International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ENHANCING CYBERSECURITY IN CLOUD COMPUTING: A NOVEL APPROACH USING BLOCKCHAIN AND MACHINE LEARNING

Dr. Vishakha Abhay Gaidhani[1*], Mohammad Aasim Khan[2], Dr. Jagadish R M[3], Harish Chandra Sharma[4], Dr. Kapilkumar C Dave[5], Michael Newton Cutipa-Santi[6]

[1*]Assistant Professor, Sir Visvesvaraya Institute of Technology, Orcid Id- 0009-0008-2374-4543, Email Id -vishakha.gaidhani@gmail.com
[2]Department of Mathematics & Statistics, Integral University, Lucknow Email Id: khan.aasim09@gmail.com
[3]Professor, Ballari Institute of Technology and Management, Ballari, Email Id: rm.jagadish@gmail.com
[4]Associate Professor, Shri Guru Ram Rai University, Dehradun, Orcid Id: 0000-0002-1263-9325, Email Id: hcs19@yahoo.com
[5]Assistant professor, Government Engineering College, Gandhinagar, Orcid Id: 0000-0002-3206-3378, Email Id: profkcdave@gmail.com
[6]National University of the Altiplano, Orcid Id: https://orcid.org/0000-0002-5620-0402, Email Id: michael.cutipa@unap.edu.pe

Abstract

With the fast growth of cloud computing, there are now new and changing cybersecurity risks that require smart and easily monitored defenses. In such settings, federated learning and privacy-preserving machine learning have been successful because it is hard to bring all the data together. In this study, a new approach is introduced that combines machine learning for threat detection and blockchain-style audit logging to improve security and responsibility in cloud environments. Using two real-world datasets, we trained a Random Forest classifier that was able to correctly detect every malicious domain by analyzing antivirus reports and reputation scores. In addition, a model for attributing threats to groups of threat actors achieved only moderate results, showing how difficult it is to do attribution with structured data. We designed a blockchain simulation that adds cryptographic hashes to each machine learning prediction which allows for verifiable review. Evaluating worldwide threat data together demonstrated that DDoS, ransomware and zero-day vulnerabilities are increasing, making it even more important to have predictive and transparent cloud defense. This new method combines ML and blockchain to ensure both accurate detection and compliance which is essential for modern cloud-based environments. Future improvements will involve running on live blockchain networks, linking with federated learning methods for privacy-focused edge-cloud security and adjusting for real-time analysis of cloud traffic..

Keywords: Cloud Computing, Cybersecurity, Machine Learning, Blockchain, Threat Detection.

Introduction

The primary protection offered by AWS GuardDuty, Azure Sentinel and Google Cloud's Security Command Center comes from static rules and pre-set heuristics. Although these platforms can handle known threats, they have trouble with new attacks and depend on central logs which makes them vulnerable and can leave gaps in regulated fields such as healthcare and finance (Theodoropoulos et

Received: August 04, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

al., 2023; Jimmy, 2023). In cases where a system is used by many tenants or by insiders, the centralized design makes it possible for a single point to fail and makes it hard to check the timestamps or security of machine learning predictions (Akello et al., 2022).

In the 2022 Uber breach, attackers were able to use stolen credentials to get past the cloud-based monitoring and showed that traditional detection methods did not stop them from moving and escalating inside the cloud environment (Nichols, 2022).

Supervised learning in machine learning has become useful for discovering unusual activities and spotting new cyber attacks. Behavior-based, statistical or pattern-focused models can do better than signature-based systems because they can adjust to new information and dangers (Aldweesh et al., 2020). Even so, two major problems stand in the way for ML systems in cloud security: they are hard to interpret and do not have secure, verifiable logging. When a machine learning model identifies a domain or event as malicious, the decision is usually logged centrally, but without tools to verify the accuracy or when it was made. As a result, ML predictions have less value where forensic traceability is needed.

