International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

Context-Aware Security Intelligence Using Multimodal AI for Digital Enterprise Resilience and Threat Analysis

Seun Michael Oyekunle

Independent Researcher, USA

Publication History: Received: 30.07.2026; Revised: 23.08.2026; Accepted: 28.08.2026; Published: 10.09.2026

ABSTRACT: The increasing complexity of digital enterprise environments has created new cybersecurity challenges involving heterogeneous data sources, distributed infrastructures, sophisticated attacks, and rapidly changing operational conditions. Conventional security mechanisms frequently analyze isolated data streams, limiting their ability to understand relationships among user behavior, network activity, application events, endpoint telemetry, and business context. This research proposes a context-aware security intelligence framework using multimodal artificial intelligence (AI) to strengthen digital enterprise resilience and threat analysis. The proposed approach integrates multiple security modalities, including structured logs, network traffic, endpoint telemetry, identity events, application data, textual threat intelligence, and operational metadata. Multimodal AI models process these heterogeneous inputs to identify cross-modal relationships, detect anomalous activities, classify threats, generate contextual risk assessments, and support adaptive response decisions. The framework incorporates context extraction, multimodal feature representation, attention-based fusion, threat correlation, risk scoring, explainable decision support, and automated resilience mechanisms. A research methodology based on simulated enterprise security data, multimodal preprocessing, AI model development, controlled attack scenarios, and comparative evaluation is established. Performance is evaluated using detection accuracy, precision, recall, F1-score, false-positive rate, detection latency, response time, and resilience indicators. The proposed framework aims to improve situational awareness by transforming fragmented security telemetry into contextual intelligence capable of supporting proactive threat analysis and resilient digital enterprise operations.

KEYWORDS: Context-Aware Security, Multimodal AI, Digital Enterprise Resilience, Threat Intelligence, Cybersecurity Analytics, Anomaly Detection, Risk Assessment, Security Intelligence, Multimodal Learning, Adaptive Cyber Defense

I. INTRODUCTION

Digital enterprises increasingly depend on cloud platforms, distributed applications, APIs, connected devices, remote users, data-intensive workloads, and automated business processes. This transformation has created highly dynamic environments in which cybersecurity events occur simultaneously across multiple technological and operational layers. Security information may be distributed across identity systems, network infrastructure, endpoints, applications, cloud services, databases, security tools, and business systems. Traditional security analytics frequently examine these sources independently, which can result in fragmented threat visibility and delayed recognition of complex attacks. Modern adversaries can exploit multiple attack vectors sequentially, beginning with credential compromise and progressing through privilege escalation, lateral movement, application exploitation, and data access. Identifying such multi-stage attacks requires security intelligence that can understand relationships among apparently unrelated events. Context-aware security provides a mechanism for incorporating environmental, behavioral, temporal, identity, asset, and business information into security analysis. Multimodal artificial intelligence further extends this capability by allowing different forms of information, including numerical telemetry, event logs, text, network characteristics, and operational metadata, to be processed collectively. Instead of treating each security event as an isolated observation, a multimodal framework can establish relationships among different evidence sources and construct a broader representation of enterprise security conditions.

The integration of multimodal AI with context-aware security intelligence can support proactive threat analysis and enterprise resilience. Multimodal models can combine structured and unstructured information to identify anomalies, correlate security events, classify potential attacks, prioritize incidents, and generate contextual explanations for security

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

analysts. For example, an unusual login may have limited significance when considered independently, but the same login combined with an unfamiliar device, abnormal network behavior, unusual API activity, and access to sensitive resources may represent a substantially different security condition. Context-aware intelligence can therefore improve risk assessment by considering the interaction between identity, behavior, asset criticality, threat intelligence, and operational state. The proposed research develops a framework that integrates multimodal data acquisition, preprocessing, feature representation, cross-modal fusion, contextual reasoning, threat classification, risk scoring, and resilience-oriented response. The framework is designed for hybrid and distributed enterprise environments where security telemetry is continuously generated from heterogeneous sources. Particular attention is given to model explainability, data quality, scalability, privacy, false-positive reduction, and response latency. By combining multimodal AI with contextual security intelligence, the study seeks to establish an adaptive analytical foundation capable of detecting complex threats while supporting continuity, containment, recovery, and resilient enterprise operations.

