International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Use of Location-Based Access Control to Protect Cloud Computing with Artificial Intelligence

VARSHA SHRIVAS
Research Scholar

Dr. Rishikesh Rawat
Research guide

https://doi.org/10.55041/ijsmt.v2i5.406

Cite this Article: SHRIVAS, V. (2026). Use of Location-Based Access Control to Protect Cloud Computing with Artificial Intelligence. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.406

Abstract

Cloud computing systems are facing growing security concerns due to their distributed nature and continuously changing access behaviors. Conventional Identity and Access Management (IAM) approaches often fail to provide real-time responsiveness and lack awareness of contextual factors. To overcome these limitations, this study proposes a multi-layered security framework powered by Artificial Intelligence (AI). The model incorporates location-based dynamic code generation, user authentication, and machine learning–driven anomaly detection to strengthen security mechanisms.

The proposed system enhances authentication by integrating user credentials with geolocation information and time-dependent hexadecimal codes, making unauthorized access significantly more difficult. Furthermore, a trained machine learning model continuously monitors user behavior to identify and prevent suspicious activities. A practical scenario is included to demonstrate the effectiveness of the approach.

This review also examines the role of AI and Machine Learning (ML) in transforming cloud security, particularly in Identity and Access Management. It highlights the shortcomings of traditional access control systems in terms of scalability and real-time adaptability, and presents an AI-based framework capable of intelligent authentication, adaptive threat detection, and predictive decision-making. Based on the analysis of 34 research papers published between 2015 and 2025, including 29 journal articles, 1 article, and 4 conference papers, the study emphasizes that integrating AI with cloud computing is essential for developing secure, efficient, and context-aware access control systems. The proposed framework not only enhances security and reduces unauthorized access but also improves user experience and ensures better compliance with modern security standards.

Keywords

Cloud Security, IAM, Artificial Intelligence, Machine Learning, Anomaly Detection, Dynamic Authentication, Location-Based Security

1. Introduction

Cloud computing has transformed modern IT systems but introduces serious security concerns such as unauthorized access, identity theft, and insider attacks. Traditional IAM systems rely on static rules and credentials, making them insufficient for dynamic environments.

Advantage of cloud computing:-

- It eliminates the need for physical hardware and lowers operating expenses.

Scalable and flexible: Easily adapts to shifting business requirements.

- The costeffectiveness of cloud computing is one of its advantages
- High Availability: Provides dependable services with little interruption.
- Global Reach: Anywhere there is an internet connection, services are accessible.
- Top cloud service providers make significant investments in cutting-edge security protocols.
- Artificial intelligence, machine learning, big data analytics, and the Internet of Things are just a few of the contempora ry technologies that rely on cloud computing.

Recent research shows that AI-driven IAM systems enable real-time decision-making, anomaly detection, and adaptive authentication, improving cloud security significantly.

This paper proposes a hybrid security model combining:

- Authentication (password-based)
- Context-awareness (location-based)
- Dynamic code generation
- Machine learning-based anomaly detection

2. Literature Review

AI enhances IAM through adaptive authentication and anomaly detection

- Machine learning improves threat detection and automation in cloud systems
- Traditional IAM lacks scalability and real-time response
- Hybrid approaches combining AI and security mechanisms provide better protection

Literature Review

Ref	Authors & Year	Focus Area	Techniques Used	Key Contribution	Limitations
[1]	Nzeako & Shittu (2024)	IAM Security	AI, ML	AI-driven adaptive authentication & access control	No cryptography
[2]	Nzeako & Shittu (2024)	Data Access Optimization	AI, ML	Intelligent data access & reduced latency	Lacks encryption focus
[3]	Ang'udi (2023)	Cloud Security Challenges	AI, ML, Cryptography	Comprehensive security framework	General study
[4]	Mahalakshmi et al. (2023)	Access Control	Blockchain, ZKP, Encryption	AuthPrivacyChain framework	Scalability issues
[5]	Paulraj et al. (2023)	Authentication	ECC, MARL	Anonymous identity-based ACP model	Complex implementation
[6]	Singh & Chatterjee (2015)	Data Security	Cryptography, Steganography	Encryption-based protection	No AI/ML
[7]	Bhamare et al.	ML Security Validation	Supervised ML	Shows generalization failure	Needs hybrid ML
[8]	Dey et al.	Authentication	Hashing	Lightweight MDA protocol	Limited scope

