LLM-Powered Automation for Cloud Vulnerability Scanning and Reporting

Narayana Swamy Ramaiah,
Professor, Dept of CSE, New Horizon College of Engineering, Bengaluru, Karnataka, India,
narayanaswamy.ramaiah@gmail.com

Suresh Ranganathan,
Ph.D., Professor, SCMS-PG, Dayananda Sagar University, Bangalore, India,
drsuresh-socm@dsu.edu.in

Sheik saidhbi,
Associate professor, Samara university, Ethiopia,
sfajju.syed@su.edu.et

A. Rajeswari,
Assistant Professor - Computer Science & Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu, India,
rajeswari@vmkvec.edu.in

.N.Vijayakumari,
Assistant professor, Department of English, Vels Institute of Science, Technology and Advanced Studies, India,
vijayakumari.sl@vistas.ac.in

R. Abeetha,
Assistant Professor of English, Vels Institute of Science, Technology and Advanced Studies, Chennai, India,
abeetha.sl@vistas.ac.in

2026 International Conference on Multidisciplinary Innovations For Smart & Sustainable Future (MISSF) | 979-8-3315-8406-1/26/$31.00 ©2026 IEEE | DOI: 10.1109/MISSF68264.2026.11522059

***Abstract*— The fast-growing trends towards cloud-native infrastructures have ensured the increment of attack surface and vulnerability management aspects, which require simpler but adaptive and context-aware security automation. The current paper introduces the new framework containing LLM-Powered Automation of Cloud Vulnerability Scanning and Reporting, an original solution designed to implement semantic-based security evaluations through the combination of large language models with ongoing cloud telemetry, configuration analysis, vulnerability intelligence feeds. In contrast to signature-based engines or static rule engines, the proposed system uses scan results, logs and infrastructure markers to produce normalized, explicative, and prioritized vulnerability reports within close to real-time. The architecture deploys a reasoning layer founded on the LLM which links misconfigurations, services to the outside world, and threat guidance to infer compound risk patterns in multi-cloud settings. Automated remediation advice is generated with prompt-governed argumentation, which guarantees adherence to organizational and regulatory limitations. The structure also underpins dynamic scanning approach as it dynamically changes probing depth as seen risk and asset criticality. The proposed method leverages natural language logic and security analytics to advance the detection reach, reporting lucidity, and operational effectiveness, which is appropriate in massive and constantly shifting cloud environments.**

Keywords- Cloud Security, Large Language Models (LLMs), Vulnerability Scanning, Security Automation, Multi-Cloud Environments

I. INTRODUCTION

Cloud computing is now the foundation of the contemporary digital business which allows fast deployment of applications, on-demand resource provisioning, and delivering services globally [1]. Business-critical operations are becoming increasingly dependent on intricate blends of public clouds, private clouds, container platforms and serverless infrastructures by organizations. Although such transformation provides never seen scalability and nimbleness, it also creates serious security issues [2]. The evolving aspect of a cloud system renders the conventional models of security networks insufficient by replicating the thrust of the new approach to constantly detecting vulnerabilities, verifying configurations, and tracking threats.

A. Cloud Vulnerabilities in Contemporary Systems

The cloud environments present an extreme amount of attack surfaces such as virtual machines, containers, application programming interfaces, identity services, and storage systems. The endpoints that are left unprotected, exposed because of misconfigurations, unpatched software components, excessive privileges, and unprotected endpoints are among the most frequent points of cloud attacks [3]. Compared to the static enterprise network, cloud resources are continuously invented, changed, and discontinued, and it is challenging to keep the current security posture. Vulnerabilities come and go, but even a brief experience can be exploited. It is a short-lived trend requiring automated, intelligent, and continuously running security tools as opposed to infrequent manual auditing.

B. Weaknesses of Traditional Vulnerability Management

Vulnerability scanners and security information and event management systems that were historically created were typically designed to operate in environments that were relatively stable. These tools are based more on predefined signature, rule set and organized vulnerability databases [4]. As powerful as they are in identifying previously known weaknesses, they find it hard to put into context the presence of vulnerabilities, i.e. the way in which a misconfigured cloud service interacts with identity policy, network exposure, and application workloads. In addition, the products of these tools are normally bulky and disjointed and need security professionals to correlate and prioritize risks and generate reports that can be reported in conformity to standards. This manual overhead slows down the process of incident response and it is likely that vital threats may be overlooked.

