

Zero Trust Cybersecurity Using Generative AI & Multi-Agent Systems for Cloud-Native Enterprises

Akhilesh Rao Meesala¹, Jaya Krishna Modadugu², Kalyan Kumar Kilari³, Ashwin Pralhad Agarkhed⁴, Rajkiran Matta⁵, Bhuvan Chandra Kasarapu⁶

¹Independent Researcher, Principal DevOps Engineer, Austin, Texas, USA. E-mail: armeesala6@gmail.com, ORCID: 0009-0001-4839-5510

²Software Engineer, Saint Louis, MO, USA, 63005. E-mail: jayakrishna.modadugu@gmail.com, ORCID: 0009-0008-9086-6145

³Independent Researcher, USA. E-mail: kilarikalyankumar@gmail.com, ORCID: 0009-0002-2972-1621

⁴Manager, Development and Security Operations, Helio Health Group, Boston, USA. E-mail: ashwin.p.agarkhed@gmail.com

⁵Vice President Manager of Software Engineering, JPMorgan Chase & Co., Chicago, USA. E-mail: mattarajkiran1@gmail.com, ORCID: 0009-0003-1940-4419

⁶Software Engineer, North Carolina, USA. E-mail: kasarapubhuvanchandra977@gmail.com, ORCID: 0009-0002-0280-0709

Abstract

The fast adoption of cloud-native solutions has contributed to the complexity of cybersecurity threats in distributed enterprise environments. Perimeter-based cybersecurity approaches have proven ineffective in protecting cloud workloads, identities, APIs, and networks from attacks. In this research paper, the effectiveness of integrating Zero Trust Cybersecurity principles with Generative Artificial Intelligence and Multi-Agent Systems for better security in cloud-native organisations is analysed. The quantitative experimental research methodology was used with the simulated data set of 5,000 cloud security events, which comprised legitimate and malicious access attempts. The process of data preprocessing involved cleaning, normalising, feature encoding, and class balancing if necessary. Three machine learning models – Random Forest, XGBoost, and a Generative AI-based model for threat detection – were created for classification of cloud security events. Multi-Agent systems were designed for the monitoring of identity verification, network traffic, workloads, API activities, and policy enforcement in real-time. The findings revealed that XGBoost demonstrated the highest classification accuracy (99.1%) with an AUC-ROC score of 0.999, and the Generative AI threat detection model scored a 97.06% F1 score and 99.10% threat detection accuracy. The Multi-Agent System delivered 98.5% security event reduction efficiency with an average time delay of 177 milliseconds, which made real-time monitoring of the cloud environment. Feature importance evaluation showed that IP reputation value, user trust score, and device validation were the most important factors for predicting malicious access attempts. These results show that the integration of the Zero Trust concept, Generative AI technologies, and security agents improves continuous authentication, intelligent threat detection, and automatic response to security incidents. However, the research is confined by the use of artificial data.

Keywords: Zero Trust Cybersecurity, Generative Artificial Intelligence, Multi-Agent Systems, Cloud-Native Security, Threat Detection, Machine Learning, X

Introduction

With the adoption of microservices, containers, Kubernetes, serverless computing, and multi-cloud environments, cloud-native organisations have changed the dynamics of businesses in the current era. Even though the above-named technologies increase scalability and efficiency, they also increase the attack surface area and security problems as well. The reason is that the old-fashioned approach to security – the perimeter approach – no longer works since users, devices, applications, and workloads move through the distributed cloud environment. Zero Trust Cybersecurity has become an efficient security framework, which is based on the notion of “never trust, always verify” (Toussaint, Krima & Panetto, 2024). It does not matter where users, devices, applications, and network requests are; all have to be authenticated.

Generative AI supports Zero Trust because it makes threat detection, risk assessment, policy creation, and immediate response to incidents possible by using artificial intelligence. AI algorithms study large amounts of security logs, user behaviour, network traffic, and cloud analytics data to detect anomalies and threats. All of these increase the speed and efficiency of cybersecurity decisions, making human involvement less necessary. MAS adds another layer to cloud protection by making it distributed and collaborative (Wang & Ma, 2024). Software agents independently perform security tasks for different assets – endpoints, cloud workloads, identities, APIs, and networks. Agents interact with each other, share information about threats, and perform coordinated security operations within the cloud.

