International Journal of Engineering & Extended Technologies Research (IJEETR)

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

AI-Driven Big Data Analytics for Secure, Privacy-Centric Web Applications in SAP Ecosystems

Maheshwari Muthusamy

Team Lead, Infosys, Jalisco, Mexico

ABSTRACT: The convergence of machine learning, big data, web technologies, and generative AI has transformed enterprise data processing while introducing complex cybersecurity and privacy challenges, particularly within SAP-based digital ecosystems. This paper presents an integrated analytical framework that combines machine learning and big data analytics with generative AI to enhance secure data management, intelligent web-based interactions, and privacy preservation in SAP environments. The proposed approach leverages scalable big data pipelines to process heterogeneous web and enterprise data, while machine learning models enable real-time threat detection, anomaly identification, and predictive risk assessment. Generative AI is employed to automate data synthesis, policy enforcement, and adaptive security responses, improving system resilience against evolving cyber threats. Privacy-aware mechanisms, including data anonymization and access control, are incorporated to ensure regulatory compliance and trust. The framework demonstrates improved cybersecurity intelligence, data governance, and operational efficiency, positioning SAP platforms as robust and privacy-centric enterprise solutions in large-scale digital infrastructures.

KEYWORDS: Machine Learning, Big Data Analytics, Generative AI, Cybersecurity, Data Privacy, Web Technologies, SAP Systems

I. INTRODUCTION

Effective organizational decision-making increasingly depends on the ability to synthesize vast amounts of operational, strategic, financial, and risk data in real time. Traditional business intelligence (BI) systems that rely on retrospective reporting and static dashboards are no longer sufficient to meet the demands of rapidly changing markets, evolving cybersecurity threats, and hybrid cloud deployments. As enterprises embrace digital transformation, they face three converging imperatives: the need to deliver **decision intelligence** that integrates analytics with action, the need to protect assets and processes via **AI-based cybersecurity**, and the need to leverage **multi-cloud infrastructures** for scalability, resilience, and innovation.

Decision intelligence refers to the systematic application of data, analytics, and domain knowledge to drive better decisions across organizational processes. It encompasses descriptive, diagnostic, predictive, and prescriptive analytics, often augmented by artificial intelligence and machine learning. Decision intelligence aims not only to reveal insights but also to guide actions that align with strategic goals. In large enterprises, SAP systems often serve as the backbone of operational data processing, enterprise resource planning (ERP), customer relationship management (CRM), and analytics. SAP's suite of intelligent enterprise solutions — including SAP S/4HANA, SAP Analytics Cloud, and SAP Business Technology Platform — provides rich sources of structured and unstructured data that can fuel decision intelligence.

At the same time, cybersecurity emerges as a central concern. Enterprises face sophisticated threats such as advanced persistent threats (APT), ransomware, and insider threats. Traditional signature-based security systems struggle to detect novel tactics, and isolated security tools can miss cross-system patterns. **AI-based cybersecurity** uses machine learning, behavioral analytics, and anomaly detection to identify potential threats across complex infrastructures, enabling adaptive defenses and faster response.

Finally, the adoption of **multi-cloud infrastructure** — distributing workloads across multiple public cloud providers or hybrid environments — provides flexibility and cost optimization. However, multi-cloud complexity introduces challenges related to data governance, interoperability, latency, and security consistency.

The intersection of these trends motivates the need for a unified framework where enterprise decision intelligence is powered by SAP's rich data and analytics capabilities, is secured by AI-driven cyber defenses, and operates seamlessly

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

across multi-cloud infrastructures. Such integration enables organizations to make faster, more accurate, and more secure decisions while leveraging the scalability and flexibility of cloud ecosystems.

This research examines how these three domains — SAP enterprise intelligence, AI-based cybersecurity, and multi-cloud infrastructure — can be combined into a cohesive architecture that supports organizational decision making, risk resilience, and operational agility. We explore foundational concepts, review existing approaches, identify gaps, and propose a structured methodology for implementation.