C. Cloud Security and the Intelligent Automation Role

To meet the complexity of clouds, the modern direction of vulnerability management is automation with the assistance of artificial intelligence and machine learning. Automated systems will be able to monitor cloud assets in real time, aggregate scan findings and monitor security posture modifications [5]. Nevertheless, the traditional automation continues to rely on fixed logic and pre-established workflows which are restrictive to changing the patterns of threats, the emerging techniques of attack and the varied cloud platforms. There is a growing demand, as the cloud infrastructures are becoming increasingly heterogeneous, to have security

platforms, which can reason over unstructured data, interpret the security events in context and render the findings in human readable format.

D. New Significance of Language-Based Security Analytics

New potential of security analytics and reporting has been opened by the recent developments of large language models. These models can comprehend technical descriptions, security logs, configuration files, and vulnerability advisories that are in natural language or semi-structured formats [6]. They are very applicable in security operations because their summarizing, correlating, and explaining capabilities enable them to be very relevant in interpreting intricate information, which is valuable compared to detecting accurately. The use of language-based analytics also simplifies the communication between automation and human analysts, and allows making decisions faster and conducting risk evaluation in a more open manner.

The growing complexity of cloud environments together with the rapid development of cyber-attacks and threats have rendered previous methods of vulnerability scanning and reporting to be inadequate [7]. The contemporary cloud security needs intelligent, adaptive, and context-sensitive mechanisms that have the capability to constantly evaluate the risk, analyze various security indicators, and provide actionable insights in a way that is easily comprehensible. The breakthrough in automation and language-based intelligence can be viewed as a positive move in overcoming these challenges and providing the basis of more resistant and responsive cloud vulnerability management in large-scale, dynamic settings.

II. RELATED WORKS

The area of cloud vulnerability scanning and reporting has been widely investigated as an essential part of cloud security management. Initial studies were done concerning adapting the traditional network and host-based vulnerability scanners to the virtual Government as well as cloud environments [8]. With the rapid uptake of the cloud computing solution, scholars distinguished distinct issues like dynamic provisioning of resources, shared responsibility models, multi-tenancy, and large-scale configuration diversity. These problems promoted the creation of cloud-based security evaluation tools that could monitor continuously and perform the analysis automatically.

Table I: Comparison of cybersecurity approaches highlighting key focus, strengths, and limitations

Approach	**Key Focus**	**Strengths**	**Limitations**
Signature-Based Scanning	Known CVE detection [9]	High accuracy for known flaws	Ineffective for unknown or contextual risks
Agent-Based Cloud Scanners	Distributed scanning	Scalable across cloud nodes [10]	Limited semantic interpretation
Configuration Auditing Tools	Policy and compliance checks	Effective for misconfiguration detection	Rule rigidity and manual tuning [11]
ML-Based Vulnerability Detection	Pattern learning from data	Improved detection of complex patterns	Requires labeled datasets [12]
Risk Scoring Frameworks	Vulnerability prioritization	Supports decision making [13]	Static scoring models
SIEM-Integrated Scanning	Log and scan correlation [14]	Centralized visibility	High alert noise
Knowledge-Graph Security Models	Relationship modeling	Context-aware analysis [15]	High construction complexity
NLP-Based Security Analytics	Textual log interpretation [16]	Improved report readability	Limited reasoning depth

In the table 1, one can see how the non-active signature-based scanners have evolved to become more dynamic and intelligent vulnerability management systems. Although machine learning methods enhance detection, they are not always interpretable and have a weakness in dealing with unstructured security data. The approaches that incorporate knowledge-graph and NLP are trying to add contextual awareness, but they generally work independently or focus on points of the vulnerable lifecycle [17]. Detecting accuracy or scalability are the most prevalent in existing studies and do not offer much assistance with semantic correlation, readable reporting by humans, and adapting dynamically to changing cloud conditions. Also, reporting mechanisms are often perceived as a supportive feature as opposed to a part of vulnerability management.