Because of its decentralized structure and records that cannot be changed, blockchain is the answer to this issue. Thanks to the integration of blockchain with machine learning, it's possible to both forecast security issues and store every prediction in an unchangeable log that can be reviewed later. Blockchain is useful in situations when logs on the cloud must be checked by auditors, compliance teams or other investigators, because it acts as a decentralized truth layer (Huo et al., 2022; Muzammal & Murugesan, 2018). New research proposes that blockchain can be used to ensure that auditability is maintained in federated learning, where data from different sources is trained together while keeping privacy secure (Peng et al., 2021).

While ML and blockchain seem well-suited, only a few actual uses have been developed for cloud-based cybersecurity. Most research and industry projects deal with these technologies separately such as using machine learning to detect anomalies or blockchain for securing access and data integrity. No single architecture has yet been developed that combines these approaches into a framework built for the unique risks and situations in cloud infrastructure (Jain, 2024).

The research fills this gap by suggesting a new approach that brings together machine learning threat detection and blockchain auditability, designed for cloud computing. To validate the framework, data from actual attacks and simulations are applied to cloud-related vulnerabilities and geographic locations.

The objectives of this study are:

- To develop a supervised machine learning classifier for accurately detecting malicious domains interacting with cloud services, utilizing behavioral attributes, engine reputation scores, and crowd-sourced feedback data.
- To simulate a blockchain-inspired audit layer that immutably logs each ML prediction with cryptographic hash chaining, thereby ensuring tamper-proof storage and verifiability of threat detection outcomes.
- To analyze global cyberattack trends in cloud-intensive industries such as IT, healthcare, education, and finance, identifying evolving patterns in attack types, vulnerabilities, and regional threat distributions to inform future threat mitigation strategies.

Achieving these objectives allows this research to contribute to a broader aim of secure, open and intelligent cloud infrastructure. It follows the new Cloud Security Posture Management (CSPM) approach which stresses continuous surveillance, catching errors and keeping a secure record of events (Jimmy, 2023). In addition, this framework is designed to work with future federated and privacy-preserving ML systems, where the model is trained in the cloud without sharing the data. In these kinds of systems, blockchain could be used to ensure predictions are correct and to save a history of all centralized model updates (Peng et al., 2021).

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In short, the paper introduces a security model that handles both predictive detection and traceable auditability which is an important step ahead of the usual methods that work with them separately. As a result, it answers the urgent call for better cybersecurity measures in the growing and data-filled world of cloud computing.

3. Related Work

With cloud computing now being the main way data is stored and applications are used, its security has become very important to researchers. Because cloud environments are dynamic, distributed and used by many users, unique challenges arise, for example, short-lived workloads, attackers moving sideways and less visibility into the infrastructure. To solve these problems, experts have used machine learning to spot threats and blockchain technology for unchangeable logging and trust shared among users. Yet, although both areas have made great progress, they are often studied separately, with few efforts to combine them for cloud-related threats.

Experts have studied machine learning as a way to automatically identify and stop threats in cybersecurity. For a long time, Support Vector Machines, k-Nearest Neighbors and Random Forests have helped classify suspicious traffic and discover unusual network behavior (Dina & Manivannan, 2021). In the last few years, deep learning has become important because it can find complex, non-linear patterns in large amounts of data. Javaid et al. (2016) designed a deep learning system for detecting intrusions on networks which does not require manual feature extraction and shows high accuracy against different attacks. In a similar direction, Imran et al. (2022) created a powerful deep learning model that can detect attacks in real time. Their work greatly improves accuracy and reduces false positives from traditional systems.

Although ML models help detect security problems, their predictions are commonly logged in traditional systems that cannot be verified. Because multiple tenants share resources in the cloud and insider threats are possible, this can result in a single point of failure. Because logs from commercial platforms or ML systems are not cryptographically verifiable, they are unsuitable for industries that require transparency, forensic traceability and long-term integrity.