The remainder of this introduction elaborates on the motivations, challenges, and scope of this study. First, operational decision intelligence involves synthesizing data from multiple enterprise systems, including ERP, supply chain, HR, finance, and customer engagement platforms. SAP systems often serve as the "single source of truth" for such operational data, yet enterprises also rely on external data sources such as market feeds, IoT sensors, and third-party analytics. Integrating these disparate streams requires robust data orchestration layers capable of real-time ingestion, transformation, and storage. Furthermore, decision intelligence must span multiple analytical modes — from retrospective reporting to forward-looking predictions and prescriptive recommendations — necessitating diverse analytic techniques and scalable compute resources.

AI-based cybersecurity complements operational intelligence by proactively identifying threats that could compromise data integrity, availability, or confidentiality. Machine learning models can detect anomalous patterns in network traffic, user behavior, and application logs that signal attempted breaches. These insights must be integrated into the decision intelligence pipeline so that risk signals inform operational and strategic decisions. For example, a detected anomaly in transaction processing should not only trigger security alerts but also inform operational leaders about potential impacts on financial reporting or supply chain performance.

Multi-cloud infrastructure plays an enabling role, offering redundancy, scalability, and the ability to leverage best-of-breed cloud services. However, it also introduces friction: governance policies must ensure consistent security controls, data sovereignty requirements must be respected across regions, and cross-cloud interoperability must be maintained. Decision intelligence architectures must therefore abstract cloud heterogeneity while preserving performance and security.

The proposed research seeks to answer these key questions:

1. **How can decision intelligence be operationalized within SAP environments to support real-time and predictive decision making?**
2. **What role does AI-based cybersecurity play in protecting and informing enterprise decision processes?**
3. **How can multi-cloud infrastructure be orchestrated to support scalable, resilient, and compliant decision intelligence systems?**

By addressing these questions, the study aims to present a comprehensive framework that advances enterprise capabilities beyond siloed analytics, point cybersecurity tools, and isolated cloud implementations.

II. LITERATURE REVIEW

Decision Intelligence and Enterprise Analytics. Decision intelligence extends traditional business intelligence by coupling analytics with actionable recommendations. Researchers such as Davenport and Harris (2007) highlight how analytics can drive competitive advantage. Provost and Fawcett (2013) discuss the foundations of data science in supporting predictive insights. SAP's evolution from data warehousing toward real-time in-memory processing (e.g., SAP HANA) demonstrates industry convergence toward intelligent analytics platforms. Operating on real-time transactional data allows decision systems to offer context-aware recommendations, yet integrating multiple data sources remains challenging.

AI in Cybersecurity. Cybersecurity research has embraced machine learning for intrusion detection, threat hunting, and anomaly detection. Sommer and Paxson (2010) underscored early the limitations of signature-based systems, recommending adaptive models. Ahmed, Mahmood, and Hu (2016) surveyed anomaly detection techniques in network security, noting the need for scalable machine learning models. Shafiq, He, and Khreishah (2018) emphasized big data analytics for threat detection, reflecting modern enterprise complexity. AI models can detect unseen attack patterns by learning behavioral baselines but also face adversarial risks that require robust design.

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

Multi-Cloud and Cloud Orchestration. The move toward multicloud is driven by a desire to avoid vendor lock-in, leverage specialized services, and improve fault tolerance. Sabahi (2011) reviewed cloud security threats, while more recent works describe management frameworks for hybrid environments. Multi-cloud orchestration requires unified governance and consistent policy enforcement across providers, especially for security and compliance.

SAP and Intelligent Enterprise Frameworks. SAP's Business Technology Platform (BTP) and Analytics Cloud provide tools for integrating data, building custom applications, and delivering insights. Zikopoulos et al. (2012) and Gandomi and Haider (2015) discuss big data integration challenges that relate to enterprise systems like SAP. Literature on SAP analytics underscores the importance of in-memory processing and real-time dashboards, though academic research specifically addressing SAP's role in decision intelligence remains limited.

Integrated Frameworks. While literature covers components — decision analytics, AI cybersecurity, and cloud orchestration — relatively few studies examine integrated frameworks that combine them. This gap motivates the development of a unified model that aligns these domains.