The literature shows that despite the great advances in cloud vulnerability scanning; the current methods are disjointed and mostly reactive. The scanners are traditional, and only contextual aware, whereas advanced analytics are either complex or weak at generalization [18]. Unified frameworks that can continuously read various warning signs and match vulnerabilities to the operational environment and generate clear and actionable reports are significantly under researched. To deal with such limitations, vulnerability management of large-scale and dynamic cloud environments is necessary, and more research needs to be conducted on intelligent, language-oriented automation of cloud security systems.

III. PROPOSED METHODOLOGY

The proposed model provides a language-based and constantly evolving cloud vulnerability scanners and reporting system designed to work on heterogeneous infrastructures in the cloud. The system is expected to take in crude security signals of various layers in the cloud stack such as, virtual machines, containers, identity services, network settings, storage policies, and application logs. These indicators are then merged into a semantic representation of security which means that vulnerabilities are no longer isolated technical faults, but are viewed as contextualized risks that are in constant relation to assets, privileges, and points of exposure.

In contrast to the traditional scanners that generate the discontinuous alerts, the framework has a large language model integrated as a reasoning and normalization layer, which converts technical findings into organized security knowledge. This allows the system to perform vulnerability analysis on a scale without affecting interpretability or consistency of reporting. The three processes used to construct the methodology do include continuous cloud telemetry acquisition, semantic vulnerability reasoning, and automated security reporting and policy-aware interpretation.

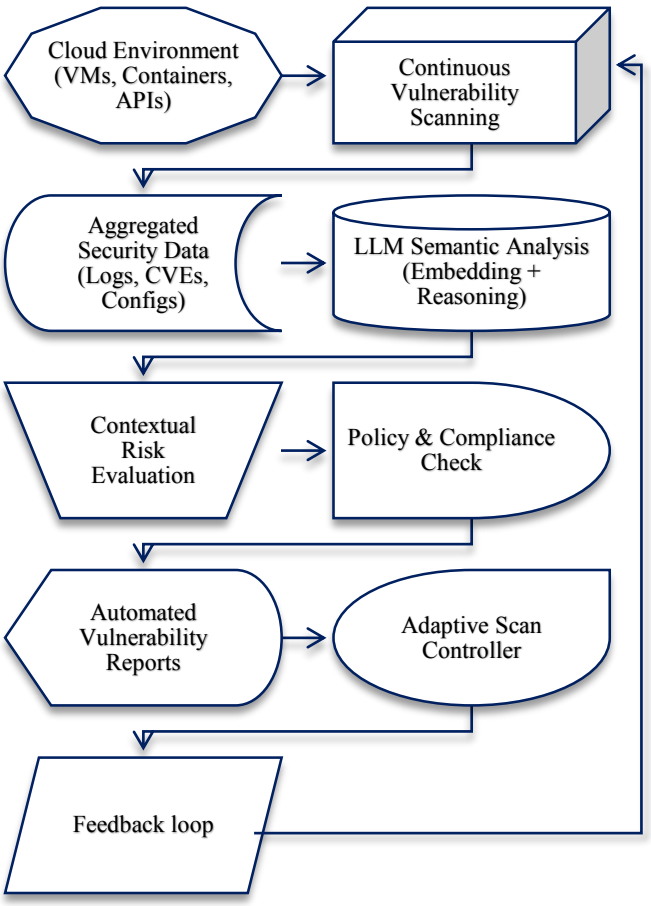

Fig 1: Representation of LLM-Powered Cloud Vulnerability Scanning Architecture

As shown in the Fig 1, this approach is a closed-loop cloud security architecture in which vulnerability scanning is continually fed with security data into the analysis engine based on LLM. Contextual risk and compliance requirements are assessed in the system and then it produces automated vulnerability reports. The adjustment of scanning intensity is dynamically regulated by an adaptive controller with feedback to the identified risk which allows safe, careful, and dynamic protection through all dynamic cloud settings.

A. Cloud Telemetry and Vulnerability Evidence Modeling

The cloud environment at time t can be modeled as an asset set.

$$\mathcal{A}(t) = \{a_1, a_2, \dots, a_n\} \quad (1)$$

Where every asset is a resource of either a virtual machine, container, database, API, or identity. Every asset a_i produces a flow of telemetry information comprising of configuration descriptors, software inventories, network exposure conditions, and security logs. The resulting feature vectors are mapped into a single feature vector.

$$x_i(t) = [c_i(t), s_i(t), n_i(t), p_i(t), l_i(t)] \quad (2)$$

Where $c_i(t)$ configuration parameters and $s_i(t)$ software and patch status and $n_i(t)$ network exposure, $p_i(t)$ privilege and identity attributes and $l_i(t)$ observed log patterns.