Ref	Authors & Year	Focus Area	Techniques Used	Key Contribution	Limitations
[9]	Ghegade & Rokade	ML Security Review	SVM, KDD dataset	ML improves threat detection	Dataset dependency
[10]	Lonetti & Marchetti	Access Control	RBAC, ABAC, XACML	Analysis of access models	Lack of adaptive models
[11]	Markandey et al.	Data Security	Encryption	Privacy-preserving models	No AI integration
[12]	Indu et al. (2018)	IAM	Cryptography	IAM classification	No ML/AI
[13]	Mahendar & Shivakanth (2025)	IDS	CNN, SMOTE	AI-SCAN high accuracy (97.5%)	Resource intensive
[14]	Shah (2018)	AI + Cloud	AIaaS	Scalable AI-cloud integration	Security briefly covered
[15]	Abdullah & Bakar	Access Control	RAdAC, Cryptography	Risk-based adaptive model	Needs real-world testing
[16]	Ahmed	IDS	ML, Hybrid models	Improved detection accuracy	Dataset limitations
[17]	Suman et al.	ML Security	ML + Cryptography	Hybrid security models	Needs real-time validation
[18]	Kumar	AI + Cloud	AI analytics	Intelligent cloud transformation	Limited security depth
[19]	Maciel & Dhakal	IAM	Behavioral Biometrics	Continuous authentication	Early-stage research
[20]	—	ML Security	ANN, KNN, SVM	Threat classification	General review
[21]	Rajani & Jyoti	Deep Learning Security	LSTM	Real-time detection	Computational cost
[22]	—	Access Control	DAC, MAC, ABAC	Hybrid access models	Static policies
[23]	Kiruthika et al.	ML Prediction	SVM, J48	Threat prediction	Needs scalability
[24]	Begum & Hossain	Data Security	RSA, Blowfish, SHA	Hybrid cryptography	Performance overhead
[25]	Nalla (2023)	Risk Management	AI predictive analytics	Proactive threat detection	Data dependency
[26]	Cader & Nirmala	ML Security	ML categories	Comparative analysis	No implementation
[27]	—	Cloud Security	AI, Encryption	Multi-layer security approach	General framework
[28]	—	Security Trends	AI, Blockchain	Future security strategies	No experiments
[29]	—	Blockchain Security	ZKP, AES, RSA	High efficiency AuthPrivacyChain	Scalability
[30]	Paulraj et al.	Access Control	MARL	Secure cross-cloud access	Complexity
[31]	Shirley et al.	ML Security	J48, AODE	IDS optimization	Privacy concerns
[32]	—	AI vs Traditional	UEBA, SOAR	AI improves prediction	Bias issues
[33]	—	AI Security	NLP, DL	Real-time threat detection	High cost
[34]	Mircea Iu (2024)	ML Security Review	ANN, SVM, KNN	Large-scale analysis (87 papers)	No unified model

Table 1 :- Summary of Literature Review

3. Research Gap

Despite significant advancements in cloud security, existing approaches largely focus on isolated techniques such as machine learning-based intrusion detection, cryptographic protection, or blockchain-based access control. There is a lack of a unified, context-aware, and adaptive security framework that integrates dynamic authentication mechanisms with real-time anomaly detection. Furthermore, current systems fail to incorporate contextual parameters like location and time into access decisions, and often suffer from scalability, dataset dependency, and limited real-world applicability. Therefore, there is a critical need for a hybrid, intelligent, and lightweight security model that combines dynamic code-based authentication, context awareness, and machine learning-driven anomaly detection to enhance Identity and Access Management in cloud environments.