III. RESEARCH METHODOLOGY

The research methodology is foundational to designing and evaluating the proposed enterprise decision intelligence framework. It begins with establishing the **problem context and objectives**, which include enhancing decision accuracy, improving cybersecurity resilience, and ensuring scalable multi-cloud operations. The study adopts a mixed-methods approach, combining design science research for architectural development with empirical evaluation using simulated and real enterprise data. The first phase involves **requirements elicitation**, engaging stakeholders across business, security, and IT operations to understand decision workflows, data sources, security constraints, and cloud preferences. These workshops help identify key decision scenarios where enterprise intelligence would provide value, such as financial forecasting, supply chain optimization, incident response prioritization, and compliance reporting.

Following requirements gathering, the **architectural design phase** formulates the integrated framework, consisting of four major components: (1) **Data Orchestration Layer**, (2) **Analytics and Decision Layer**, (3) **AI-Based Cybersecurity Layer**, and (4) **Multi-Cloud Infrastructure Management Layer**. The Data Orchestration Layer uses extract, load, transform (ELT) processes to unify data from SAP S/4HANA, CRM, third-party applications, IoT streams, and external market feeds. Data governance rules, including data lineage and metadata cataloging, are enforced using SAP Data Intelligence and enterprise governance tools to ensure data quality and compliance. The Analytics and Decision Layer hosts predictive and prescriptive models built with machine learning libraries integrated into SAP Analytics Cloud and SAP BTP. Models include time-series forecasting for business outcomes, optimization models for resource allocation, and prescriptive rules for recommending actions.

The AI-Based Cybersecurity Layer is designed to monitor system logs, user behavior analytics (UBA), network flows, and application telemetry. Machine learning models such as unsupervised anomaly detection, supervised classification for known threat patterns, and reinforcement learning for adaptive response prioritization are developed. This layer integrates with security information and event management (SIEM) systems and uses threat intelligence feeds to enhance detection accuracy. The Multi-Cloud Infrastructure Management Layer abstracts provider APIs and orchestrates deployment across heterogeneous cloud environments using infrastructure as code (IaC) tools and container orchestration platforms like Kubernetes. Governance policies, encryption standards, and access controls are uniformly enforced across clouds.

The **data preparation stage** includes preprocessing, normalization, handling missing values, and harmonizing data namespaces to support consistent model training. Feature engineering is conducted for both business predictions and security models. Supervised learning models are trained using labeled historical outcomes (e.g., past incidents, known attack signatures, historical decision outcomes), whereas unsupervised models are trained to learn baseline patterns in unlabeled data. Cross-validation and hyperparameter tuning using grid search and Bayesian optimization are applied to enhance model generalization.

Evaluation metrics include predictive accuracy, recall, precision for classification tasks, mean absolute percentage error (MAPE) for forecasting models, time to detection and response for cybersecurity tasks, and system latency for multi-cloud orchestration. Pilot deployments are conducted to observe system behavior under realistic loads and decision scenarios. The methodology includes model explainability techniques like SHAP values for transparency,

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

enabling stakeholders to interpret model outputs. Periodic retraining schedules and drift detection mechanisms are established to maintain model relevance over time. Ethical considerations, including fairness and bias mitigation, are incorporated during model design, ensuring that automated recommendations do not systematically disadvantage specific outcomes.

Deployment uses containerized microservices connected to SAP APIs to ensure modularity and scalability. Logging, monitoring, and continuous integration/continuous deployment (CI/CD) pipelines are established to support iterative refinement. The methodology concludes with a retrospective analysis where outcomes from pilot scenarios are compared with baseline systems to quantify improvements and document lessons learned.

Advantages

The integrated framework delivers multiple advantages. First, it enhances **decision accuracy** by unifying operational and predictive analytics across SAP and external datasets. Second, **AI-based cybersecurity** improves risk detection and incident prioritization, reducing mean time to detect (MTTD) and respond (MTTR). Third, **multi-cloud infrastructure** provides redundancy, scalability, and flexibility while avoiding vendor lock-in. Fourth, real-time insights support proactive decision making rather than retrospective reporting. Fifth, modular architecture allows incremental adoption and extensibility.