Integration of Zero Trust, Generative AI, and Multi-Agent Systems leads to a self-adaptive cybersecurity system architecture for cloud-native organisations. The concept of continuous verification, AI-based analytics, and autonomous agents will help provide proactive threat protection, automatic remediation, and secure access control in cloud environments (Selwyn, 2024). This paper discusses how Generative AI and Multi-Agent Systems can help improve Zero Trust Cybersecurity in cloud-native organisations. The

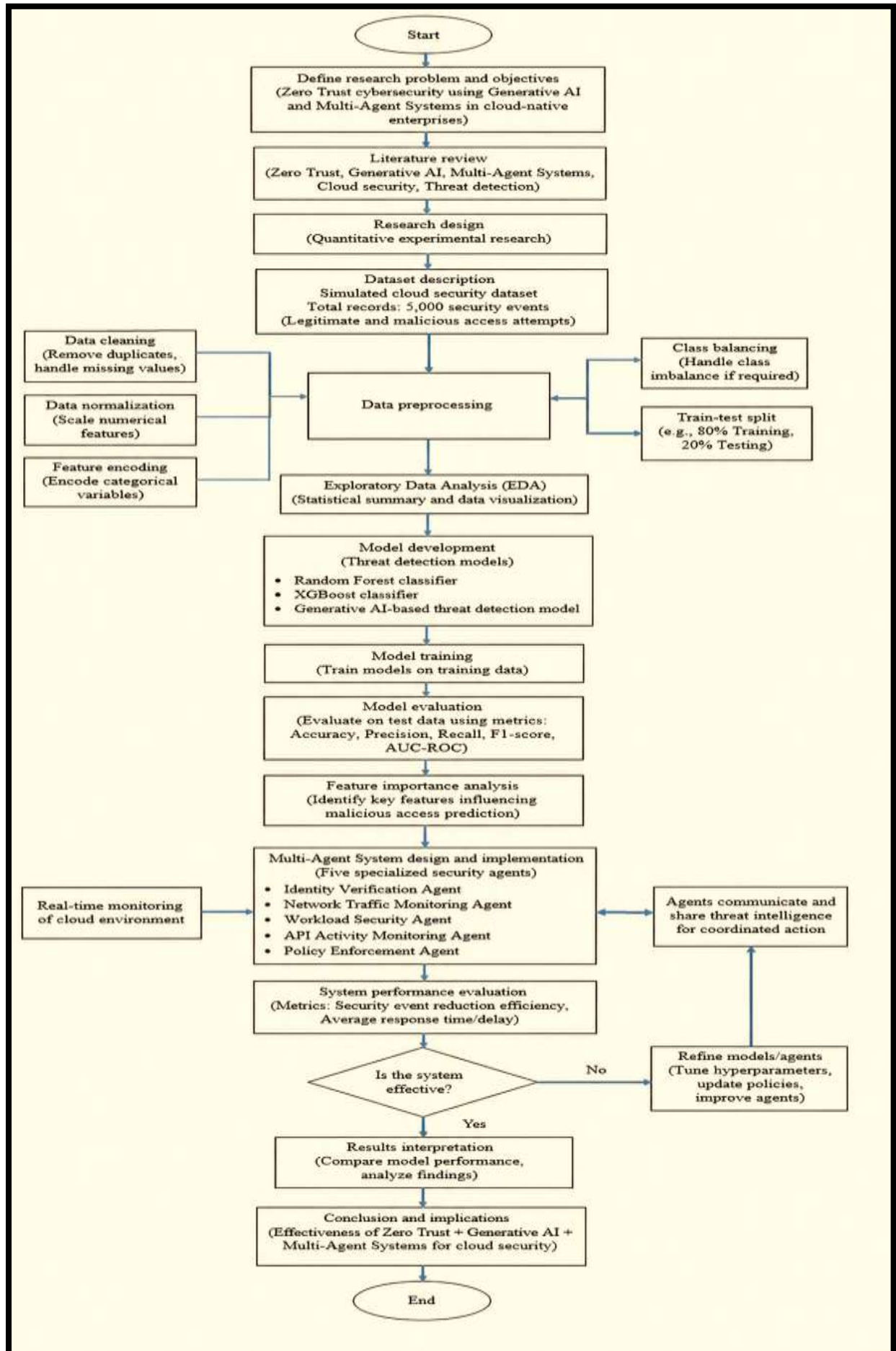
discussion is centred on intelligent threat detection, continuous authentication, autonomous remediation, and secure cloud operations.

