approach can detect access anomalies earlier and reduce undifferentiated review effort compared with periodic SoD review alone. These findings remain simulation based and require empirical validation against production telemetry before deployment conclusions can be drawn. The framework and evaluation method therefore provide a foundation for subsequent SAP security research and empirical refinement.

Research integrity and reproducibility

The quantitative results in this manuscript are simulation-based unless a cited external study is explicitly identified. They are not audited production outcomes and should not be generalized beyond the stated assumptions. Before submission, the authors should archive the synthetic-data generator or input dataset, parameter definitions, random seeds, model and software versions, source code, raw outputs, and analysis scripts in a persistent repository and replace this statement with the repository DOI. The reported study uses no human participants or personal data.

Funding, competing interests, author contributions, and data/code availability must be completed in the format required by the selected journal before submission.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19 to 31.
2. Akoglu, L., Tong, H., & Koutra, D. (2015). graph-based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 29(3), 626 to 688.
3. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. Journal of Information Systems, 22(2), 195 to 214.
4. Anderson, J. P. (1980). Computer security threat monitoring and surveillance. James P. Anderson Co.
5. Botha, R. A., & Eloff, J. H. P. (2001). Separation of duties for access control enforcement in workflow environments. IBM Systems Journal, 40(3), 666 to 682.
6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153 to 1176.
7. Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. International Journal of Accounting Information Systems, 12(2), 152 to 160.
8. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15.
9. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222 to 232.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401007

10. Eberle, W., & Holder, L. (2009). Anomaly detection in data represented as graphs. Intelligent Data Analysis, 13(4), 663 to 689.
11. Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 4(3), 224 to 274.
12. Garbis, J., & Chapman, J. W. (2021). Zero trust security: An enterprise guide. Apress.
13. Homer, J., Zhang, S., Ou, X., Schmidt, D., Du, Y., Rajagopalan, S. R., & Singhal, A. (2013). Aggregating vulnerability metrics in enterprise networks using attack graphs. Journal of Computer Security, 21(4), 561 to 597.
14. Hu, V. C., Ferraiolo, D. F., Chandramouli, R., & Kuhn, D. R. (2017). Attribute-based access control. Artech House.
15. 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). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162
16. Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), 574 to 588.
17. Kerman, A., Borchert, O., Rose, S., & Tan, A. (2020). Implementing a zero trust architecture (Project description). National Cybersecurity Center of Excellence, National Institute of Standards and Technology.
18. Kindervag, J. (2010). No more chewy centers: Introducing the zero trust model of information security. Forrester Research.
19. Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding attributes to role-based access control. IEEE Computer, 43(6), 79 to 81.
20. Little, A. G., & Best, P. J. (2003). A framework for separation of duties in an SAP R/3 environment. Managerial Auditing Journal, 18(5), 419 to 430.
21. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In Proceedings of the 2008 Eighth IEEE International Conference on Data Mining (pp. 413 to 422). IEEE.
22. Lunt, T. F. (1993). A survey of intrusion detection techniques. Computers & Security, 12(4), 405 to 418.
23. Molloy, I., Chen, H., Li, T., Wang, Q., Li, N., Bertino, E., Calo, S., & Lobo, J. (2010). Mining roles with multiple objectives. ACM Transactions on Information and System Security, 13(4), Article 36.
24. Noble, C. C., & Cook, D. J. (2003). Graph-based anomaly detection. In Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 631 to 636). ACM.
25. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
26. Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. In Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis (pp. 4 to 11). ACM.
27. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2), 38 to 47.
28. SAP SE. (2020). Security guide for SAP S/4HANA 2020. SAP Help Portal.
29. SAP SE. (2021). Security administration: Managing authentication and authorization of the SAP Business Technology Platform. SAP Help Portal.
30. SAP SE. (2021). Security guide for SAP S/4HANA 2021. SAP Help Portal.
31. SAP SE. (2022). Security guide for SAP S/4HANA 2022. SAP Help Portal.
32. Shashanka, M., Shen, M.-Y., & Wang, J. (2016). User and entity behavior analytics for enterprise security. In 2016 IEEE International Conference on Big Data (Big Data) (pp. 1867 to 1874). IEEE.
33. Simon, R. T., & Zurko, M. E. (1997). Separation of duty in role-based environments. In Proceedings of the 10th Computer Security Foundations Workshop (pp. 183 to 194). IEEE.
34. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305 to 316). IEEE.
35. Vaidya, J., Atluri, V., & Guo, Q. (2007). The role mining problem: Finding a minimal descriptive set of roles. In Proceedings of the 12th ACM Symposium on Access Control Models and Technologies (pp. 175 to 184). ACM.
36. Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. Auditing: A Journal of Practice & Theory, 10(1), 110 to 125.
37. Xu, Z., & Stoller, S. D. (2015). Mining attribute-based access control policies. IEEE Transactions on Dependable and Secure Computing, 12(5), 533 to 545.