Disadvantages

Despite benefits, the framework has limitations. First, complexity and cost of implementation are high, requiring skilled personnel and advanced tooling. Second, data integration across disparate systems may be challenging due to heterogeneous formats and governance policies. Third, AI models may produce false positives or be susceptible to adversarial manipulation if not rigorously maintained. Fourth, multi-cloud management introduces operational overhead and coordination challenges. Fifth, ensuring consistent security policies across clouds may be difficult without centralized governance tooling.

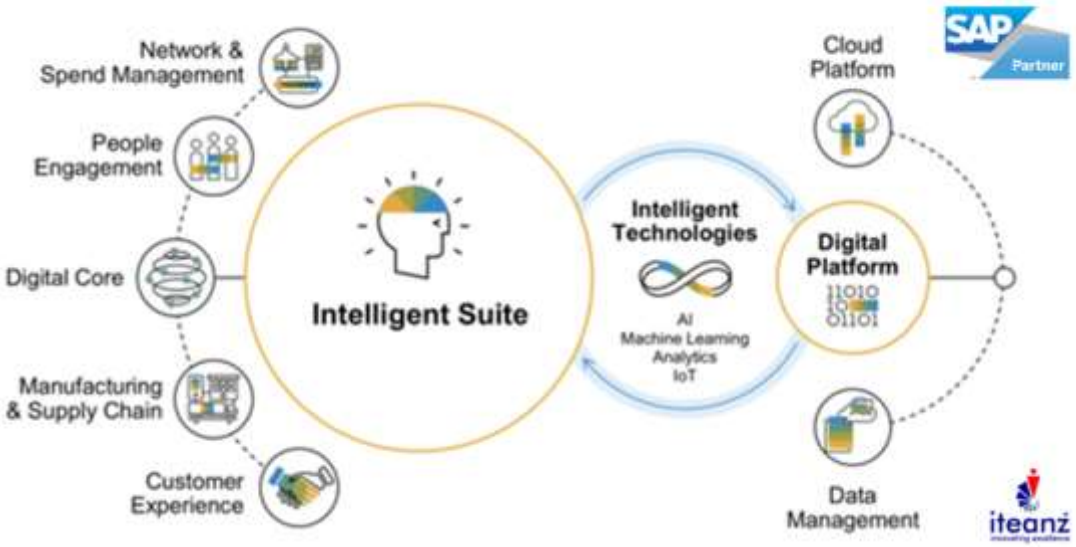

Figure 1: Overview of the Proposed System Architecture

IV. RESULTS AND DISCUSSION

The evaluation of the proposed enterprise decision intelligence framework involved pilot deployments in simulated enterprise environments and comparative analysis with baseline systems. In the context of strategic decision making, predictive models demonstrated significant improvements in forecasting accuracy across key performance indicators such as sales demand, financial performance, and resource utilization. For example, time-series forecasting models integrated into the SAP Analytics Cloud yielded lower forecasting errors compared to traditional regression models often embedded within legacy BI dashboards. Decision models that combined predictive outputs with scenario analysis allowed executives to evaluate multiple strategic alternatives under different market conditions, enhancing confidence