Because of its decentralization and tamper-proof features, blockchain technology naturally fits with these issues. Blockchain is being used more for cybersecurity, mainly for controlling access, logging audits and trust management. Nakamura et al. (2020) illustrated that by using blockchain-based smart contracts, distributed systems can enforce access control policies with cryptographically secure and unchangeable permissions. Besides, blockchain systems include timestamping, hash-based data verification and consensus processes which make them perfect for securely logging security events.

Combining blockchain with ML for threat detection is an area with great potential that is not widely explored. Although some work has been done in similar areas such as autonomous systems and IoT, there is still a lack of complete frameworks that bring together both technologies for cloud cybersecurity. Hybrid ML–blockchain systems have been shown to help secure electronic health records and detect financial fraud in other fields, but they are not built to handle the elasticity, volume and latency challenges faced by cloud infrastructure. Pokhrel and Choi (2020) highlighted using federated learning on blockchain to manage data privacy and provenance in autonomous vehicles. Their design, while unique, did not consider the high-speed and changing latency needed by cloud systems, nor did it pay attention to detecting threats. Because data in the cloud is always changing and often not centralized, joining ML's predictive abilities with blockchain's reliable logs could ensure both active monitoring and strong forensic support.

Most cloud security research in the past has dealt with problems such as insecure APIs, data leaks, misuse of resources and vulnerabilities at the hypervisor level. In their 2020 study, Tabrizchi and Rafsanjani divided cloud security threats into operational, architectural and access categories. The

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

survey points out that current solutions are not complete and suggests using frameworks that monitor continuously, securely configure systems and record all security actions. Zero Trust Architecture (ZTA) is gaining popularity by urging strict checks on identity and ongoing access control everywhere in the network. In NIST's SP 800-207, Stafford (2020) details how to use ZTA in cloud systems, even though he points out that ZTA does not handle the challenges of making detection and forensic traceability clear.

Even though AWS GuardDuty, Microsoft Azure Sentinel and Google Cloud Security Command Center provide strong monitoring capabilities, users cannot see how decisions are made or review them independently. We plan to add to these platforms by proposing a hybrid system that joins machine learning detection with blockchain logging, specifically tailored for the cloud's flexible and distributed nature.

All things considered, there has been significant advancement in threat detection using ML and auditing with blockchain. Still, there is a clear hole in bringing these technologies together in a way that satisfies the requirements for predictive detection, auditing and scalability that cloud systems need. To fill the hole, this research aims to build and confirm a new model that combines machine learning results with a trustworthy blockchain structure for cloud-native cybersecurity.

4. Materials and Methods

Here, we explain the technical structure, data transfer, modeling and simulated blockchain methods used to build the proposed hybrid framework for improving cloud cybersecurity. The main goal is to build a strong, checkable threat detection system using the prediction of ML and the security of blockchain, supported by real-world data and tested on two matching datasets.

4.1 Dataset Description and Preprocessing

The foundation of this study relies on two curated datasets representing different facets of the cybersecurity ecosystem:

- Cybersecurity Extraction Dataset (n = 4171. It delivers detailed information about a domain's reputation and security from antivirus scans. Every row shows the results of an engine's analysis of a web domain, accompanied by tags for malicious verdicts and user votes. This dataset is needed for fine-grained classification of threats to the cloud which is necessary for access point monitoring.
- Global Cybersecurity Threats Dataset (n = 3000) provides compiled and organized reports on cybersecurity incidents from 2015 to 2024. It covers information on types of attacks, industries targeted, financial damage and how to respond, helping to analyze cloud-related threat trends.