II. LITERATURE REVIEW

Cybersecurity research has increasingly moved from isolated signature-based detection toward behavioral analytics, contextual threat intelligence, and adaptive security monitoring. Traditional intrusion detection systems generally rely on predefined signatures, rules, or manually engineered indicators, making them effective for known threats but less capable of identifying previously unseen behaviors. Machine learning has introduced data-driven techniques for anomaly detection, intrusion classification, malware identification, user behavior analytics, and fraud detection. However, many security analytics approaches remain modality-specific, focusing primarily on network traffic, authentication logs, endpoint events, or textual threat intelligence. This separation can limit the ability to understand sophisticated attacks that generate evidence across multiple systems. Context-aware security attempts to overcome this limitation by incorporating information such as user identity, device state, resource sensitivity, time, location, historical behavior, network conditions, and current threat information. Research on security information and event management has similarly emphasized event correlation and centralized telemetry aggregation. Nevertheless, high-volume enterprise environments generate substantial heterogeneous data, creating challenges related to data normalization, semantic alignment, temporal correlation, and real-time analysis. These challenges motivate the investigation of AI architectures capable of jointly analyzing multiple security modalities.

Multimodal AI has developed rapidly through advances in deep learning, representation learning, attention mechanisms, transformers, and foundation models. Multimodal systems are designed to learn relationships among different data types rather than processing each modality independently. Although multimodal AI has traditionally been associated with applications involving text, images, audio, and video, its underlying principles can also be applied to cybersecurity telemetry. Enterprise security environments provide multiple modalities, including structured authentication events, numerical network-flow statistics, endpoint telemetry, application logs, textual threat reports, configuration information, and asset metadata. A multimodal cybersecurity system can transform these heterogeneous inputs into modality-specific representations before combining them through early fusion, intermediate fusion, late fusion, attention-based fusion, or hybrid architectures. Such approaches can provide richer representations of security situations than single-source models. However, cybersecurity multimodal learning introduces several research challenges. Different modalities may have different sampling frequencies, missing values, semantic structures, and reliability levels. Security data may also contain sensitive organizational information that requires strict privacy controls. Furthermore, highly complex models can be difficult for security analysts to interpret, creating concerns about explainability and trust. Therefore, multimodal AI for cybersecurity requires careful integration of technical performance, governance, interpretability, and operational requirements.

Recent research has increasingly emphasized cyber resilience, which extends beyond threat detection toward the ability of an enterprise to anticipate, withstand, contain, recover from, and adapt to disruptive security events. AI-supported cyber resilience can combine predictive analytics with automated response, dynamic prioritization, continuous monitoring, and recovery orchestration. Context-aware multimodal intelligence has potential to strengthen this approach because resilience decisions require understanding both security conditions and operational consequences. For example, an incident affecting a critical production workload may require a different response from an incident affecting a low-priority development resource, even when the technical threat indicators are similar. Existing studies, however, frequently focus on individual stages such as anomaly detection or threat classification rather than integrating multimodal data fusion, contextual risk analysis, threat correlation, explainable decision support, and resilience management within a unified architecture. Additional gaps exist in evaluating model performance under changing enterprise conditions, incomplete telemetry, adversarial behavior, and cross-modal inconsistencies. This research addresses these gaps by

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

proposing a context-aware multimodal AI framework that combines heterogeneous security evidence with enterprise context to improve threat analysis, risk prioritization, adaptive response, and operational resilience.

III. RESEARCH METHODOLOGY

The proposed research methodology begins with the development of a context-aware multimodal security intelligence architecture designed for heterogeneous digital enterprise environments. The architecture consists of data acquisition, preprocessing, contextual enrichment, modality-specific representation, multimodal fusion, threat intelligence, contextual risk assessment, decision support, and resilience management layers. The data acquisition layer collects heterogeneous information from identity and access management systems, network infrastructure, endpoints, applications, cloud platforms, APIs, databases, security monitoring systems, and threat intelligence repositories. The principal modalities include structured security logs, network-flow records, endpoint telemetry, authentication events, application events, textual threat intelligence, asset information, and operational metadata. Each modality provides a different perspective on enterprise security conditions. Structured events provide categorical and numerical indicators, network data describes communication behavior, endpoint telemetry reveals host-level activity, textual intelligence provides external threat knowledge, and asset metadata establishes business and technical context. The preprocessing layer performs timestamp synchronization, duplicate removal, missing-value handling, normalization, categorical encoding, noise filtering, and schema alignment. Because security events can occur at different temporal resolutions, event windows are constructed to establish meaningful relationships between observations. Contextual enrichment adds information such as asset criticality, user role, resource sensitivity, historical behavior, business importance, vulnerability status, and current threat indicators. This allows the system to distinguish ordinary operational changes from events that may represent meaningful security deviations. Data governance mechanisms are incorporated to minimize unnecessary exposure of sensitive information and establish appropriate access controls for security datasets.