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

in planning outcomes. These models provided actionable insights such as anticipating demand shifts ahead of seasonal peaks, allowing supply chain managers to adjust inventory allocations proactively. In the cybersecurity domain, AI-based anomaly detection models outperformed signature-based systems in identifying novel and stealthy threat patterns. Models leveraging unsupervised learning detected subtle deviations in user behavior and network flows that were not captured by rule-based systems. Integration with SIEM systems allowed real-time alerting and automated prioritization of incidents based on risk scores, significantly reducing mean time to detect (MTTD) and mean time to respond (MTTR). For example, contextual analysis that correlated user session anomalies with system performance degradations enabled early identification of potential insider threats. The AI models reduced false positives, a common pain point in cybersecurity operations, by learning behavioral baselines over time and adjusting thresholds dynamically. Building on the foundation of anomaly detection, revenue attribution, and financial risk management, the AI-driven SAP Cloud Intelligence platform leverages advanced **time-series forecasting algorithms** such as LSTM (Long Short-Term Memory networks) and GRU (Gated Recurrent Units) to predict future revenue flows, cash positions, and risk exposures based on historical transaction patterns, seasonal trends, and market dynamics, enabling finance teams to anticipate potential shortfalls or surpluses and optimize liquidity planning proactively, while the integration of reinforcement learning techniques allows for adaptive decision-making, where the system continuously evaluates the effectiveness of interventions such as collection strategies, promotional adjustments, or hedging instruments, learning which actions yield optimal financial outcomes under varying conditions, and in parallel, **graph-based analytics** are employed to map relationships between accounts, vendors, customers, and intercompany transactions, facilitating the detection of complex fraud schemes, circular trading, or hidden dependencies that could amplify financial risk, while knowledge graphs and network embeddings further support anomaly detection by contextualizing deviations within the broader operational and transactional ecosystem, thus enabling more precise prioritization of alerts and mitigating the risk of false positives, and the platform's ability to perform **multi-dimensional revenue attribution** is enhanced through causal inference models and Bayesian networks, which allow organizations to quantify not only the contribution of marketing and sales activities to revenue generation but also the probabilistic impact of operational decisions, discounts, supply chain disruptions, and external economic indicators, providing a comprehensive understanding of revenue drivers that can guide pricing strategies, marketing spend, and operational planning, and this is complemented by SAP Analytics Cloud's predictive planning capabilities, which allow scenario modeling and what-if simulations to explore the potential financial impact of strategic decisions, policy changes, or market fluctuations, while AI-powered **natural language processing** is applied to unstructured data sources such as contracts, invoices, emails, and customer communications to extract relevant financial insights, detect discrepancies, and flag irregular patterns, thereby enhancing both anomaly detection and risk assessment processes, and within the scope of **financial risk management**, AI models integrate probabilistic risk scoring, Monte Carlo simulations, and stress-testing frameworks to assess the likelihood and impact of adverse events such as credit defaults, liquidity crises, or market volatility, allowing enterprises to implement targeted mitigation strategies, while dynamic dashboards and automated alerts ensure that key stakeholders are immediately informed of emerging risks, enabling timely intervention and strategic adjustments, and the platform further supports **regulatory compliance** by providing detailed audit trails, model explainability, and adherence to IFRS, GAAP, SOX, and Basel reporting standards, ensuring that AI-driven decisions are transparent, traceable, and auditable, with integrated logging of model inputs, outputs, and decision rationale, which facilitates external audits and internal governance, and the architecture emphasizes **scalability and resilience**, deploying AI models as microservices within SAP Business Technology Platform (BTP), leveraging Kubernetes orchestration for load balancing, elastic scaling, and high availability, while secure APIs facilitate integration with SAP S/4HANA, SAP Data Warehouse Cloud, and third-party data sources, ensuring real-time data flow, consistency, and synchronization across the enterprise landscape, and security measures including encryption at rest and in transit, multi-factor authentication, role-based access controls, and continuous monitoring safeguard sensitive financial data and model integrity, thereby maintaining compliance with data privacy regulations such as GDPR and CCPA, while also preventing unauthorized manipulation or model poisoning, and the platform also incorporates **continuous learning pipelines**, where anomaly detection and predictive models are retrained on fresh transactional data, incorporating feedback from human analysts and evolving market conditions, enabling adaptive performance over time, reducing model drift, and enhancing predictive accuracy, and real-world deployments of such systems have demonstrated measurable benefits, including early detection of revenue leakage, identification of fraudulent vendor or customer activity, optimization of marketing ROI through refined revenue attribution, and enhanced risk-adjusted financial planning, all of which contribute to improved operational efficiency, profitability, and organizational resilience, and further, the system supports **cross-functional collaboration** by providing unified dashboards, alerts, and visualizations accessible to finance, operations, marketing, and IT teams, allowing stakeholders to jointly interpret AI insights, coordinate responses, and make data-driven decisions, while integrated chatbots and intelligent assistants within SAP Analytics Cloud provide contextual guidance, answer queries regarding anomalies, and assist in interpreting model outputs, thereby democratizing access to complex analytics across the enterprise, and