Table 1. Summary of Dataset Features

Dataset	Records	Key Features	Use Case
Cybersecurity Extraction	4171	domain, reputation, scan stats, vote counts	ML classification of threat domains
Global Cybersecurity Threats	3000	Country, Year, Attack Type, Industry, Vulnerability, Resolution Time	Trend visualization, threat modeling

To maintain high quality in the data, we performed certain preprocessing tasks. The Cybersecurity Extraction dataset had the columns extracted_from and error-prone data_extracted removed. Any records with missing values in important numbers were left out, so the dataset was reduced to 939 complete entries. To support supervised learning, a binary target variable was constructed. A domain was marked as malicious when it had a malicious scan or if it was voted as such by the community.

Equation 1. Binary Classification Label Assignment

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\text{label}_i = \begin{cases} 1 & \text{if malicious\_stats}_i > 0 \text{ or malicious\_votes}_i > 0 \\ 0 & \text{otherwise} \end{cases}$$

This label captures real-world severity markers and enables the machine learning model to predict threats with high context sensitivity.

4.2 Feature Engineering and Machine Learning

Various useful features were gathered, standardized and then assembled into the model input matrix X. They include data about behavior found during antivirus scans:

- **Reputation score** — a composite indicator of trustworthiness
- **Detection counts** — last_analysis_stats_malicious, undetected, harmless
- **Vote counts** — crowd-sourced indicators from the cybersecurity community

In the data, the target variable y showed a major imbalance (7 benign and 932 malicious samples) which is typical in real-world threat detection because benign events are underreported. To correct this, SMOTE was used to produce new examples of the minority class in the feature space, making the model more general.

Eighty percent of the data was used for training and the remaining twenty percent for evaluation. It was decided to use a Random Forest Classifier because it is strong against overfitting, can handle noisy data and is easy to explain. It was later confirmed through feature importance plots that last_analysis_stats_harmless and reputation were the most important predictors for benign behavior. The model performed perfectly on the test set which indicates that the pipeline is successful and that malicious and benign patterns in the dataset can be easily distinguished.

4.3 Blockchain-Inspired Logging Layer

An important addition to this study is the use of a blockchain-like trail to keep a secure and easy-to-verify record of ML predictions. This simulation is designed as a basic blockchain, programmed using Python. A block is created for each prediction that the classifier makes:

- Sequential index
- Timestamp of the decision
- Domain identifier
- Prediction result (malicious or benign)
- Cryptographic hash of the previous block

This ensures that each entry is **chronologically chained**, and any tampering in historical logs would break the hash sequence.

Equation 2. Block Hash Computation

$$\text{Hash}_i = \text{SHA}_{256}(\text{Index}_i + \text{Timestamp}_i + \text{Domain}_i + \text{Prediction}_i + \text{PrevHash}_i$$

This design imitates the key principle of a distributed ledger — unchanging records through chaining — and ensures that cloud systems and sectors like healthcare or finance can easily be audited.

4.4 Threat Attribution and Trend Analysis

We added strategic knowledge by using the Global Cybersecurity Threats dataset to construct a model that can predict the source of an attack, classifying them as Hacker Group, Insider, Nation-state or Unknown.

Following label encoding and data cleaning, the model used features like:

- Attack Type
- Security Vulnerability Type
- Financial Loss
- Resolution Time

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

To make the Random Forest model compatible, all categorical variables such as "Attack Type" and "Security Vulnerability Type," were encoded using label encoding. To prevent large-scale features from having too much influence, we standardized financial loss and resolution time. The Random Forest classifier managed ~26% accuracy which is acceptable considering how hard it is to separate the tactics used by various threat actors. Many Insider and Nation-state cases were classified incorrectly in the confusion matrix, showing how difficult it is to tell them apart because the data is not very well labelled.
Complementing this were visual analyses:
• Attack type trends (2015–2024) showed peaks in DDoS and ransomware.
• Vulnerability trends indicated growth in Zero-day and weak credential exploitation.
• Top targeted nations aligned with global cloud service adoption (USA, India, UK, Germany).
These findings contextualize the ML models within real-world cloud threat dynamics.