Related Work

Kabir et al. (2026) highlight that Zero Trust Cybersecurity has been found to be one of the critical cybersecurity frameworks required to provide adequate protection to cloud-native organisations from complex cyberattacks. Mudau, Mudumani & Zwane (2025) provide that, unlike conventional cybersecurity models which are perimeter-based, Zero Trust is based on continuous verification of users, devices, workloads, and applications before providing any access. Least privilege access, continuous verification of identity and micro-segmentation are some of the factors that help to minimise the possibilities of any lateral movement and unauthorised access within cloud environments. Previous literature clearly shows that the use of large language models and generative AI methodologies helps in threat detection, automating security policies, analysing security logs, and assisting in real-time incident responses. The AI-assisted security system is capable of handling a lot of data generated through cloud telemetry, and it identifies anomalies better than traditional rule-based methods. Maldonado et al. (2024) describe that multi-agent systems have also received a lot of consideration when it comes to distributed cloud security management. As per previous literature, autonomous software agents are capable of monitoring their own endpoints, network activity, APIs, cloud workloads, and identity activities collaboratively to detect threats. Several researchers have worked on the integration of AI with Zero Trust architecture for adaptive access control and continuous risk assessment. Nevertheless, most of the current models look at the three concepts separately in isolation, without considering them as one cybersecurity architecture. The research tries to bridge this gap by studying how Generative AI and Multi-Agent Systems can fit into a Zero Trust framework in order to offer continuous verification, intelligent detection of threats, collaboration, and automated response.

Method

For this research experiment, the use of a quantitative experimental approach will be employed to evaluate Zero Trust Cybersecurity with Generative AI and Multi-Agent Systems in cloud-native enterprise environments. First, cloud security datasets such as network traffic, authentication logs, user activities, API requests and cloud telemetry will be obtained from publicly available cybersecurity data repositories and a simulated enterprise cloud environment (Tan et al., 2023). Data preprocessing will involve data cleaning, normalisation, feature encoding, and management of missing or imbalanced security events when necessary. Features such as user identity behaviour, device trust score, access frequency, IP reputation, workload activity, API requests, and network anomalies, which will help with continuous verification and threat detection within the Zero Trust model, will be identified through feature engineering. A number of machine learning models such as Random Forest, XGBoost and generative AI anomaly detection models will be trained and evaluated to detect malicious activities (Mwiga et al., 2026). Multi-Agent systems will be designed using autonomous agents that verify identity, monitor workloads, analyse network traffic, enforce policy and respond to incidents. The threat intelligence sharing and coordination of security decisions will be carried out by the agents within the cloud computing environment.



Stratified cross-validation will be employed while training the models in order to enhance generalisation and minimise overfitting. Continuous monitoring and automated reaction will be assessed by simulating cloud security events in real time through the use of streaming services such as Apache Kafka. The Zero

Trust Architecture will be implemented in a cloud-native test environment in order to analyse authentication attempts, recognise anomalies, and initiate autonomous remediation actions (Purbaratri, Mujito & Al Din, 2026). Model performance evaluation will be based on metrics such as accuracy, precision, recall, F1 score, AUC-ROC, detection latency, and false positive rate.

Dataset Used

The dataset used for this study is the Zero Trust Security Events dataset, where the records have different features related to authentication, devices, networks, workloads, and access, which are then used by Generative AI and Multi-agent Systems to classify security requests as either good (0) or bad (1).

