# AURA-X: AI-Powered Framework for Secure Cloud Access

Manpreet Kaur [1], Monika Sachdeva [2], Rajeev Kumar Bedi [3]

{ mk.ripple59@gmail.com [1], monika@ptu.ac.in [2], rajeevbedi12@gmail.com [3] }

Project Associate, Dept. of CSE, IKGPTU, Kapurthala, India[1], Professor , Dept. of CSE, IKGPTU, Kapurthala, India[2], Associate Professor, Dept. of CSE, IKGPTU, Kapurthala, India[3]

**Abstract.** Cloud services have gradually become part of routine work for individuals and organizations, yet their growing use has also opened several unnoticed weaknesses in access control and account-level security. Existing rule-based systems work reasonably well for predictable situations but often fall short when users behave differently or when an attacker takes advantage of valid credentials. In this work, We propose AURA-X, a conceptual model that observes routine access behavior of cloud users and identifies situations where the pattern appears unusual or risky. The framework brings together ideas from anomaly detection, behavior analysis, ensemble learning, and explainability so that alerts are not only timely but also understandable to administrators. Federated learning is considered in the design to ensure that sensitive information does not need to be centrally collected. The intention of the model is to offer a practical and transparent way to strengthen cloud login and access monitoring without depending on a single vendor or platform.

**Keywords:** Cloud security monitoring, Secure cloud access, Intrusion detection, AURA-X (Access Usage Risk Analyzer with eXplainability), Artificial Intelligence, Ensemble learning, Federated learning.

## 1 Introduction

In today's world, cloud computing makes its existence everywhere from personal computers to mobile. Some popular applications of cloud company are google drive, dropbox, google photos, Onedrive and many more [1]. Cloud computing provides scalability, agility, and affordability, making it the preferred choice for governments, corporations, and citizens worldwide through IaaS, SaaS, and hybrid models. However, these benefits come with drawbacks including privilege abuse, credential theft, and illegal access.

In 2024, organizations worldwide reported a terrifying rise in the cloud-specific threats. According to Cisco's Cybersecurity Readiness Index and other global threat intelligence reports:

- 37% faced credential stuffing attacks — Cisco Report, 2024 [2,3]

IICTDS 2025, December 19-20, Chandigarh, India
Copyright © 2026 EAI
DOI 10.4108/eai.19-12-2025.2362667

- 35% were hit by ransomware — Cisco Report, 2024 [2,4]
- 32 % social engineering - Cisco Report, 2024 [2]
- 32% suffered from supply chain attacks — Cisco Report, 2024 [2]
- 27% encountered cryptojacking — Cisco Report, 2024 [2,5]
- 11% expect AI-driven threats — Cisco Report, 2024 [2]
- 70% of breaches due to misconfigurations or human error -Infosecurity Magazine/CheckPoint, 2024 [6,11]
- 60% involved privileged account exploits — Cisco Talos, 2024 [7,10]
- 31% affected by phishing — Verizon Enterprise, 2024 [8]
- 15% involved zero-day vulnerabilities - Verizon Enterprise, 2024 [8]
- 25% from API exploitation — Gartner/Exabeam, 2024 [9]