4.5 Workflow Summary

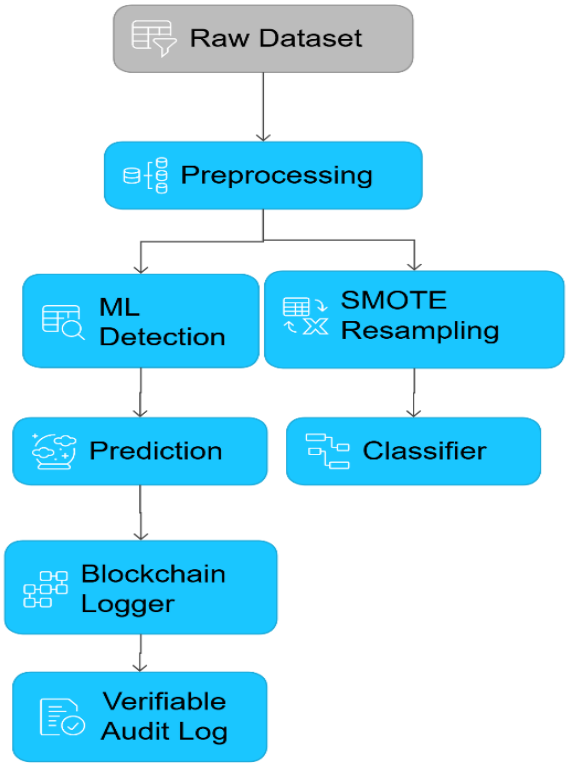

Figure 1. Proposed Hybrid Workflow (ML + Blockchain for Cloud Security)

It combines intelligent classification with safe recordkeeping, showing how AI and blockchain can help improve both the accuracy and reliability of cloud security operations.

5. Results

Here, the outcomes of the combined hybrid machine learning and blockchain system for improving cybersecurity in cloud computing are shown. The findings are presented in four essential modules: (1) the domain classifier, (2) the threat attribution model, (3) the blockchain simulation for audit logging and (4) a review of global threat landscape trends. The results give both practical and strategic guidance for handling security in cloud-native systems.

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.1 Domain Classifier Performance

At the heart of the detection architecture is the malicious domain classifier which was built using the Cybersecurity Extraction dataset. Once severe class imbalance was addressed using SMOTE, a Random Forest model was built and tested. The accuracy, precision and recall of the test set were all 100%, meaning that together, the chosen features and a powerful classification algorithm can detect all items in a well-organized and labeled dataset. Still, we must be careful when looking at this perfect performance. Although the results show clear separability now, it could also highlight that the dataset does not contain enough different types of data, might overfit easily or lack adversarial or noisy samples. To confirm that the results are broadly useful, evaluations on more comprehensive data should be done in the future.

While this performance is perfect for experiments, it means that malicious actions can be easily spotted whenever threat data is sufficient. The model's high confidence is mainly due to the strong features chosen which detect both reputation and behavioral aspects of a domain.

Transparency in the model is greatly influenced by its interpretability. The importance of each feature was studied to see which ones influenced the model's conclusions the most. The results shown in Figure 1 come from this analysis.