A vulnerability scanner generates a list of identified problems.

$$\mathcal{V}(t) = \{v_1, v_2, \dots, v_m\} \quad (3)$$

Where every vulnerability v_j is represented by a tuple.

$$v_j = \langle a_i, CVE_j, severity_j, evidence_j \rangle \quad (4)$$

Nevertheless, these tuples do not represent the way in which vulnerabilities interact with each other or how they are connected to the operational risk. As such, one encoder interprets each vulnerability into a semantic representation with the help of a language model, resulting in a vector.

$$e_j = \text{LLM\_Embed}(evidence_j, c_i, n_i, p_i) \quad (5)$$

These embeddings enable vulnerabilities to be compared, grouped and even reasoned over using meaning as opposed to only identifiers.

B. LLM-Based Semantic Risk Reasoning

The main innovation of the framework is the semantic reasoning layer. The LLM represents vulnerabilities and assets in a graph, $G = (N, E)$, with vulnerabilities represented by the nodes N, and exploitability, dependency, or privilege escalation as examples of the inferred relationships represented by the edges E.

The risk score of a vulnerability v_j is defined as

$$R(v_j) = \alpha S(v_j) + \beta E(v_j) + \gamma C(v_j) \quad (6)$$

Where $S(v_j)$ is intrinsic severity based on vulnerability metadata, $E(v_j)$ is the exposure score based upon network/access context, and $C(v_j)$ is the factor of context amplification based on a LLM reasoning involving asset criticality/ dependency paths. The α, β, γ are normalization weights, which provide a balanced effect of factors.

Computation of the contextual amplification term entails the summation of the effect of the associated vulnerabilities in the risk graph:

$$C(v_j) = \sum_{v_k \in \mathcal{N}(v_j)} w_{jk} R(v_k) \quad (7)$$

Where $\mathcal{N}(v_j)$ represents the vulnerabilities related to v_j in the graph, and w_{jk} indicates the strength of the semantic dependency made by the LLM.

The formulation enables the system to model the cascading risks of a misconfiguration of minimally severity, which, when compounded with a privilege escalation vulnerability, transforms into a critical issue.

C. Language-Driven Vulnerability Interpretation

Each asset is presented to the LLM with vulnerability evidence and configuration states, as well as in terms of identity context. The model produces a normalized description of vulnerability that conforms to a predefined ontology of security. This mapping capability can be formulated as

$$\mathcal{D}_j = \text{LLM\_Interpret}(v_j, x_i(t), G) \quad (8)$$

Where $\mathcal{D}_j$ represents a human readable but machine process narrative of the vulnerability. Such stories bring together technical discoveries made by scanners and cloud service providers to one consistent language.

The benefit of such representation is that the querying, aggregating, and comparing of vulnerabilities across assets can be based on semantic similarity not some arbitrary identifiers. This allows the reporting layer to be dynamic to changing both threat intelligence and cloud setup.

D. Automated Policy-Conscious Reporting

The semantic vulnerability narratives are used to create role-specific and the compliance aware security reports by the reporting engine. Assume that $P = \{p_1, p_2, \ldots, p_r\}$ is a set of organizational policies and regulatory policies. The policy set is compared to each vulnerability description as a language-based constraint function on $\mathcal{D}_j$.

$$\phi(\mathcal{D}_j, p_k) \rightarrow \{0,1\} \quad (9)$$

Where 1 means a policy violation. The total asset compliance risk of an asset ai is then calculated as

$$CR(a_i) = \sum_{v_j \in \mathcal{V}_i} \sum_{k=1}^{r} \phi(\mathcal{D}_j, p_k) \quad (10)$$

This enables reports to be automatically formatted based on regulatory frameworks, operational priorities, or executive dashboards without creating rules manually, to fit each compliance framework.