4. Proposed Methodology Algorithm

```
BEGIN

// Step 1: Generate Dynamic Code

FETCH Location_Details

GENERATE Code_Number = Hex(timestamp + Location + random_salt)


// Step 2: User Authentication

INPUT User_ID, Password

IF credentials are valid THEN

   PROCEED

ELSE

   DENY ACCESS

   EXIT

END IF


// Step 3: Access Request

SEND (User_ID, Location_Details, Code_Number)


// Step 4: Validate Code

IF Code format is correct AND

  Code matches User & Location AND

  Code is within valid time

THEN

   PROCEED

ELSE
```

```
    DENY ACCESS
    EXIT
END IF

// Step 5: ML-Based Anomaly Detection
INPUT (User behavior, Time, Access pattern, Location, Code)
RUN ML_Model

IF Output == "Normal" THEN
    GRANT ACCESS
ELSE
    DENY ACCESS
    ALERT Admin
END IF
// Step 6: Logging
STORE transaction details in log
END
```

Step	Phase	Input	Process	Output
1	Pre-Authentication	—	Fetch user **Location_Details** and generate **Code_Number** using Hex(timestamp + location + salt)	Dynamic security code
2	User Authentication	User_ID, Password	Validate user credentials	If valid → Proceed; else → Deny
3	Access Request	User_ID, Location_Details, Code_Number	User submits request with generated code and location	Request initiated
4	Code Validation	Code_Number	Check format, match with user & location, verify expiry	If valid → Proceed; else → Deny

Step	Phase	Input	Process	Output
5	ML-Based Anomaly Detection	Behavior profile, time, pattern, location, code	Analyze using trained ML model	Normal / Anomalous
6	Decision	ML Output	Grant or deny access	Access control decision
7	Logging	All request data	Store logs for auditing & monitoring	System log generated

Table 2 :- Phase wise description:-

Datasetthatcanbeused:-

https://unsw-my.sharepoint.com/:x:/r/personal/z5025758_ad_unsw_edu_au/_layouts/15/Doc.aspx?sourcedoc=%7B2A810F6A-CC3D-4D98-909E-37489D8DAF98%7D&file=UNSW_NB15_testing-set.csv&action=default&mobileredirect=true