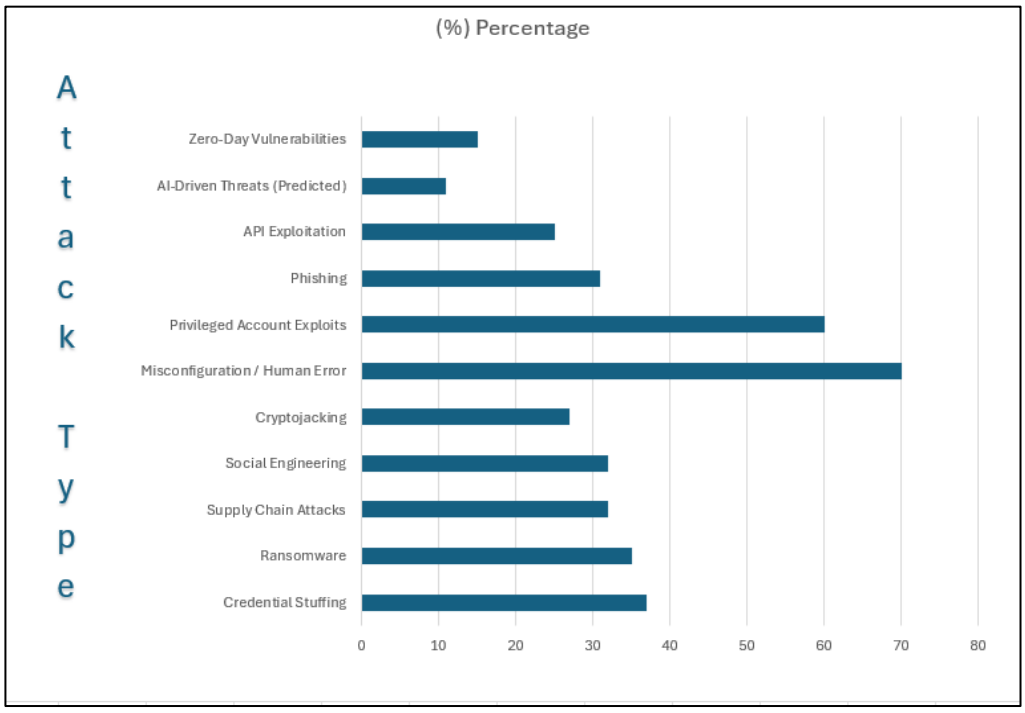



**Fig. 1.** Common Cloud Server Attack Vectors and Their Prevalence in 2024.

## 2 Literature Review

Several research efforts have been carried out in AI-driven cloud access security and a few notable contributions are summarized below:

Recent advancements in cloud-based intrusion detection increasingly focused on multi-stage, intelligent frameworks that combine anomaly detection, ensemble classification and explainability. Seth et al. (2021) proposed a novel ensemble-based intrusion detection system that integrates multiple machine learning classifiers to enhance detection accuracy and reduce false positives [12]. Their model validated on benchmark datasets, demonstrated over 98% accuracy, reinforcing the effectiveness of ensemble learning in classifying flagged sessions.

Sarhan, Layeghy and Portmann (2021) examined how well machine-learning-based intrusion detection systems hold up when applied across different network settings, with particular attention to how model decisions can be interpreted [13]. Their work showed that the choice of features plays a major role in model behaviour, and they used SHAP explanations to make the reasoning behind individual predictions more transparent.

Building on the need for interpretability, Mane and Rao (2021) explored a combination of explanation techniques—including SHAP, LIME and contrastive methods—within a deep-learning intrusion detection framework [14]. The findings in their research confirmed that it is possible to keep detection performance high when providing analysts with clear and interpretable reasons behind suspicious-traffic classifications.

A comprehensive analysis performed in article published in IEEE Communications Surveys & Tutorials 2023, which reviewed explainable intrusion detection in cloud and IoT environment [15]. Here, survey discussed ongoing challenges and highlighted emerging strategies intended to improve transparency, trust and the overall responsiveness of modern cybersecurity systems.

## 3 Challenges in Cloud Access Security

A. Lack of Real-time detection

Most conventional cloud security tools tend to raise alerts only after an attack has already begun. In many cases, by the time malware executes or an intruder gains access to sensitive data, the system issues its warning. Such delayed detection becomes a serious limitation in cloud environments for several reasons:

- Automatic processes: In the cloud, servers and apps start and stop automatically. Before a security alert is triggered, the attacker may have already deleted all traces or moved into other areas of the system.
- Hacking speed: Cyberattacks today happen extremely fast. Hackers use automated tools like ransomware, which can lock and encrypt all your cloud files in just a few minutes, or crypto jacking malware, which silently hijacks your cloud servers to mine cryptocurrency within seconds.
- Missed early warning signals: If systems don't keep an eye on activity all the time and in real time, they miss the chance to stop a threat before it does a lot of damage.

B. Context blindness

Many older or legacy cloud security solutions, often deployed through "lift-and-shift" approaches which lack the contextual intelligence required for effective, adaptive threat detection and protection:

- User context: Systems may not analyze factors such as user role, geolocation, device type, or usual working hours. For example, an employee logging in at 3 a.m. from an unknown IP or device is treated the same as a regular access.
- Behavior tracking: It is easy to see whether anything is wrong when we know what someone usually does. For example, if a user usually opens reporting tools but suddenly tries to access secure files like source code, that unusual behavior can be flagged as a possible threat.
- Zero trust security: In the cloud, security needs to be flexible and smart. Instead of using fixed rules, the system should constantly check things like who the users are, what they are doing and where they are coming from. This helps to protect systems better than using one-size-fits-all rules.

C. Insider threats

Insider threats are serious issue in the cloud because people inside the company already have access to the resources of the system. They might make mistakenly or misuse their access that can putting systems in danger. This happens because:

- People have access to many things: One account may reach servers, databases and apps. If hacked, attackers can do a lot of damage to the system.
- Hidden tools used by staff: Employees sometimes install their own apps or cloud services without approval of company. Since IT team doesn't know about these activities so nobody checks them for risks.
- Infected personal devices: Someone's phone or laptop may have malware or virus. When they log in, attackers use their login details to get inside.
- Attackers using normal tools: Hackers can use built-in cloud features to steal data quietly without alerting security system.