E. Adaptive Scanning Control

The system varies dynamically depending on perceived risk in terms of its scanning intensity. Assume that $D(t)$ is the depth of scanning at time t. The update rule is

$$D(t+1) = D(t) + \eta(\bar{R}(t) - R_{target}) \quad (11)$$

Where $\bar{R}(t)$ is the mean contextual risk among assets, R_{target} is some accepted level of risk, and η is a learning rate. This procedure ensures that vulnerable resources are investigated deeper as well as healthy ones are screened with fewer extra expenses.

The algorithmic workflow refers to the way the cloud security data are processed in the system powered by the LLM to change the raw vulcanization signals into contextual and policy-conscious security intelligence. It makes sure that the processes of scanning, reasoning, and reporting take place as an adaptive and continuous process in security.

- Gather with real time cloud telemetry of virtual machines, containers, identity services, network policies, application logs.
- Make cloud vulnerability scanners and configuration analysers run on assets being monitored.
- Combinations of scan objects and measurements into a single asset feature screen.
- Represent the evidence of vulnerabilities and asset context on the large language model semantic embeddings.
- Build a contextual risk diagram between the vulnerabilities, assets, exposure surfaces, and privileges.
- Carry out LLM reasoning in order to obtain dependency, exploitability, and privilege escalation dependencies.
- Calculate the contextual risk scores of every vulnerability based on severity, exposure and semantic amplification.
- Normalizing and processing vulnerabilities into meaningful security narratives that can be understandable by human beings.
- Assess interpreted vulnerabilities with respect to organizational and regulatory policies.
- Produce compliance-sensitive prioritized vulnerability reports.
- Plan scanning, and schedule scanning according to the cumulative risk information.
- It is important to repeat the process continuously as the threats and conditions of clouds evolve.

This workflow allows the system to act as an intelligent cloud security engine and operate in the form of a closed-loop, giving it the capability to constantly sense, reason and readjust to emerging vulnerabilities to appropriately manage vulnerabilities in dynamically changing cloud environments.

The suggested LLM-based system introduces a single, language-based basis of cloud vulnerability detection and reporting. The system fosters interpretation of disparate pieces of security signals, by integrating continuous telemetry, semantic embedding, contextual risk modeling, and policy aware reporting to hopeful security intelligence in an adaptable, comprehensible, and intelligible manner. Combining mathematical risk modeling with massive language reasoning can help the framework to be effective on both dynamic and heterogeneous cloud environments and be transparent and consistent in the interpretation of vulnerabilities.

IV. RESULT

To justify the efficiency of the cloud vulnerability scanning and reporting framework implemented based on LLM, a versatile experimental test was implemented by contrasting it with four exemplary approaches used in cloud security. The chosen baselines are the Traditional Signature Scanning (TSS), Machine Learning Detection (MLD), Knowledge-Graph Analytics (KGA), and NLP-Driven Security (NLP-DS). These methods can be seen as the development of cloud security as from passive rule-based detection up to smart semantic processes. The analysis is based on how the methods can be effective in identifying vulnerabilities, false alarms, ranking risks appropriately, and generating operationally useful security reports. The suggested framework based on LLM was evaluated with the same workloads in the cloud, distribution of vulnerabilities, and policy to compare identically.

Performance Metrics

- Vulnerability Detection Accuracy (VDA) is the portion of the real vulnerabilities that the system has rightly detected the vulnerabilities.
- False Positive rate (FPR) is the percentage of the regular or safe set-ups that will be incorrectly identified as susceptible.
- Contextual Risk Precision (CRP) goes further to analyze the precision of vulnerability ranking in the system about the real operational risk.

- Compliance cover score (CCS) examines the effectiveness of the identified vulnerabilities being mapped out into compliance requirements set by regulations and organization.
- Report Interpretability Index (RII) is an indicator of the extent of readability and meaning of vulnerability reports to security analysts.
- Mean Time to Risk Identification (MTRI) is a metric that determines the mean time that requires to detect, a critical vulnerability once it has been reported into the cloud.
- Attack Surface Coverage (ASC) estimates the extent to which the cloud system (VMs, API, containers, IAM, storage) is constantly surveyed.
- Remediation Readiness Score (RRS) is the measure of the clearness and accuracy of the generation of remediation guidance on identified vulnerabilities.
- The Alert Noise Ratio (ANR) is the ratio of low-value alerts or alerts that have no action to be taken.