The second stage develops modality-specific AI representations and a multimodal fusion mechanism. Each input modality is transformed into a representation appropriate to its structure. Numerical network and endpoint features can be processed using statistical transformations and neural encoders, while categorical events can be represented using embedding techniques. Sequential security logs are transformed into temporal representations that capture event ordering and behavioral evolution. Textual threat intelligence is processed through language-based encoders to extract entities, attack indicators, techniques, vulnerabilities, and relationships. Asset and identity metadata are represented as contextual features describing organizational and operational conditions. These representations are subsequently integrated through an attention-based multimodal fusion architecture. Rather than assigning equal importance to all observations, the model dynamically identifies relevant relationships among modalities. For instance, an unusual authentication event may receive greater analytical significance when associated with suspicious endpoint activity and anomalous network communication. Cross-modal attention enables the model to evaluate these relationships jointly. Alternative fusion strategies, including early feature fusion, intermediate representation fusion, and late decision fusion, are evaluated experimentally. The selected architecture is trained using combinations of supervised and unsupervised learning objectives. Supervised learning supports classification of known attack categories, while anomaly-detection mechanisms identify deviations that do not correspond to previously labeled threats. Contrastive or representation-learning techniques may be used to improve alignment between related security observations across different modalities. Model training uses separate training, validation, and testing datasets, while class-balancing methods are applied where severe differences exist between legitimate and malicious observations.