D. Data imbalance

Cloud systems run tons of normal tasks every day including users logging in, files moving around, API requests and background jobs. Actual attacks are very rare in comparison, which makes things difficult:

- Security tools may get busy in normal activity and missed the real attacks.
- Machine-learning models trained mostly on safe data may not recognise the unusual or dangerous events.
- Analysts may get too many alerts that can accidentally ignore real threats.
- To handle this, we need better anomaly-detection methods, semi-supervised learning, generating fake attack samples, and smarter alert prioritizing.

Traditional security system such as fixed rules and signature checks—often fails because attackers know how these tools work and escape triggering them. New approaches like Cloud Shield and RADS offer real-time detection of threats such as crypto mining, DDoS and zero-day exploits, and they provide faster and more accurate results [16]. As threats

evolve, AI- and ML-driven methods are increasingly essential for modelling behavioural baselines and generating dynamic risk scores that respond to changing attack patterns [17].

## 4 Proposed Methodology

The proposed methodology AURA-X (Access Usage Risk Analyzer with eXplainability) is an AI-powered framework designed to monitor, analyse, and secure user access patterns in cloud computing environment. Instead of relying only on static rules or role-based permissions, AURA-X uses machine learning to understand what "normal" access looks like for each user and quickly detect when something unusual or risky access happens:

Components of AURA-X:

- Anomaly detection: AURA-X learns directly from cloud access logs using unsupervised learning without requirement of labeled data. It studies how each user normally behaves as when and where they log in or what devices they use. If the system notices unusual activity that does not match a user's normal pattern, it raises a flag. These unusual activities might point to unauthorized access, stolen passwords or insider misuse.
- Federated learning: Normally, security systems collect all user data in one place for training, which can create privacy risks. AURA-X avoids this by using federated learning. This means the model is trained locally on each cloud node or user device and only the learned patterns are shared. Sensitive personal data never leaves the user's environment but the system still benefits from collective learning across many users.
- Context-aware risk scoring: Every user access request is checked against its context: Who is the user? Where are they logging in from? Which device and time of day? What kind of resources are they trying to reach? Using these factors, AURA-X calculates a real-time risk score. If the score is high, the system can send an alert or block the login attempt before damage occurs.
- Adaptive response mechanism: Based on the risk score, AURA-X can automatically respond in different ways:
    - Enforcing multi-factor authentication
    - Temporarily suspending sessions
    - Notifying security teams for manual review
- Ensemble learning for high accuracy: Instead of depending on just one algorithm, AURA-X combines the strengths of several models such as Isolation Forest, Autoencoders, and LSTM networks. This machine learning approach increases accuracy, reduces false alarms and ensures detection of even sensitive or complex threats.

In AURA-X, it first collects cloud access logs (login time, device details, and activity patterns). It analyses these logs to detect unusual behavior using anomaly detection. Suspicious sessions are then classified by machine learning models as safe or malicious. If malicious behavior is found, the system can block access, ask for extra verification or notify the security team. At the same time, AURA-X explains why the action was taken. For example, login blocked because the

device was unknown and access came from an unusual location. The following algorithm explains how AURA-X analyzes and secures cloud access:

Algorithm 1: AURA-X (Access Usage Risk Analyzer with eXplainability)

1. Initialize log data sources:
   cloud_logs ← fetch_logs_from_all_available_sources()
2. Preprocessing and feature extraction:
   For each log_entry ∈ cloud_logs:
      Extract key behavioral features:
       - Device type / OS / browser
       - Geolocation
       - Session duration
                - IP address
                - Timestamp
          - MAC address
          - Frequency and pattern of usage
3. Build feature matrix:
   F ← construct_session_matrix(log_entries)
4. Anomaly detection:
   anomalous_sessions ← detect_anomalies(F)
   // Using unsupervised anomaly detection techniques
   If anomalous_sessions ≠ ∅ then:
      Optionally:
         additional_anomalies ← apply_alternative_unsupervised_methods(F)
         anomalous_sessions ← anomalous_sessions ∪ additional_anomalies
5. Risk classification:
   For each session s ∈ anomalous_sessions:
      Determine risk label ← classify_using_ml_model(s)
      Store (session, label) in classified_sessions
6. Explainable analysis:
   For each (session, label) ∈ classified_sessions:
      explanation ← generate_explanation(session, label)
       – Local explanation: why this session was flagged
       – Global explanation: overall model reasoning
      Append (session, label, explanation) to audit_log
7. Security response mechanism:
   For each (session, label) where label = “malicious”:
      Execute:
         - Request additional authentication