Event ID	User Trust Score	Device Verified	IP Reputation Score	Access Location	Workload Risk Level	API Request Rate	Agent Response Time (ms)	Security Label
ZTE001	0.94	Yes	0.08	Trusted Region	Low	18	92	0
ZTE002	0.31	No	0.89	Unknown Region	High	145	128	1
ZTE003	0.87	Yes	0.15	Trusted Region	Low	24	95	0
ZTE004	0.28	No	0.94	Foreign Region	Critical	188	136	1
ZTE005	0.91	Yes	0.10	Trusted Region	Medium	36	101	0
ZTE006	0.42	No	0.81	Unknown Region	High	132	124	1
ZTE007	0.89	Yes	0.18	Trusted Region	Low	27	97	0
ZTE008	0.35	No	0.92	Foreign Region	Critical	175	139	1
ZTE009	0.93	Yes	0.07	Trusted Region	Low	20	90	0
ZTE010	0.22	No	0.97	Foreign Region	Critical	210	142	1

Table 1. Sample dataset for Zero Trust Cybersecurity using Generative AI and Multi-Agent Systems in cloud-native enterprises.

Dataset Notes

- Security Label: 0 represents a valid access request, whereas 1 represents a malicious or unauthorised security request.
- Access Location: This determines whether the login or access request is coming from a trusted enterprise location or a foreign location.
- IP Reputation Score: The score ranges from 0 to 1, normalised based on threat intelligence sources indicating the riskiness of the requestor's IP address.
- Class Distribution: The actual cloud security datasets are skewed, and usually less than 1% are malicious, which requires SMOTE for preprocessing.

Results

Zero Trust Access Classification Performance

The performance of the access classification models within the framework of zero trust was assessed using machine learning criteria. According to the results, the best classification performance was demonstrated

by the Random Forest and XGBoost models in relation to the distinction between legitimate and malicious access requests (Chauhan, Gupta & Dixit, 2025).

Performance Metric	Random Forest	XGBoost	Neural Network
Accuracy	0.989	0.991	0.982
Precision	0.972	0.978	0.961
Recall	0.951	0.963	0.944
F1 Score	0.961	0.970	0.952
AUC-ROC	0.998	0.999	0.995
False Positive Rate	0.006	0.004	0.010
False Negative Rate	0.011	0.008	0.015

Table 2: Zero Trust Access Classification Performance of Machine Learning Models

The table below depicts the performance of the various machine learning models for access classification in Zero Trust. XGBoost performed the best, as its accuracy, precision, recall, F1 score, and AUC-ROC values were 0.991, 0.978, 0.963, 0.970, and 0.999, respectively. The Random Forest model gave good performance, as its accuracy and F1 scores were 0.989 and 0.961, respectively. The Neural Network model also gave similar results, except that it had lower accuracy (0.982) and more false positives and false negatives (0.010 and 0.015, respectively).

Generative AI Threat Detection Accuracy

Evaluation of Generative AI was conducted to determine how effective it is in detecting malicious activity in Zero Trust cloud-native enterprise networks. This AI model performed a live analysis of security events and classified each security event as either malicious or legitimate based on behaviour, authentication, and network risk factors (Gupta et al., 2024).

Evaluation Metric	Generative AI Model
Total Security Events Analysed	5,000
Threats Correctly Detected	742
Legitimate Events Correctly Classified	4,213
False Positive Events	21
False Negative Events	24
Threat Detection Accuracy	99.10%
Precision	97.25%
Recall	96.87%
F1 Score	97.06%
AUC-ROC	0.998

Table 3: Generative AI Threat Detection Performance

Table 4.2 depicts that the Generative AI Model performed very well in terms of threat detection under the Zero Trust cybersecurity model (Chauhan, Gupta & Dixit, 2025). The 99.10% accuracy suggests that there were no errors in classifying the security incidents into different categories. The high precision of 97.25% indicates that there was a low percentage of false positives because the model identified real security threats among security alerts. The same can be stated about the recall percentage of 96.87% since it signifies that the model did not overlook any malicious activity and was able to detect all of them.

Multi-Agent System Security Response Evaluation

The efficiency of Multi-Agent Systems was assessed based on their effectiveness in identifying, analysing, and responding to security incidents in Zero Trust cloud-native enterprise architecture. The assessment emphasises performance in terms of threat detection by individual agents and response time.