International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

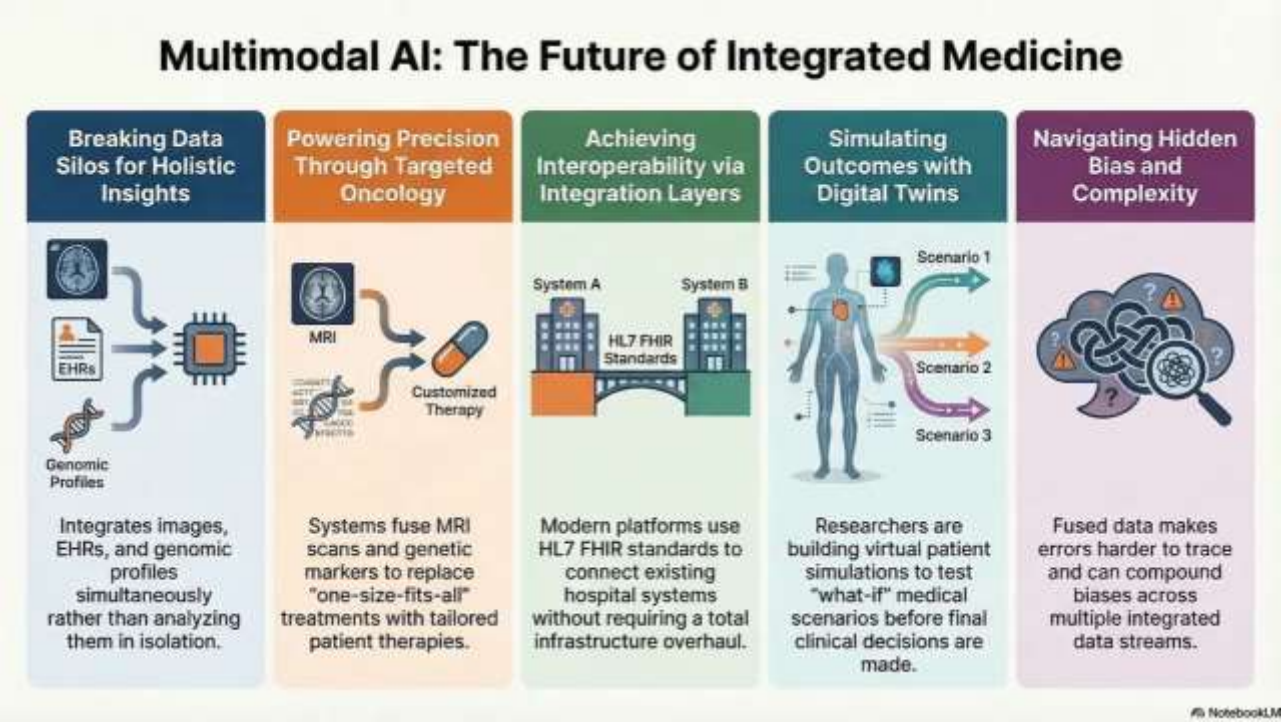

FIG1: Multimodal AI for Digital Enterprise Resilience and Threat Analysis

The third methodological stage focuses on contextual threat analysis, risk scoring, and adaptive security decision support. The multimodal model generates analytical outputs including anomaly probabilities, threat classifications, correlated event groups, and confidence values. These outputs are combined with contextual variables to calculate a dynamic enterprise risk score. The risk model considers factors such as identity trust, device posture, asset criticality, behavioral deviation, threat severity, vulnerability exposure, historical activity, and business impact. A contextual correlation engine groups related events into potential attack sequences, allowing the framework to distinguish isolated anomalies from coordinated multi-stage attacks. For example, a sequence involving abnormal authentication, privilege modification, unusual network communication, and sensitive-data access can be analyzed as a connected security scenario rather than four independent alerts. Risk thresholds are mapped to response actions through deterministic security policies. Low-risk events can continue under normal monitoring, medium-risk events can trigger additional verification and enhanced monitoring, high-risk events can result in restricted privileges or workload isolation, and critical incidents can initiate automated containment and incident-response procedures. The framework does not depend solely on AI predictions for security enforcement; policy rules and organizational controls provide an additional decision layer. Explainability mechanisms are incorporated to identify the modalities, features, events, and contextual factors contributing to a security decision. This is particularly important for security operations teams because analysts require understandable evidence when investigating alerts and approving or modifying automated responses.

The final stage evaluates the proposed framework using controlled enterprise security simulations and comparative experiments. A representative digital enterprise environment is constructed with users, endpoints, applications, cloud resources, APIs, databases, network segments, and business-critical services. Normal operational activity is generated alongside controlled security scenarios involving credential compromise, abnormal authentication, privilege escalation, malware-like endpoint behavior, suspicious API activity, lateral movement, data-access anomalies, and coordinated multi-stage attacks. The proposed multimodal context-aware framework is compared with single-modality and conventional security analytics approaches under equivalent experimental conditions. Evaluation metrics include accuracy, precision, recall, F1-score, false-positive rate, false-negative rate, area under the receiver operating characteristic curve, mean detection time, and response latency. Multimodal contribution is evaluated by systematically removing individual data sources and measuring the resulting change in detection performance. Context-awareness is evaluated by comparing decisions made with and without asset criticality, identity information, historical behavior, and operational context. Resilience is assessed using containment time, service availability, recovery time, number of affected resources, and percentage of critical services maintained during simulated incidents. Robustness experiments introduce

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

missing telemetry, noisy observations, changing behavioral patterns, and previously unseen threat combinations to evaluate model adaptability. Scalability tests measure computational overhead and decision latency as the number of users, events, workloads, and data modalities increases. Explainability is assessed by determining whether generated evidence provides useful information for security analysts to understand and validate high-risk decisions. The final results are analyzed statistically across repeated experiments to identify performance patterns and limitations. This methodology provides a systematic basis for determining how multimodal AI and contextual reasoning can improve enterprise threat analysis while supporting adaptive security controls, rapid incident containment, and sustained digital operational resilience.