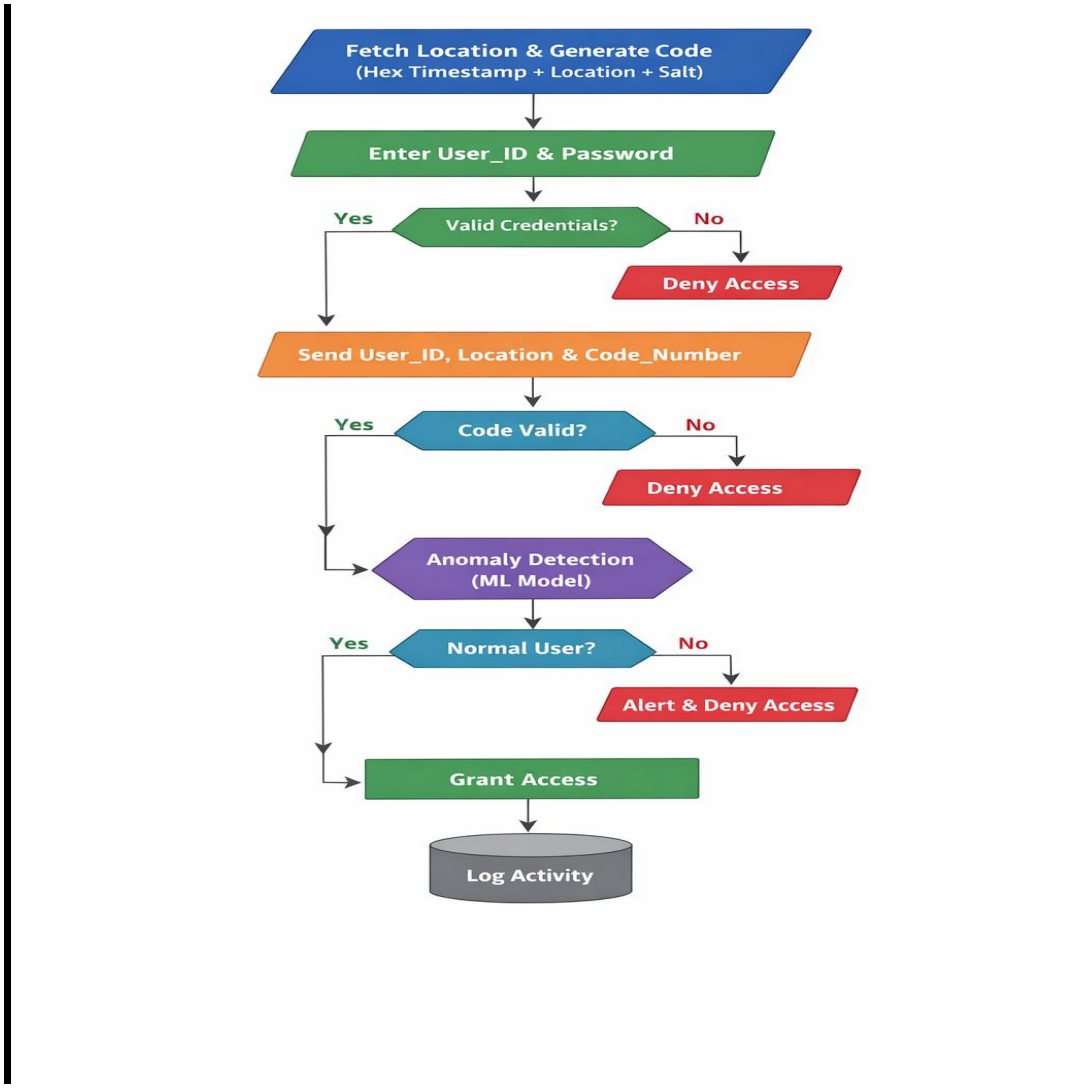

Figure 1:- Flow chart of Algorithm

5. Example

Secure Login in Cloud System

User: Rahul
Location: Bhopal, India
Time: 10:30 AM

Step 1: Code Generation
Timestamp = 1710757800
Location = Bhopal
Salt = X7A9

Code = Hex(1710757800 + Bhopal + X7A9)
Generated Code = A3F9B7C

Step 2: Authentication

- User enters:
  - User_ID = Rahul123
  - Password = ******

Credentials Valid

Step 3: Access Request
Rahul123, Bhopal, A3F9B7C

Step 4: Code Validation

- Code format correct
- Matches location
- Not expired

Step 5: ML Anomaly Detection

Parameter	Value
Location	Same as usual
Time	Normal
Behavior	Normal
Device	Known

ML Output: **Normal**

Step 6: Decision

Access Granted

Step 7: Logging
User: Rahul123
Status: Success
Time: 10:30 AM
Location: Bhopal

Attack Scenario Example

- Location: Unknown (Russia)
- Time: 3 AM
- Behavior: Abnormal

ML Output: Anomalous
Access Denied + Alert sent

6. Conclusion

The proposed cloud-based secure login system utilizes dynamic code generation based on a combination of timestamp, location, and a random salt value to deliver a robust and adaptive authentication mechanism. By incorporating contextual factors such as time and geographical location along with randomized elements, the system effectively minimizes the risks associated with replay attacks, credential compromise, and unauthorized access.

This method strengthens conventional authentication techniques by introducing dynamic, one-time verification codes, which are difficult for attackers to replicate or predict. Furthermore, when integrated with cloud security frameworks and machine learning-based monitoring systems, it enables real-time detection of suspicious activities, enhances data security, and ensures stronger access control mechanisms. Overall, the proposed approach supports the development of a secure, scalable, and intelligent authentication framework for modern cloud computing environments.

7. Future Scope

The proposed system can be further improved through several enhancements aimed at strengthening security, scalability, and overall usability:

1. **Integration with Machine Learning Techniques**

Future advancements may incorporate AI/ML algorithms to analyze user behavior patterns—such as login time, device usage, and access frequency—to automatically detect anomalies and potential security threats.

2. **Multi-Factor Authentication (MFA)**

Enhancing the system by combining dynamic codes with additional authentication methods, such as biometrics (fingerprint or facial recognition) or OTP-based verification, can provide an extra layer of security.

3. **Blockchain-Enabled Authentication**

Implementing blockchain technology can enable decentralized identity management and ensure tamper-resistant authentication records, thereby increasing system transparency and trust.