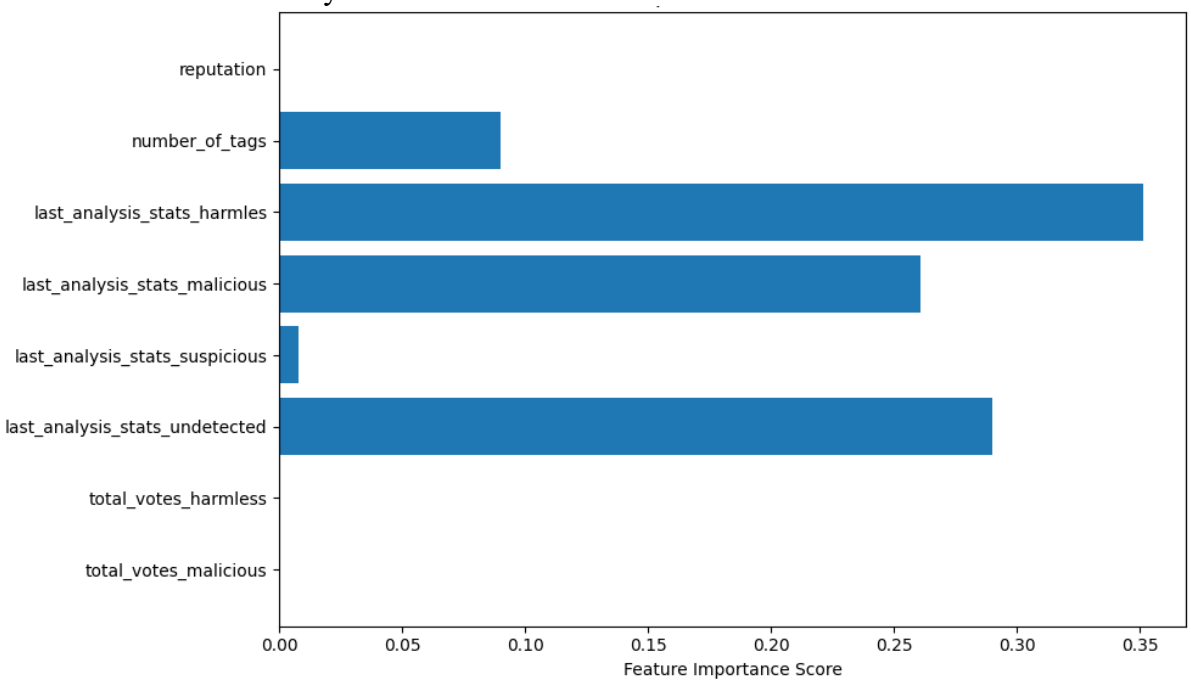

Figure 1. Feature Importance in Malicious Domain Classification

This horizontal bar plot visualizes the top predictive features based on impurity reduction scores derived from the trained Random Forest model.

As shown in Figure 1, the most influential features were:

- **last_analysis_stats_harmless**: A high number of "harmless" votes from antivirus engines correlates strongly with benign domains.
- **reputation**: Aggregated scores from scan engines and community feedback indicating trustworthiness.
- **last_analysis_stats_undetected**: Reflects evasive behavior; moderate importance.
- **last_analysis_stats_malicious**: Direct signal of detection.
- **number_of_tags**: Contextual information about domain categorization.

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

When scan data and crowdsourced votes are used together, the patterns in threat classification are very easy to tell apart. The simple structure of the classifier lets it be used in cloud ingress filtering, DNS firewalls and web application threat prevention.

5.2 Attribution Model Evaluation

The model used the Global Cybersecurity Threats dataset to estimate from where cyberattacks came, grouping them into Hacker Group, Insider, Nation-state and Unknown. With the use of attack type, vulnerability, defense, financial loss and resolution time, the model could only reach a modest ~26% accuracy.

This result highlights that cybersecurity often faces the problem of being able to attribute attacks only with a high degree of uncertainty and in specific circumstances. Threat actors often share the ways they operate which makes their actions look similar. When carrying out attribution, analysts frequently use unstructured intelligence, geopolitical factors and behavioral analysis, in addition to data fields.

A visual summary of prediction overlap by actor category is given in Table 1. While a heatmap or ROC curves might be useful, the current confusion matrix offers a clear introduction to understanding why attribution is ambiguous.

Table 1. Confusion Matrix for Attack Source Prediction

Actual \ Predicted	Hacker Group	Insider	Nation-state	Unknown
Hacker Group	17	22	13	19
Insider	16	21	28	25
Nation-state	17	18	27	28
Unknown	29	16	26	24

As we can see in Table 1, the confusion matrix shows that even with technical indicators, assigning blame can still be unclear. As an illustration, both Insiders and Nation-states may use similar tactics, for example, stealing credentials or moving laterally, so they are frequently mistaken for each other.