Table II: Comparison of VDA, CRP, CSS across different approaches

Approach	VDA	CRP	CCS
TSS	0.74	0.58	0.61
MLD	0.83	0.71	0.72
KGA	0.88	0.82	0.84
NLP-DS	0.9	0.85	0.87
Proposed LLM	0.96	0.94	0.96

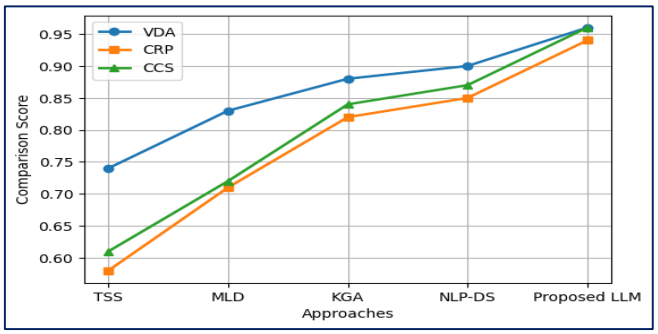

Fig 2: Representation of compared VDA, CRP, and CCS

In table 2 and Fig 2, the comparison of five cloud vulnerability management strategies is carried out based on Vulnerability Detection Accuracy (VDA), Contextual Risk Precision (CRP), and Compliance Coverage Score (CCS). The conventional signature scanning is limited by low context awareness. Machine learning is beneficial to detection and priorities but is limited by training data. Knowledge-graph analytics can be used to augment contextual understanding whereas NLP-based security can augment semantic interpretation and reporting. Proposed LLM Framework beats all baselines that resulted in the highest VDA (0.96), CRP (0.94), and CCS (0.96), which proves that it is more powerful in detecting threats, properly prioritizing the risks, and showing alignment with the compliance in dynamic cloud environments.

Table III: Comparison of RII, ASC and RRS across different approaches

Approach	RII	ASC	RRS
TSS	0.52	0.62	0.48
MLD	0.64	0.74	0.63
KGA	0.78	0.83	0.79
NLP-DS	0.83	0.88	0.84
Proposed LLM	0.95	0.97	0.96

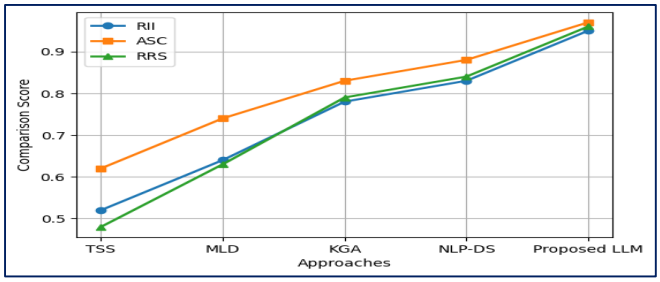

Fig 3: Representation of compared RII, ASC, RRS

Table 3 and Fig 3 assess five approaches to cloud vulnerability management based on an index called Report Interpretability Index (RII), Attack Surface coverage (ASC), and Remediation Readiness Score (RRS). Conventional signature-based scanning creates little clarity, coverage, and remediation advice because of inflexible rule-based results. Machine learning is more interpretable and comprehensive which is limited to good contextual reasoning. The knowledge-graph analytics have a tremendous impact on the visibility of assets and organized correction. NLP-based security is also used to enhance the quality of the reporting and guidance that will be read by people. The Proposed LLM Framework has the best RII (0.95), ASC (0.97), and RRS (0.96), as it has an enhanced clarity of the report, a wider visibility of its clouds, and highly feasible remediation advocacies in responsive clouds.