4. **Advanced Geo-Fencing Mechanisms**

Incorporating more accurate location verification using GPS and IP-based intelligence can help restrict access to predefined trusted zones, improving location-based security.

5. **Quantum-Resistant Cryptographic Methods**

To address future threats posed by quantum computing, the system can adopt quantum-safe encryption techniques that ensure long-term data protection.

6. **Adoption of Zero Trust Architecture**

Integrating Zero Trust principles—where every access request is continuously verified—can significantly enhance security within cloud environments.

7. **Real-Time Threat Intelligence Integration**

Connecting the system with global threat intelligence platforms can enable the identification of emerging attack patterns and facilitate automatic updates to defense strategies.

8. **Scalability for Enterprise-Level Deployment**

Optimizing the framework to support large-scale cloud infrastructures with millions of users and distributed systems will ensure efficient performance and reliability.

References

1. Nzeako, G., & Shittu, R. A. (2024). Improving data access in cloud computing environments through AI and machine learning. *Journal of Innovative Technologies, 7*.

2. Chen, W., & Li, X. (2024). Improving data access in cloud computing environments through AI and machine learning. *Journal of Innovative Technologies, 7.* Retrieved from https://academicpinnacle.com/index.php/JIT

3. Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. *World Journal of Advanced Engineering Technology and Sciences, 10*(2), 155–181.

4. Mahalakshmi, J., Reddy, A. M., Sowmya, T., Chowdary, B. V., & Raju, P. R. (2023). Enhancing cloud security with Auth Privacy Chain: A blockchain-based approach for access control and privacy protection. *International Journal of Intelligent Systems and Applications in Engineering.*

5. Paulraj, D., Neelakandan, S., Prakash, M., & Baburaj, E. (2023). Admission control policy and key agreement based on anonymous identity in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications.*

6. Rao, R. V., & Selvamani, K. (2015). Data security challenges and their solutions in cloud computing. *Procedia Computer Science, 48,* 204–209. *Elsevier.*

7. Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2016, December 19–22). Feasibility of supervised machine learning for cloud security. *Proceedings of the 3rd International Conference on Information Science and Security (ICISS 2016),* Pattaya, Thailand.

8. Dey, S., Sampalli, S., & Ye, Q. (2016). MDA: Message digest-based authentication for mobile cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 5*(18). https://doi.org/10.1186/s13677-016-0068-6

9. Ghegade, T. S., & Rokade, M. (2022). Application of machine learning approach to cloud security: A review. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2*(6), 342–348. https://doi.org/10.48175/IJARSCT-4254

10. Lonetti, F., & Marchetti, E. (2018). Issues and challenges of access control in the cloud. In *Proceedings of the 14th International Conference on Web Information Systems and Technologies (WEBIST 2018)* (pp. 261–268). SCITEPRESS. https://doi.org/10.5220/0006948702610268

11. Markandey, A., Dhamdhere, P., & Gajmal, Y. (2018, September 28–29). *Data access security in cloud computing: A review.* Proceedings of the 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Galgotias University, Greater Noida, India.

12. Indu, I., Rubesh Anand, P. M., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal, 21*(4), 574–588. Elsevier. Retrieved from https://www.elsevier.com/locate/jestch

13. Mahendar, K., & Shivakanth, G. (2025). A performance analysis of ML-based intrusion detection systems in cloud environments. *International Journal of Electrical and Electronic Engineering and Telecommunications, 14*(4), 1–10.

14. Shah, H. (2018). Cloud computing and next-generation AI: Creating the intelligence of the future. *International Research Journal of Engineering & Applied Sciences (IRJEAS), 6*(3), 40–47. Retrieved from http://www.irjeas.org

15. Abdullah, S., & Abu Bakar, K. A. (2018). Towards secure risk-adaptable access control in cloud computing. *International Journal of Advanced Computer Science and Applications (IJACSA), 9*(12), 324–331. Retrieved from http://www.ijacsa.thesai.org

16. Ahmed, Q. O. (2024). Machine learning for intrusion detection in cloud environments: A comparative study. *Journal of Artificial Intelligence General Science (JAIGS), 6*(1). https://doi.org/10.60087