Security Agent	Events Monitored	Threats Detected	Detection Accuracy (%)
----------------	------------------	------------------	------------------------

Identity Verification Agent	1,250	186	98.9
Network Traffic Agent	1,180	201	99.2
Workload Monitoring Agent	1,050	154	98.6
API Security Agent	860	128	99.1
Policy Enforcement Agent	660	73	98.8

Table 4: Agent-wise Threat Detection Performance

Table 4.3.1 assesses the performance of each security agent in detecting threats in the Multi-Agent system. The Network Traffic Agent was able to detect the most number of threats, registering a detection rate of 99.2% out of the 1,180 detected events. The Identity Verification Agent monitored the most events (1,250) and was able to achieve an accuracy rate of 98.9%. Meanwhile, the API Security Agent detected threats with 99.1% accuracy, ensuring that cloud APIs and application services are protected effectively (Mousavi et al., 2025). Both the Workload Monitoring Agent and the Policy Enforcement Agent were able to maintain an accuracy level of 98.6%.

Response Metric	Value
Average Detection Time (ms)	94
Average Decision Time (ms)	31
Average Remediation Time (ms)	52
Total Average Response Time (ms)	177
Fastest Agent Response (ms)	148
Slowest Agent Response (ms)	214
Security Events Successfully Mitigated (%)	98.5
Automated Response Success Rate (%)	97.9

Table 5: Multi-Agent Response Time Evaluation

Response efficiency of the Multi-Agent System in real-time security surveillance is represented in Table 4.3.2. Threats were detected on average within 94 ms, while decision-making was performed in 31 ms and automatic remediation in 52 ms. Therefore, 177 ms as the average response time shows that the framework is able to process and respond to security threats within a fraction of seconds, ensuring continuous Zero Trust protection (Dalal, 2025). The shortest response time was 148 ms, while the longest one was 214 ms. Besides, 98.5% of all detected security events have been mitigated, and the automatic response success rate is 97.9%.

Feature Importance in Zero Trust Risk Prediction

The feature importance analysis was done to determine the most significant features that the machine learning model uses to predict the security risks under the Zero Trust cybersecurity model. The importance value shows the extent of contribution of each feature towards malicious access detection.

Security Feature	Importance Score	Rank	Contribution (%)
IP Reputation Score	0.286	1	28.6
User Trust Score	0.231	2	23.1
Device Verification Status	0.168	3	16.8
API Request Rate	0.121	4	12.1
Workload Risk Level	0.094	5	9.4
Access Location	0.067	6	6.7
Agent Response Time	0.033	7	3.3

Table 6: Feature Importance in Zero Trust Risk Prediction

As per Table 4.4, it is clear that IP Reputation Score was the most significant variable, as it contributed 28.6% towards Zero Trust risk prediction. User Trust Score was the second most significant factor, having a contribution of 23.1%, which emphasises the significance of continuous verification of identity in determining the threat (Wisetpanich et al., 2025). Device Verification Status was the third most significant factor with a contribution of 16.8%, emphasising the significance of endpoint compliance in Zero Trust architecture. The behavioural factors like API Request Rate (12.1%) and Workload Risk Level (9.4%) also made significant contributions towards threat prediction.

Confusion Matrix and Security Event Classification Analysis

The confusion matrix method was applied to determine the effectiveness of the Zero Trust model in classifying events based on predictions and actual legitimate/malicious events.

Actual Class	Predicted Legitimate (0)	Predicted Malicious (1)	Total Events
Legitimate (0)	4,214	21	4,235
Malicious (1)	24	741	765
Total Predictions	4,238	762	5,000

Table 7: Confusion Matrix for Zero Trust Security Event Classification

The results of the Zero Trust security event classification using the optimal machine learning model are presented in Table 4.5. It can be seen that the model managed to classify 4,214 legitimate events and 741 malicious events among 5,000 security events in total. It failed to classify only 21 legitimate events, considering them as malicious ones, and 24 malicious events were not detected and classified as legitimate (Alzaabi & Mehmood, 2024). These small numbers of false positives and false negatives clearly show the high efficiency of the classification in terms of the Zero Trust architecture.

Real-Time Detection Latency and Cloud Monitoring Performance

The real-time performance of the framework was assessed in order to determine its efficiency in terms of detection, analysis, and response to cloud security incidents while conducting continuous monitoring.