- Apply temporary access restrictions or session suspension
- Raise an alert for the security team, including why the session was flagged
- Create an incident report for IT team that meets compliance requirements

8. End

Benefits of the AURA-X framework

- Detects suspicious activity even when valid credentials have been compromised by analysing behavioural patterns rather than relying solely on passwords.
- Improves confidence in automated decisions by incorporating Explainable AI (XAI), allowing administrators to understand why certain actions are flagged
- Helps stop attackers from moving deeper into the system or extracting sensitive information through timely, real-time monitoring.
- Facilitates deployments that prioritise both security and user privacy across public and private cloud environments.
- Supports the secure functioning of government cloud platforms, including those operated by NIC and MeitY.
- Enhance protection to data and privacy for sectors like healthcare, energy, banking and other critical infrastructure.

## 5 Conclusion

In our study, we developed AURA-X, a conceptual model that analyzes user behavior to make cloud environment secure for user access and easier to maintain the system security. It can be trained using machine learning and ensemble learning models using data stored in cloud logs which holds user's login information. We can detect unauthorized access or unusual actions, without depending on any cloud providers. By considering login patterns, API calls and user sessions, it can catch strange behavior early and reduce the chance of someone getting into the system without permission. Model uses multiple decision methods together, which makes it more reliable and reduces unwanted alerts. AURA-X also supports trustworthy cybersecurity practices which have main motives to protect privacy and security of user data. For now, it is just a conceptual model which have complete algorithm but the system will be tested in real cloud environments, expanded with federated learning, and test on bigger datasets to see how well it performs, protects privacy and maintains security in cloud computing environment.

## References


[1] Alshuwaier, F.A.; Alshwaier, A.A.; Areshey, A.M.: Applications of cloud computing in education. IEEE. pp. 1–6 (2012)

[2] Cisco Systems: Cybersecurity Readiness Index 2024: Navigating the Threat Landscape. Cisco (2024). Available at [Link]

[3] Longstreet, A.: The State of Identity Security for 2024: Identity-Based Threats, Breaches, & Security Best Practices. BeyondTrust (2024). Available at [Link]

[4] Cisco Talos Intelligence Group: 2024 Year in Review. Cisco Talos (2024). Available at [Link]

[5] Schneider, J., Smalley, I.: What is Cryptojacking? IBM Think (2024). Available at [Link]

[6] Coker, J.: Human Error Contributed to 95% of Data Breaches in 2024. Infosecurity Magazine (2025). Available at [Link]

[7] Cisco Talos Intelligence Group: 2024 Year in Review: Threat Intelligence Report. Cisco Talos (2024). Available at: [link]

[8] Verizon Enterprise: 2024 Data Breach Investigations Report (DBIR). Verizon (2024). Available at [Link]

[9] Schwake, E.: A Salt Security Perspective on the 2024 Gartner Market Guide for API Protection. Salt Security (2024). Available at [Link]

[10] Longstreet, A.: The State of Identity Security for 2024: Identity-Based Threats, Breaches, & Security Best Practices. BeyondTrust (2024). Available at [Link]

[11] Exabeam: 61 Cloud Security Statistics You Must Know in 2025. Exabeam (2025). Available at [Link]

[12] Seth, S., Chahal, K.K., Singh, G.: A Novel Ensemble Framework for an Intelligent Intrusion Detection System. IEEE Access. pp. 128566–128580 (2021)

[13] Sarhan, M., Layeghy, S., Portmann, M.: Evaluating Standard Feature Sets Towards Increased Generalisability and Explainability of ML-Based Network Intrusion Detection. IEEE Transactions on Network and Service Management. pp. 1542–1556 (2021)

[14] Mane, S., Rao, D.: Explaining Network Intrusion Detection System Using Explainable AI Framework. arXiv (2021). Available at: [Link]

[15] Alyami, H.H., Ferrag, M.A., Ahmim, A., Maglaras, M.: Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions. IEEE Communications Surveys & Tutorials. pp. 1343–1376 (2023)

[16] He, Z., Lee, R.B.: CloudShield: Real-Time Anomaly Detection in the Cloud. arXiv (2021). Available at: [Link]

[17] Sanagana, D.P.R.: Preventing Insider Threats in Cloud Environments: Anomaly Detection and Behavioral Analysis Approaches. Science, Technology & Human Values. pp. 225–232 (2023). Available at: [Link]