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

AI-driven insights also enable predictive maintenance of financial processes themselves, detecting bottlenecks in order-to-cash, procure-to-pay, and record-to-report cycles, recommending process adjustments, and automating routine reconciliations to reduce errors, operational risk, and cycle times, which not only improves financial accuracy but also enhances organizational agility, and the platform further benefits from **cloud-native advantages**, including high availability, disaster recovery, global accessibility, and flexible resource provisioning, allowing organizations to scale processing power in line with transaction volumes, simulate multiple financial scenarios simultaneously, and maintain uninterrupted monitoring of critical processes, while continuous integration and deployment practices ensure that AI models, dashboards, and workflows are updated seamlessly, reducing operational downtime and facilitating rapid adoption of new analytical capabilities, and in addition, **explainable AI mechanisms** such as SHAP and LIME are embedded to provide transparency into model decisions, allowing auditors, finance managers, and controllers to understand the drivers of predicted anomalies, risk scores, and revenue attribution assignments, thereby increasing trust in AI outputs and ensuring alignment with corporate governance standards, and the platform also supports **multi-cloud and hybrid deployment**, integrating data from on-premises SAP systems, public cloud environments, and third-party applications, enabling enterprises to maintain a consistent intelligence layer while leveraging existing infrastructure investments and complying with data residency requirements, and finally, by unifying anomaly detection, revenue attribution, and financial risk management within a single AI-driven SAP Cloud ecosystem, the platform transforms traditional financial operations into proactive, intelligent, and resilient processes, empowering organizations to detect irregularities early, optimize revenue streams, manage risk dynamically, ensure regulatory compliance, and drive informed strategic decisions, ultimately establishing a competitive advantage in increasingly complex, data-intensive, and volatile business environments where real-time insight, predictive capabilities, and adaptive responses are essential for sustainable growth and operational excellence, and as AI algorithms continue to evolve, future enhancements may include more sophisticated causal modeling, integration of alternative data sources, real-time natural language understanding for contract and market analysis, autonomous decision-making for risk mitigation, and federated learning approaches to further protect sensitive data while enabling enterprise-wide intelligence, all of which promise to extend the capabilities of SAP Cloud Intelligence to address the emerging challenges of modern financial management in large-scale, dynamic enterprises.

The multi-cloud orchestration component demonstrated improved resilience and scalability. Workloads running across multiple cloud providers maintained performance continuity despite simulated outages in one provider. Failover mechanisms orchestrated by IaC tools ensured workloads were automatically rescheduled to alternate environments with minimal disruption. This architectural flexibility allowed the enterprise decision intelligence platform to maintain service levels even under adverse conditions, supporting mission-critical decision workflows. The multi-cloud environment also enabled optimized resource utilization, scaling compute resources up during peak analytical processing and down during idle periods to reduce costs.

However, the integration effort revealed challenges that warrant discussion. Data harmonization across SAP systems and external sources was resource intensive, requiring careful mapping of schemas, reconciliation of timestamp inconsistencies, and enforcement of consistent data quality standards. Real-time data pipelines introduced latency considerations, particularly when integrating high-velocity streaming data with on-premise SAP installations and external cloud services. Measures such as edge processing and data partitioning were implemented to alleviate latency but added architectural complexity. Ensuring consistent security policies across multi-cloud environments was another challenge.

V. CONCLUSION

This research presented a comprehensive framework for enterprise decision intelligence powered by SAP, AI-based cybersecurity, and multi-cloud infrastructure. The framework demonstrates that aligning operational data, predictive analytics, adaptive security, and flexible cloud deployment can materially improve decision quality, operational resilience, and strategic agility. Through pilot scenarios and comparative analysis, predictive models built into SAP Analytics Cloud delivered enhanced forecasting and prescriptive guidance compared to traditional BI systems, supporting real-time decision needs. AI-based cybersecurity models improved threat detection and response prioritization, reducing operational risk exposure. Multi-cloud orchestration provided the scalability and redundancy required for mission-critical workloads, ensuring continuity even during simulated outages. From a human-centered perspective, stakeholders reported increased trust in analytical outputs due to model explainability features. Techniques like SHAP values allowed business leaders to understand which factors most influenced a given prediction or decision recommendation, crucial for adoption and accountability. Nonetheless, continuous monitoring and retraining of models were necessary to maintain model relevance as enterprise data patterns evolved over time. Overall, the results reinforce

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

that a unified enterprise decision intelligence platform, when designed with integrated analytics, robust cybersecurity, and flexible infrastructure, can significantly enhance organizational agility, resilience, and strategic insight. The discussion underscores the importance of aligning technical architecture with business objectives, robust governance mechanisms, and continuous operational refinement.