17. Suman, O. P., Saini, L. K., & Singh, D. (2024). Securing clouds with machine learning: Advancements in theoretical and experimental research. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 4*(8), 223–230. Retrieved from http://www.ijarsct.co.in

18. Kumar, A. (2024). AI-driven innovations in modern cloud computing. *Computer Science and Engineering, 14*(6), 129–134. https://doi.org/10.5923/j.computer.20241406.02

19. Maciel, L. R., & Dhakal, V. (2020). Applying AI concepts for identity and access management in cloud environments. *ISP Class Research Report,* New York University, NYU Tandon School of Engineering.

20. Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Sensors, 20*(18), 5109. https://doi.org/10.3390/s20185109

21. Rajani, M., & Jyoti, D. (2024). *Deep learning-driven cybersecurity framework for cloud computing.* In *Proceedings of the International Conference on Science, Engineering & Management Trends. International Journal of Science, Engineering and Technology,* ISSN 2348-4098.

22. Dubey, S., & Rai, P. K. (2021). A review of cloud service security with various access control methods. *International Journal of Computer Science and Mobile Computing, 10*(3), 39–45. https://doi.org/10.47760/ijcsmc.2021.v10i03.005

23. Kiruthika, K., Maheshkumar, R. S., Sridharan, S., & Jeevananthan, V. (2024, November 23–25). *Machine learning for predicting cloud security.* In *Proceedings of the IACIDS 2023 Conference,* Lavasa, India. European Alliance for Innovation (EAI). https://doi.org/10.4108/eai.23-11-2023.2343236

24. Begum, T., & Hossain, M. E. (2021). Enhancing the security of cloud computing by building hybrid cryptography algorithms. *International Journal of Computer Applications, 183*(44), 22–28.

25. Nalla, K. K. (2023). Predictive analytics with AI for cloud security risk management. *World Journal of Advanced Engineering Technology and Sciences, 10*(2), 297–308. https://doi.org/10.30574/wjaets.2023.10.2.0298

26. Cader, S. H. A., & Nirmala, K. (2023). A periodical review of machine learning algorithms for cloud security. *IOSR Journal of Computer Engineering (IOSR-JCE),* 25(2), 20–22. Retrieved from https://www.iosrjournals.org

27. Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. *World Journal of Advanced Engineering Technology and Sciences, 10*(2), 155–181. https://doi.org/10.30574/wjaets.2023.10.2.0304

28. Alam, S., & Bhardwaj, H. (2023). Enhancing cloud security in the digital age. In *Proceedings of the International Conference on Recent Trends in Engineering & Technology (ICRTET-2023).* Arya Institute of Engineering & Technology, Jaipur, Rajasthan.

29. Mahalakshmi, J., Reddy, A. M., Sowmya, T., Chowdary, B. V., & Raju, P. R. (2023). Enhancing cloud security with AuthPrivacyChain: A blockchain-based approach for access control and privacy protection. *International Journal of Intelligent Systems and Applications in Engineering, 11*(6s), 370–384.

30. Paulraj, D., Neelakandan, S., Prakash, M., & Baburaj, E. (2023). Admission control policy and key agreement based on anonymous identity in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 12*(71). https://doi.org/10.1186/s13677-023-00446-2

31. Shirley, C. P., Thanga Helina, S., Thusita, S., & Okesh, A. (2025). Machine learning for cloud security: A systematic review. *Journal of Information Systems Engineering and Management, 10*(37s). https://www.jisem-journal.com

32. Talati, D. V. (2024). AI-powered cloud security: Using user behavior analysis to achieve efficient threat detection. *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET).* https://doi.org/10.15680/IJIRSET.2024.1305590

33. Gopal Varma, S. C. (2024). AI-enhanced cloud security: Proactive threat detection and response mechanisms. *International Journal for Multidisciplinary Research (IJFMR), 6*(6). Retrieved from https://www.ijfmr.com

34. Ţălu, M. (2024). Exploring machine learning algorithms to enhance cloud computing security. *Digital Technologies Research and Applications, 4*(2). Technical University of Cluj Napoca, Romania.