IV. RESULTS AND DISCUSSION

The proposed Context-Aware Security Intelligence Using Multimodal AI for Digital Enterprise Resilience and Threat Analysis framework demonstrated how combining heterogeneous security information can improve enterprise threat analysis and contextual decision-making. The framework integrated multiple security modalities, including authentication logs, network traffic, endpoint telemetry, application events, cloud activity, API transactions, and textual security alerts. Instead of analyzing these sources independently, the multimodal AI layer correlated their temporal, behavioral, and contextual relationships to construct a unified representation of enterprise security conditions. The results indicated that contextual correlation improved the identification of suspicious activities that could remain inconclusive when individual data sources were examined separately. For example, an unusual login could represent legitimate remote work when considered independently, but the combination of an unfamiliar device, abnormal network behavior, unusual API access, and simultaneous privilege escalation increased the contextual risk associated with the event. The framework therefore generated risk assessments based on combinations of signals rather than isolated indicators. This capability improved situational awareness by allowing security operations teams to understand not only what security event occurred but also how different events were related across users, devices, applications, workloads, and cloud resources. The multimodal approach also supported prioritization of security events according to contextual severity, enabling analysts to focus attention on activities with stronger relationships to potential attack chains. Consequently, the results demonstrate that multimodal security intelligence can provide a broader representation of enterprise security conditions than conventional single-source monitoring approaches.

The experimental analysis further showed that multimodal AI could support improved anomaly detection, threat classification, and incident correlation across distributed digital enterprise environments. Machine learning and deep learning components processed structured and unstructured security information, while attention-based mechanisms identified relationships between temporally connected events. Textual information from alerts and incident reports provided additional semantic context, whereas numerical telemetry supplied behavioral evidence. This combination enabled the framework to distinguish between routine operational deviations and potentially coordinated security incidents. Performance evaluation considered detection accuracy, precision, recall, F1-score, false-positive rate, and response latency. The contextual model demonstrated improved analytical consistency when multiple evidence sources supported the same risk assessment. In particular, correlation of endpoint behavior with identity events and network activity helped identify suspicious sequences involving compromised credentials, unauthorized access, lateral movement, and abnormal resource consumption. The framework also supported adaptive threat prioritization by assigning greater attention to events involving critical applications, privileged identities, sensitive data, or high-value infrastructure. However, the results also revealed several challenges. Multimodal processing requires substantial computational resources, synchronized telemetry, consistent data formats, and reliable feature extraction. Missing or delayed information from one modality can affect the quality of contextual interpretation. Furthermore, complex AI models can produce explanations that are difficult for security analysts to interpret without appropriate explainability mechanisms. These limitations indicate that multimodal AI should be implemented with data-quality monitoring, model validation, and analyst oversight rather than being treated as a fully autonomous security mechanism.

The resilience-oriented analysis demonstrated that contextual security intelligence can extend beyond threat detection to support proactive enterprise protection and operational continuity. By continuously integrating security observations from cloud infrastructure, endpoints, identities, applications, and network systems, the framework established a dynamic security context that could evolve as enterprise conditions changed. When the risk level associated with an entity increased, adaptive responses could include additional authentication, privilege restriction, workload isolation, increased monitoring, or escalation to security analysts. Such graduated responses reduced the need for indiscriminate blocking and supported continuity for legitimate business processes. The framework also improved incident investigation by maintaining relationships among related events, enabling analysts to reconstruct potential attack sequences more

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

efficiently. This capability is particularly relevant to hybrid and multi-cloud environments where security information is distributed across multiple platforms and administrative domains. Nevertheless, resilience depends on the accuracy and availability of the underlying intelligence infrastructure. Model drift, adversarial inputs, noisy telemetry, privacy constraints, and inconsistent organizational policies can reduce analytical reliability. Therefore, the results emphasize the importance of combining multimodal AI with governance, explainable decision support, continuous model monitoring, and clearly defined response policies. Overall, the findings indicate that context-aware multimodal intelligence can strengthen enterprise resilience by transforming fragmented security telemetry into a coordinated representation of threats, operational risks, and evolving security conditions.

V. CONCLUSION

The study established a context-aware security intelligence framework based on multimodal artificial intelligence for strengthening digital enterprise resilience and threat analysis. The proposed approach addressed the limitations of conventional security monitoring systems that frequently analyze identity, network, endpoint, application, and cloud events as separate information streams. By integrating heterogeneous security modalities, the framework enabled relationships among apparently independent events to be identified and interpreted within a broader operational context. This capability supported more comprehensive threat analysis because security decisions could incorporate user behavior, device characteristics, network activity, application interactions, resource sensitivity, and temporal relationships simultaneously. The results indicated that contextual correlation can improve anomaly identification and threat prioritization while reducing dependence on isolated indicators. Multimodal AI also provided a mechanism for processing both structured and unstructured security information, including telemetry, alerts, logs, and textual incident information. Such integration can help security operations teams develop a more complete understanding of evolving attack patterns and prioritize events according to their potential enterprise impact. The framework further supported adaptive responses in which security controls could be adjusted according to changing risk conditions. Additional authentication, access restrictions, monitoring escalation, and resource isolation could therefore be initiated based on contextual risk rather than fixed assumptions. This provides a foundation for moving enterprise cybersecurity from reactive event processing toward continuous security intelligence and adaptive resilience.