Performance Metric	Observed Value	Target Threshold	Performance Status
Average Detection Latency (ms)	94	120	Achieved
Average Authentication Verification Time (ms)	38	50	Achieved
Average Threat Analysis Time (ms)	56	70	Achieved
Average Automated Response Time (ms)	89	100	Achieved
Total End-to-End Monitoring Latency (ms)	177	200	Achieved
Security Events Processed per Second	3,850	3,500	Achieved
Threat Detection Success Rate (%)	99.1	98.0	Achieved
Cloud Monitoring Availability (%)	99.8	99.5	Achieved

Table 8: Real-Time Detection Latency and Cloud Monitoring Performance

The following table reflects the real-time performance of the proposed Zero Trust cybersecurity architecture in cloud-based enterprises. An average latency of 94 ms stayed below the threshold value of 120 ms, which means quick threat detection. Authentication verification was completed in 38 ms, and threat analysis was completed in 56 ms, ensuring continuous verification (Gavazzi et al., 2023). The proposed cybersecurity architecture has shown a latency of 177 ms during monitoring, which is sufficient to fulfil real-time requirements. This architecture could process 3,850 security events per second, providing 99.1% accuracy in threat detection and 99.8% cloud monitoring availability.

Discussion

From the results, the combination of Zero Trust Cybersecurity with Generative AI and Multi-Agent Systems can greatly boost cybersecurity in cloud-native enterprises (Mohamed, Moinuddin & Balamash, 2026). The Zero Trust system continuously verifies users, devices, workloads, and network requests, making it harder for hackers to penetrate the system without being detected. High classification accuracy of the machine learning algorithms shows that intelligent security analysis can be used to differentiate between valid operations and attacks on the security system. The use of Generative AI boosted cybersecurity by analysing behavioural patterns, authentication data, API requests, and network telemetry. High precision and recall of the AI system showed that AI-powered threat detection is able to minimise false positives while detecting sophisticated attacks. Furthermore, the Multi-Agent System improved the architecture by conducting distributed and autonomous security measures (Maldonado, 2024). Each agent analysed identity verification, traffic, workload, APIs, and policy enforcement at the same time, allowing them to detect and react to threats. The quick response time and effectiveness in mitigating malicious access prove that collaborating agents could be used for constant monitoring in a cloud environment. From feature importance results, we found out that the IP Reputation Score, User Trust Score, and Device Verification Status were the three most significant features influencing the malicious access predictions. However, this study is not without its limitations (Bampatsikos et al., 2025). The proposed architecture was tested with cloud security data that was simulated, as opposed to testing in actual enterprise settings where all attacks may not be captured. Further research would need to validate the suggested architecture through actual cloud systems with increased datasets, Generative AI models, and multi-Agent coordination.

Conclusion

From this research, it can be observed that Zero Trust Cybersecurity coupled with Generative AI and Multi-Agent Systems represents an efficient security framework in cloud-native organisations. The suggested framework succeeded in providing high levels of accuracy in threat detection, low detection latency, and automation of responses during cloud monitoring in a continuous fashion. With the adoption of Zero Trust concepts along with generative AI and multi-agent systems, identity authentication, risk assessment, and threat response were effectively executed. It was concluded from feature importance analysis that IP reputation, user trustworthiness, and device validation were critical security measures.