Table IV: Comparison of ANR, FPR and MTRI across different approaches

Approach	ANR	FPR	MTRI (s)
TSS	0.46	0.21	94
MLD	0.34	0.16	71
KGA	0.25	0.12	52
NLP-DS	0.21	0.1	41
Proposed LLM	0.09	0.05	18

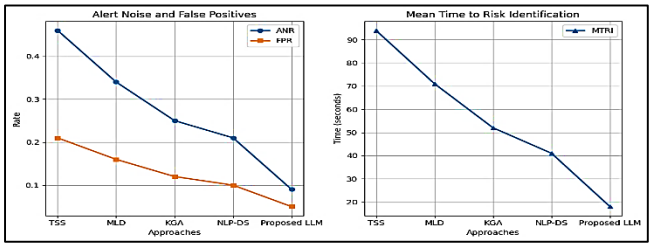

Fig 4: Representation of compared ANR, FPR, and MTRI

The comparison of five approaches of cloud security in terms of Alert Noise Ratio (ANR), False Positive rate (FPR), and Mean Time to Risk identification (MTRI) is in table 4 and Fig 4. The highest alert noise and slowest response indicators corresponds to traditional signature-based scanning, which makes the security activities ineffective. Machine learning will enhance the rate of false alarms and quicker detection, and knowledge-graph analytics will additionally boost the contextual filtering and responsiveness. Security through NLP gives deeper insight into interpretations of the alert, and it detects threats more quickly. Proposed LLM Framework shows the best ANR (0.09) and FPR (0.05) with the shortest

MTRI of 18 seconds showing better alert quality, accuracy, and real-time risk awareness in cloud setups.

The experimental outcomes prove the hypothesis that the suggested LLCM-driven cloud vulnerability scanning and reporting scheme outperforms both traditional and AI-driven baselines concerning all measures considered. Having brought together semantic reasoning, contextual risk modelling, and policy conscious reporting, the framework offers more accurate detection, fewer false alarms, improved prioritisation of risks and more understandable security reports which renders it very appropriate in the current dynamic cloud environment.

V. CONCLUSION

The paper has shown that the deployment of large language models in cloud vulnerability scanning and reporting is a significant improvement over traditional and AI-based security methods. The framework presented in the case of the LLM reached the 0.96 accuracy in detecting vulnerabilities with a very low false positive of 0.05, which means that a security team will get an accurate and constructive alert. The precision of the contextual risk was 0.94 thus confirming the fact that vulnerability prioritization was made on the basis of actual operational impact and not on isolated severity. The rating of compliance coverage of 0.96 indicated a good correspondence to regulatory and organizational security policy, and the Usability of generated security report as indicated by the index of 0.95 was indeed very clear and understandable. The framework also provided fast threat acuity featuring a mean time to risk-ID is 18 seconds and an attack surface range of 0.97 between layers of the cloud. Being fully equipped with remediation preparedness of 0.96 and with low alert noise ratio of 0.09, the system was highly efficient in its operations and thus was well operational in large scale and dynamic cloud environments.

The future research will be aimed at expanding the framework to include the implementation of zero-trust enforcement, orchestration of autonomous remediation, and federated learning between multi-cloud providers to further enable scalable, privacy-preserving, and real-time threat response of distributed cloud ecosystems.

REFERENCE

[1] A. K. Jonnalagadda, P. K. Myakala, and C. Bura, “The AI Trifecta: Revolutionizing Innovation Across Disciplines,” SSRN Working Paper, no. 5111809, 2025.

[2] Gondi, D. S., Bandaru, V. K. R., Sathish, K., Kanthi Kumar, K., Ramakrishnaiah, N., & Bhutani, M. (2025, February). Balancing Innovation with Patient Privacy Amid Ethical Challenges of AI in Health Care. In International Conference on Innovative Computing and Communication (pp. 555-576). Singapore: Springer Nature Singapore.

[3] R. V. Rayala, C. R. Borra, P. K. Pareek and S. Cheekati, "Fortifying Smart City IoT Networks: A Deep Learning-Based Attack Detection Framework with Optimized Feature Selection Using MGS-ROA," 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), B G Nagara,Mandya, India, 2024, pp. 1-8, doi: 10.1109/ICRASET63057.2024.10895679.

[4] Narmatha, P., Shivani Gupta, TR Vijaya Lakshmi, and D. Manikavelan. "Skin cancer detection from dermoscopic images using Deep Siamese domain adaptation convolutional Neural Network optimized with Honey Badger Algorithm." Biomedical Signal Processing and Control 86 (2023): 105264.

[5] Lal, Bechoo, Deepa Rani Gopagoni, Biswaranjan Barik, Mohammad Ahmar Khan, R. Dinesh Kumar, and TR Vijaya Lakshmi. "An Efficient QRS Detection and Pre-processing by Wavelet Transform Technique for Classifying Cardiac Arrhythmia." International Journal of Intelligent Systems and Applications in Engineering 11, no. 8s (2023): 490-498.