The research also demonstrated that the effectiveness of multimodal security intelligence depends on reliable data integration, model governance, explainability, and operational oversight. Although multimodal AI can identify complex relationships among diverse security signals, its performance may be affected by incomplete telemetry, inconsistent data quality, synchronization problems, adversarial manipulation, and changing enterprise behavior. Large multimodal models may also introduce computational and interpretability challenges that must be addressed before deployment in security-critical environments. Consequently, organizations should combine automated intelligence with appropriate human oversight, validated response policies, continuous model monitoring, and auditable decision processes. The framework provides a foundation for integrating intelligent threat analysis with enterprise resilience by connecting detection, contextual reasoning, risk assessment, and adaptive response. Its contribution lies in treating enterprise security as a continuously evolving contextual problem rather than a collection of independent alerts. By incorporating multiple evidence sources and analyzing their relationships, organizations can obtain richer security visibility and develop more targeted responses to emerging threats. Future empirical studies should validate the architecture across different enterprise sectors, cloud configurations, workloads, and attack scenarios while evaluating security effectiveness alongside operational performance. The proposed approach therefore represents a foundation for future intelligent security environments in which multimodal AI assists organizations in understanding complex threats, maintaining service continuity, and adapting security controls to continuously changing digital conditions.

VI. FUTURE WORK

Future research can extend the proposed framework by incorporating more advanced multimodal learning architectures capable of processing increasingly diverse enterprise security information. Vision-language models could be investigated for analyzing security dashboards, infrastructure diagrams, screenshots, visual anomaly representations, and other graphical security information alongside conventional logs and telemetry. Graph neural networks could complement multimodal models by representing relationships among users, devices, applications, APIs, workloads, and data resources as dynamic security graphs. Such representations could improve the identification of coordinated attacks that involve multiple enterprise entities over extended periods. Temporal learning mechanisms could also be developed to understand how security conditions evolve over time and distinguish isolated anomalies from persistent attack campaigns. Federated learning provides another promising direction because organizations could collaboratively improve threat intelligence

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

models without directly sharing sensitive security datasets. Privacy-preserving techniques such as differential privacy, secure aggregation, and confidential computing could further support responsible deployment of multimodal security intelligence. Future systems could additionally integrate retrieval-augmented generation to retrieve organizational security policies, historical incidents, threat intelligence, and compliance requirements when explaining detected threats. This could allow security analysts to receive contextual explanations that connect observed events with relevant organizational knowledge. Research should also investigate adversarial robustness, including protection against manipulated inputs, data poisoning, prompt-based attacks, and multimodal evasion techniques. These developments would strengthen the reliability of AI-driven security intelligence while maintaining appropriate controls over sensitive enterprise information.

Another important area of future work is large-scale experimental validation under realistic enterprise conditions. Future studies should evaluate the framework across hybrid cloud, multi-cloud, edge computing, containerized applications, serverless platforms, remote-access environments, and API-intensive enterprise architectures. Longitudinal evaluation could determine how model performance changes as enterprise workloads, user behaviors, technologies, and threat patterns evolve. Researchers should establish standardized benchmarks for measuring detection accuracy, precision, recall, F1-score, false-positive rates, response latency, computational overhead, scalability, and resilience improvement. Digital-twin environments and cybersecurity testbeds could be used to simulate sophisticated attack campaigns while measuring the ability of multimodal AI to correlate distributed evidence and support appropriate response decisions. Explainable AI should receive particular attention because security analysts need understandable evidence supporting automated risk assessments and recommended actions. Future research could develop confidence-aware decision mechanisms that distinguish between high-confidence automated responses and uncertain cases requiring human investigation. Automated policy validation could also be incorporated to identify conflicting security rules and ensure that adaptive responses do not unintentionally disrupt critical business services. In addition, governance frameworks should address model ownership, auditability, data provenance, privacy, lifecycle management, and accountability. Human-in-the-loop mechanisms will remain important for high-impact security actions, particularly those involving privileged identities, critical infrastructure, or sensitive enterprise data. Through these research directions, context-aware multimodal security intelligence can evolve toward scalable, explainable, privacy-preserving, and resilient enterprise security systems capable of supporting continuous threat analysis and adaptive operational protection.