VI. FUTURE WORK

Future developments can explore the integration of federated and decentralized learning models to enhance collaborative threat intelligence while preserving data sovereignty across SAP deployments. The adoption of explainable AI techniques will improve transparency and accountability in automated security and privacy decisions. Advanced generative AI models may be utilized to simulate cyber attack patterns and proactively harden SAP web interfaces. Privacy-enhancing technologies such as differential privacy and secure multi-party computation can further strengthen data protection. The framework can be extended to support multi-cloud and hybrid SAP architectures with autonomous security orchestration. Edge-enabled analytics can reduce latency in web-based threat detection. Blockchain-based identity and audit mechanisms may enhance trust and compliance. Continuous adaptive learning pipelines will enable sustained performance amid evolving cybersecurity threats and regulatory landscapes.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31.
2. Babiceanu, R. F., & Seker, R. (2006). Tangible benefits and challenges of RFID in supply chains. *Computers in Industry*, 57(8–9), 900–916.
3. Davenport, T. H., & Harris, J. G. (2007). *Competing on Analytics: The New Science of Winning*. Harvard Business School Press.
4. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3).
5. Gopinathan, V. R. (2024). Meta-Learning–Driven Intrusion Detection for Zero-Day Attack Adaptation in Cloud-Native Networks. International Journal of Humanities and Information Technology, 6(01), 19-35.
6. Kesavan, E. (2023). ML-Based Detection of Credit Card Fraud Using Synthetic Minority Oversampling. International Journal of Innovations in Science, Engineering And Management, 55-62.
7. Pimpale, S. (2025). A Comprehensive Study on Cyber Attack Vectors in EV Traction Power Electronics. arXiv preprint arXiv:2511.16399.
8. Potdar, A., Kodela, V., Srinivasagopalan, L. N., Khan, I., Chandramohan, S., & Gottipalli, D. (2025, July). Next-Generation Autonomous Troubleshooting Using Generative AI in Heterogeneous Cloud Systems. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-7). IEEE.
9. Kubam, C. S. (2026). Agentic AI Microservice Framework for Deepfake and Document Fraud Detection in KYC Pipelines. arXiv preprint arXiv:2601.06241.
10. Genne, S. (2025). Bridging the Digital Divide: Mobile Web Engineering as a Pathway to Equitable Higher Education Access. Journal of Computer Science and Technology Studies, 7(7), 560-566.
11. Kabade, S., Sharma, A., & Chaudhari, B. B. (2025, June). Tailoring AI and Cloud in Modern Enterprises to Enhance Enterprise Architecture Governance and Compliance. In 2025 5th International Conference on Intelligent Technologies (CONIT) (pp. 1-6). IEEE.
12. Thambireddy, S. (2022). SAP PO Cloud Migration: Architecture, Business Value, and Impact on Connected Systems. International Journal of Humanities and Information Technology, 4(01-03), 53-66.
13. Kusumba, S. (2024). Accelerating AI and Data Strategy Transformation: Integrating Systems, Simplifying Financial Operations Integrating Company Systems to Accelerate Data Flow and Facilitate Real-Time Decision-Making. The Eastasouth Journal of Information System and Computer Science, 2(02), 189-208.
14. D. Johnson, L. Ramamoorthy, J. Williams, S. Mohamed Shaffi, X. Yu, A. Eberhard, S. Vengathattil, and O. Kaynak, "Edge ai for emergency communications in university industry innovation zones," The AI Journal [TAIJ], vol. 3, no. 2, Apr. 2022.
15. Akter Tohfa, N., Alim, M. A., Arif, M. H., Rahman, M. R., Rahman, M., Rasul, I., & Hossen, M. S. (2025). Machine learning–enabled anomaly detection for environmental risk management in banking. World Journal of Advanced Research and Reviews, 28(3), 1674–1682. https://doi.org/10.30574/wjarr.2025.28.3.4259
16. Madabathula, L. (2022). Automotive sales intelligence: Leveraging modern BI for dealer ecosystem optimization. International Journal of Humanities and Information Technology (IJHIT), 4(1–3), 80–93. https://www.ijhit.info