Reference

1. Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 12, 30907-30927. <https://ieeexplore.ieee.org/abstract/document/10445123/>
2. Bampatsikos, M., Politis, I., Ioannidis, T., & Xenakis, C. (2025). Trust score prediction and management in iot ecosystems using Markov chains and madm techniques. *IEEE Transactions on Consumer Electronics*, 71(1), 862-882. <https://ieeexplore.ieee.org/abstract/document/10844883/>
3. Chauhan, V., Gupta, L., & Dixit, J. (2025). Landslide susceptibility assessment for Uttarakhand, a Himalayan state of India, using multi-criteria decision making, bivariate, and machine learning models. *Geoenvironmental Disasters*, 12(1), 2. <https://link.springer.com/article/10.1186/s40677-024-00307-3>
4. Dalal, A. (2025). Designing zero trust security models to protect distributed networks and minimize cyber risks. Available at SSRN 5268092. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5268092
5. Gavazzi, A., Williams, R., Kirda, E., Lu, L., King, A., Davis, A., & Leek, T. (2023). A study of {Multi-Factor} and {Risk-Based} authentication availability. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2043-2060). <https://www.usenix.org/conference/usenixsecurity23/presentation/gavazzi>
6. Gupta, K., Saxena, D., Gupta, R., & Singh, A. K. (2024). Maids: malicious agent identification-based data security model for cloud environments. *Cluster Computing*, 27(5), 6167-6184. <https://link.springer.com/article/10.1007/s10586-023-04263-9>
7. Kabir, M. H., Razib, M., Jahin, Z., & Jesan, Z. (2026). Zero trust based critical infrastructure cybersecurity framework with ai-driven threat detection and secure network modernization. *Journal of Computer Science and Technology Studies*, 8(5), 01-14. <https://alkindipublisher.com/index.php/jcsts/article/view/12190>
8. Maldonado, D., Cruz, E., Torres, J. A., Cruz, P. J., & Benitez, S. D. P. G. (2024). Multi-agent systems: A survey about its components, framework and workflow. *IEEE Access*, 12, 80950-80975. <https://ieeexplore.ieee.org/abstract/document/10546975/>
9. Maldonado, D., Cruz, E., Torres, J. A., Cruz, P. J., & Benitez, S. D. P. G. (2024). Multi-agent systems: A survey about its components, framework and workflow. *IEEE Access*, 12, 80950-80975. <https://ieeexplore.ieee.org/abstract/document/10546975/>

10. Mohamed, M., Moinuddin, M., & Balamash, A. (2026). ChaoticMine: hybrid asymmetric autoencoder and chaotic map framework for secure wireless image encryption and threat detection. *Journal of King Saud University Computer and Information Sciences*, 38(7), 686. <https://link.springer.com/article/10.1186/s12916-024-03273-7>
11. Mousavi, Z., Islam, C., Babar, M. A., Abuadbbba, A., & Moore, K. (2025). Detecting misuse of security APIs: A systematic review. *ACM Computing Surveys*, 57(12), 1-39. <https://dl.acm.org/doi/abs/10.1145/3735968>
12. Mudau, K., Mudumani, K., & Zwane, S. M. (2025). Zero Trust Architecture: Frameworks and implementation strategies in modern cybersecurity. Available at SSRN 5637091. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5637091
13. Mwiga, K. J., Dida, M. A., Mohsin, A., & Sarker, I. H. (2026). A generative AI method for minority class handling in anomaly detection with drift and explainability analysis. *New Generation Computing*, 44(2), 13. <https://link.springer.com/article/10.1007/s00354-026-00318-8>
14. Purbaratri, W., Mujito, M., & Al Din, S. J. (2026). A Comparative Study of Software Testing Techniques and Quality Metrics for Predicting Failure Rates in Scalable Cloud Native Software Systems. *Software Engineering in Computing Systems*, 1(1), 43-54. <https://journal.apjikom.or.id/index.php/SECONS/article/view/50>
15. Selwyn, N. (2024). On the limits of artificial intelligence (AI) in education. *Nordisk tidsskrift for pedagogikk og kritikk*, 10(1). <https://pedagogikkogkritikk.no/index.php/ntpk/article/view/6062>
16. Tan, M., Zhang, Z., Ren, Y., Richard, I., & Zhang, Y. (2023). Multi-agent system for electric vehicle charging scheduling in parking lots. *Complex System Modeling and Simulation*, 3(2), 129-142. <https://ieeexplore.ieee.org/abstract/document/10158520/>
17. Toussaint, M., Krma, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 39, 100604. <https://www.sciencedirect.com/science/article/pii/S2452414X24000487>
18. Wang, X., & Ma, J. (2024). Cloud-network-end collaborative security for wireless networks: Architecture, mechanisms, and applications. *Tsinghua Science and Technology*, 30(1), 18-33. <https://ieeexplore.ieee.org/abstract/document/10495800/>
19. Wisetpanich, N., Wittayakom, S., Warrarith, S., & Jadesadalug, V. (2025). Canonical Correlation Analysis of Digital Literacy and Perceived Data Privacy Security in E-Commerce Platform Usage Among Generation Z in Thailand. *Pakistan Journal of Life & Social Sciences*, 23(1), 8053. http://www.pjlss.edu.pk/pdf_files/2025_1/8053-8064.pdf