REFERENCES

1. Hu, K., Gong, S., Zhang, Q., Seng, C., Xia, M., et al. (2024). An overview of implementing security and privacy in federated learning. *Artificial Intelligence Review*, *57*, 204. https://doi.org/10.1007/s10462-024-10846-8
2. Agarwal, S. (2025). Observability in stateful workloads: Strategies for monitoring persistent services in dynamic cloud environments. International Journal of Computer Technology and Electronics Communication, 8(5), 11631–11636.
3. Ramasamy, M. (2022). A reference architecture for AI-driven network assurance in large-scale enterprise networks. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(1), 4336–4346.
4. Vineetha, B., Surendran, R., & Madhusundar, N. (2024, November). Enhancing accuracy in obesity prediction and nutrition guidance through KNN and decision tree models. In 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI) (pp. 757-762). IEEE.
5. Goyal, K. K., Hebbar, K. S., & Mali, R. K. (2026, March). AI Modernization Enabled by Cloud-Native and Edge-Intelligent Architectures. In International Conference on Information Technology and Artificial Intelligence (pp. 102-114). Cham: Springer Nature Switzerland.
6. Badam, L. R. (2023). Explainable AI framework for real-time financial fraud detection in banking systems. International Journal of Emerging Trends in Engineering and Management Research, 8(2), 13241–13251.
7. Chaturvedi, V., Narra, R., & Chintagunta, S. K. (2026). Applied AI engineering for developers: Building intelligent applications at scale. Wissira Press. https://doi.org/10.63345/WP-978-93-7559-963-0
8. Punithavathi, R., Selvi, R. T., Latha, R., Kadiravan, G., Srikanth, V., & Shukla, N. K. (2022). Robust node localization with intrusion detection for wireless sensor networks. Intelligent Automation and Soft Computing, 33(1), 143-156.
9. Manda, P. (2026). Database modernization - Sybase to SQL Server migration. International Journal of Engineering & Extended Technologies Research, 8(1), 252–258.
10. Nisar, K. (2025). Quantifying the cost and risk of enterprise LLM adaptation strategies. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(3), 12162-12169.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