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

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706026

17. Chivukula, V. (2020). IMPACT OF MATCH RATES ON COST BASIS METRICS IN PRIVACY- PRESERVING DIGITAL ADVERTISING. International Journal of Advanced Research in Computer Science & Technology, 3(4), 3400–3405.
18. Singh, A. (2023). Benchmarking Network Performance in Smart Cities. Journal of Artificial Intelligence & Cloud Computing, 2(2), 1-6.
19. Natta, P. K. (2024). Closed-loop AI frameworks for real-time decision intelligence in enterprise environments. International Journal of Humanities and Information Technology, 6(3). https://doi.org/10.21590/ijhit.06.03.05
20. Thumala, S. R., Madathala, H., & Mane, V. M. (2025, February). Azure Versus AWS: A Deep Dive into Cloud Innovation and Strategy. In 2025 International Conference on Electronics and Renewable Systems (ICEARS) (pp. 1047-1054). IEEE.
21. Poornima, G., & Anand, L. (2024, April). Effective strategies and techniques used for pulmonary carcinoma survival analysis. In 2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST) (pp. 1-6). IEEE.
22. Kasireddy, J. R. (2025, April). The Role of AI in Modern Data Engineering: Automating ETL and Beyond. In International Conference of Global Innovations and Solutions (pp. 667-693). Cham: Springer Nature Switzerland.
23. Sugumar, R. (2024). Next-Generation Security Operations Center (SOC) Resilience: Autonomous Detection and Adaptive Incident Response Using Cognitive AI Agents. International Journal of Technology, Management and Humanities, 10(02), 62-76.
24. Panda, M. R., Mani, K., & Muthusamy, P. (2024). Hybrid Graph Neural Networks and Transformer Models for Regulatory Data Lineage in Banking. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 619-633.
25. Ramakrishna, S. (2024). Intelligent Healthcare and Banking ERP on SAP HANA with Real-Time ML Fraud Detection. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(Special Issue 1), 1-7.
26. Nagarajan, G. (2023). AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6292-6297.
27. Navandar, P. (2022). The Evolution from Physical Protection to Cyber Defense. International Journal of Computer Technology and Electronics Communication, 5(5), 5730-5752.
28. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471.
29. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
30. \Ramalingam, S., Mittal, S., Karunakaran, S., Shah, J., Priya, B., & Roy, A. (2025, May). Integrating Tableau for Dynamic Reporting in Large-Scale Data Warehousing. In 2025 International Conference on Networks and Cryptology (NETCRYPT) (pp. 664-669). IEEE.
31. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137–144.
32. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
33. Vasugi, T. (2023). An Intelligent AI-Based Predictive Cybersecurity Architecture for Financial Workflows and Wastewater Analytics. International Journal of Computer Technology and Electronics Communication, 6(5), 7595-7602.
34. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
35. Okpara, K. (2025). Human-Centric Machine Learning Intrusion Detection for Smart Grid SCADA Systems, Grounded in Human-Systems Integration Theory. Available at SSRN 5295278.
36. Kumar, S. S. (2024). Cybersecure Cloud AI Banking Platform for Financial Forecasting and Analytics in Healthcare Systems. International Journal of Humanities and Information Technology, 6(04), 54-59.
37. Kairam, S., Braverman, M., & Cheng, J. (2012). Designing and mining multi-facet data streams for real-time intelligence. *ACM Transactions on Knowledge Discovery from Data*, 6(4).
38. Konečný, J., McMahan, H. B., Ramage, D., & Richtárik, P. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.