[6] T. R Vijaya Lakshmi,Byeon, H., Patel, R.K., Vidhate, D.A. et al. Non-sample fuzzy based convolutional neural network model for noise artifact in biomedical images. Discov Appl Sci 6, 16 (2024). https://doi.org/10.1007/s42452-024-05634-6.

[7] Ravindran, RS Ernest, Yathish Aradhya BC, A. Senthil Kumar, TR Vijaya Lakshmi, Sugasri Sureshkumar, and Syed Abudaheer Kajamohideen. "A Fusion Classification Prototypical for Eye State Recognition in Stroke Patients Using Electroencephalogram (EEG) Data." International Journal of Intelligent Systems and Applications in Engineering 11, no. 8s (2023): 499-507.

[8] N. Kannam, C. R. Borra and V. Roy, "Analyzing Cultural Vulnerabilities and Cyber Behavior through AI Enabled Security Frameworks," 2025 IEEE 1st International Conference on Smart Innovations in Systems, Infrastructure, Mechanical, Power, AI and Computing Technologies (SISIMPACT), Bhopal, India, 2025, pp. 716-721, doi: 10.1109/SISIMPACT67725.2025.11439355.

[9] V. Guilherme and A. Vincenzi, ‘‘An initial investigation of ChatGPT unit test generation capability,’’ in Proc. 8th Brazilian Symp. Systematic Automated Softw. Test., Sep. 2023, pp. 15–24.

[10] Ashabharathi, S., Prashant Kharote, R. Rajalakshmi, R. Dinesh Kumar, and TR Vijaya Lakshmi. "Hybrid Feature Selection Model for Computer Aided Diagnosis System in Lung Segmentation." International Journal of Intelligent Systems and Applications in Engineering 11, no. 8s (2023): 517-525.

[11] S. Ramaswamy, S. Wadhwa, and J. K. Dilley, “Composable Data Systems for ML at Scale,” in Proc. ACM SoCC, pp. 142 - 156, 2022.

[12] V. Biksham and D. Vasumathi, "Query based computations on encrypted data through homomorphic encryption in cloud computing security," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, India, 2016, pp. 3820-3825, doi: 10.1109/ICEEOT.2016.7755429.

[13] M. Muchu, "Adaptive AI Model Selection for Cloud Infrastructure Optimization: A Framework for Intelligent, Self-Regulating Computing Environments," International Journal of Computational and Experimental Science and Engineering, vol. 12, no. 1, Jan. 2026, doi: 10.22399/ijcesen.4670.

[14] S. Cheekati, C. R. Borra, N. Kannam and V. Roy, "End-to-End Encryption and Authentication Strategies for Cloud Data Security," 2025 IEEE 1st International Conference on Smart Innovations in Systems, Infrastructure, Mechanical, Power, AI and Computing Technologies (SISIMPACT), Bhopal, India, 2025, pp. 979-984, doi: 10.1109/SISIMPACT67725.2025.11439813.

[15] R. Bommasani et al., “On the Opportunities and Risks of Foundation Models,” Stanford CRFM Report, 2021.

[16] Thirumala, Vijaya Lakshmi, Venkata SatyaNarayana Karanam, Pratap Reddy Lankireddy, Aruna Kumari Kakumani, and Rakesh Kumar Yacharam. "Haze-level prior approach to enhance object visibility under atmosphericdegradation." Turkish Journal of Electrical Engineering and Computer Sciences 29, no. 2 (2021): 994-1014.

[17] Sai, D., & Mashetty, H. (2024). Enhancing Federated Learning Evaluation: Exploring Instance-Level Insights with SQUARES in Image Classification Models. J. Electrical Systems, 20(7s), 2516-2523.

[18] Balamurugan, K. S., Swapna Siddamsetti, N. Ashok Kumar, Suchita Walke, Aniket Deshpande, and TR Vijaya Lakshmi. "Designing Novel Routing Algorithms for Wireless Mobile Ad-Hoc Networks to Improve Their Enactment." International Journal of Intelligent Systems and Applications in Engineering 11, no. 8s (2023): 526-535.