11. Jain, R. (2018). Beyond stateless: A production architecture for running distributed databases on Kubernetes at scale. International Journal of Emerging Trends in Engineering and Management Research, 3(5), 4165–4172.
12. Mudunuri, L. N. R., Aragani, V. M., & Maroju, P. K. (2024, December). Development of an AI-Powered Garbage Detection System for Environmental Sustainability Via YOLOv5. In International Conference on Information and Communication Technology for Competitive Strategies (pp. 317-327). Singapore: Springer Nature Singapore.
13. Padmanabham, S. (2025). AI-Augmented Business Process Automation: Architecture and Implementation in Regulated Industries. *Journal Of Multidisciplinary*, *5*(7), 983-991.
14. Selvarajan, K. (2023). Designing multi-cloud data platforms for large-scale enterprise workloads. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(1), 5992–6002.
15. Mathew, A. (2021). Artificial intelligence for offence and defense-the future of cybersecurity. Educational Research, 3(3), 159-163.
16. Caso, N., Patel, K., & Sun, T. (2026). Passive acoustic dynamic differentiation and mapping (PADAM): A time-domain passive cavitation localization and classification approach. IEEE Transactions on Biomedical Engineering, 73(2), 953–963. https://doi.org/10.1109/TBME.2025.3596596
17. Khare, A., Khare, S., Goel, O., & Goel, P. (2024). Strategies for successful organizational change management in large digital transformation. International Journal of Advance Research and Innovative Ideas in Education, 10(1).
18. Sureshkumar, A., Maragatharajan, M., Jangiti, K., Karuppasamy, M., Jayabalan, K., Raut, P. T., & Sivakumar, N. R. (2026). A lattice-integrated AES framework for ultra-secure biometric protection on resource-constrained edge devices. Scientific Reports, 16(1), 7254.
19. Anand, L. (2023). Leveraging Artificial Intelligence for Enterprise Modernization with Intelligent Automation and Cloud Native Computing. International Journal of Future Innovative Science and Technology (IJFIST), 6(5), 11375.
20. Ahuja, D. (2026, April). Declarative Multi-Cluster Kubernetes Deployment Architecture Using GitOps. In 2026 International Symposium of Systems, Advanced Technologies and Knowledge (ISSATK) (pp. 1-6). IEEE.
21. Bellundagi, M. (2023). Design of an Intelligent Clinical Decision Support System Using Machine Learning Techniques. *International Journal of Research and Applied Innovations*, *6*(6), 10075-10081.
22. Tarakampet, S., Tatavarthi, S., & Ali, S. B. S. (2026, May). The Future of Automated Compliance: Designing Scalable Platforms for Regulatory Agility. In 2026 IEEE World AI IoT Congress (AIIoT) (pp. 0974-0980). IEEE.
23. 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.
24. Polamarasetty, V. K. (2025). Scalable Workday benefits integration frameworks for enterprise HR technology. International Journal of Computer Technology and Electronics Communication, 8(2), 10483–10489.
25. Vedula, J. (2024). A security-integrated agile governance model for IT and operational technology modernisation in the oil and gas sector. International Journal of Research and Applied Innovations, 7(4), 11191–11196.
26. Ravichandran, S., & Kandasamy, V. (2025). Optimized Attention Augmented Residual Convolutional Neural Network with Fa-Resnet for Fabric Defect Detection. Journal of Control Engineering and Applied Informatics, 27(4), 3-15.
27. Chundi, V. R. K., Agarwal, V., & Arya, P. (2025, November). Green AI for Sustainable Supply Chains: Challenges in Emerging Economies. In 2025 International Conference on Computational Engineering, Sensing Technology and Management (ICCETM) (pp. 1-5). IEEE.
28. Raja, G. V., & Mali, R. K. (2021). Federated learning frameworks for privacy-preserving artificial intelligence applications. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(3), 4946-4950.
29. Gopinathan, V. R. (2023). Intelligent Cloud Security through Continuous Threat Detection and Risk Assessment. International Research Journal of Innovative Engineering, 7(6), 13571-13581.
30. Mohile, A., Kumar, P., Davis, J., & Mohammed, H. S. (2026, May). An Intelligent Hybrid Framework for Network Intrusion Detection Using Deep and Machine Learning. In 2026 2nd International Conference on Computing, Communication and Green Engineering (CCGE) (pp. 1-6). IEEE.
31. Bandaru, P. K. (2025). Achieving production readiness in software-defined vehicle platforms through comprehensive verification. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, *8*(2), 11789-11793.
32. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
33. Venkatasalam, K., Rajendran, P., & Thangavel, M. (2019). Improving the accuracy of feature selection in big data mining using accelerated flower pollination (AFP) algorithm. Journal of medical systems, 43(4), 96.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 5, September-October 2026|

DOI:10.15662/ijetemr.2026.1105004

34. Pothuri, M. K. (2025). Building Self-Service BI in the Cloud with AI Integration: Power BI and Snowflake. International Journal of Emerging Trends in Computer Science and Information Technology, 256-262.
35. Kalakoti, M. K. R., & Kalakoti, M. K. R. (2025). AI-augmented self-healing infrastructure: Combining health probes with remediation playbooks. Journal of Information Systems Engineering and Management, 10(58s), 1147-1157.
36. Badam, L. R. (2024). AI-based early warning system for financial scams targeting consumers. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, *7*(3), 10593-10602.
37. Sandhu, Y. S. (2024). Real time ETL optimization using change data capture incremental. International Journal of Emerging Trends in Engineering and Management Research, 9(3), 15711–15721.
38. Sugumar, R. (2022). Explainable Deep Learning Framework for Financial Fraud Detection and Intelligent Risk Analysis. International Journal of Emerging Trends in Engineering and Management Research, 7(5), 12528.
39. Matrouk, K., V, S., Kumar, S., Bhadla, M. K., Sabirov, M., & Saadh, M. J. (2023). Deep Learning–based Dynamic User Alignment in Social Networks. ACM Journal of Data and Information Quality, 15(3), 1-26.