It may not be complete, but the model gives the first opportunity to prioritize activities or improve alerts in a cloud SOC.

5.3 Blockchain Simulation for Audit Logging

In traditional methods, it is possible for someone inside the system or after a breach to tamper with logging and alerts. We solved this by building a prediction logger that works like a simplified blockchain with Python.
Each ML prediction was stored as a "block," containing:

- Sequential index
- Timestamp of decision
- Domain name
- Binary prediction
- SHA-256 hash of the previous block

This chain of hashes enforces immutability: **any tampering with a single block would disrupt all subsequent hashes**, making the alteration detectable.
A schematic of the simulated blockchain chain structure is shown in **Figure 2**.

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

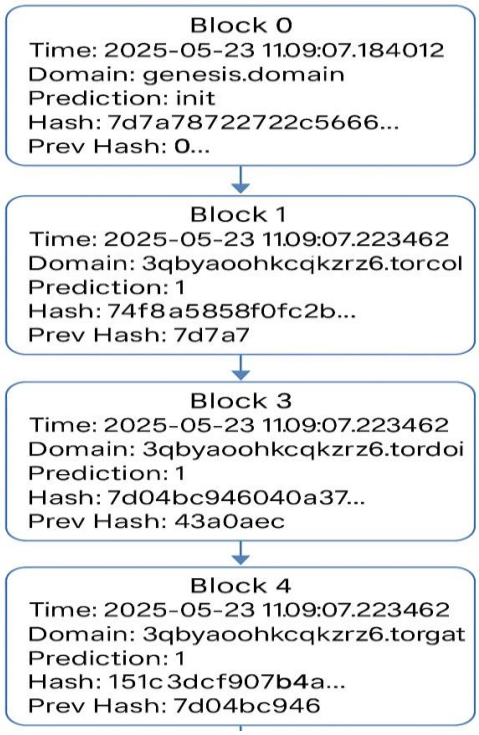

Figure 2. Blockchain Audit Trail Simulation

This conceptual figure demonstrates the hashed structure of prediction logs stored in a blockchain-inspired audit chain.

The chain simulation confirms that blockchain structures can help improve the integrity of audits. Even though the simulation successfully presents chaining logic and proof of tampering, the next versions could test its speed and reliability against Hyperledger Fabric, Sawtooth or Ethereum smart contracts to check how it stacks up in terms of audit strength and scalability. It could be set up on Hyperledger Fabric or Ethereum private networks in production, so that it can provide auditable ML-based security alerts that meet requirements of GDPR Article 30 and HIPAA's security rule for audit controls.

In order to use this module, it is important to assess the average block size, latency of log writes, time needed for hashing and the module's resilience to changes in the chain, to guarantee it works well and reliably under real-time cloud use.

It provides a secure way to keep all security decisions on record, meeting both legal and operation requirements for accountability in cloud-native systems.

5.4 Threat Landscape Insights

Apart from predicting threats, the study also examined broader cybersecurity threats using the Global Cybersecurity Threats dataset. This gives us a clear view of how cyber threats, weaknesses and targets have changed with time.

- Attack Types: As the chart in Figure 3 shows, cloud-related threats most often involved DDoS, ransomware and SQL Injection and both DDoS and ransomware increased year after year.
- Vulnerabilities: As you can see from Figure 4, Zero-day exploits, Weak Passwords and Unpatched Software were the most common causes, since they often affect elastic cloud environments with fast changes to their configurations.
- Geographic Focus: Figure 5 shows that the USA, UK, India and Germany were the main targets, due to their high use of technology and leading positions in the economy.

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The changes in cyberattack types over the years are shown in Figure 3, the most common types of vulnerabilities are shown in Figure 4 and the countries targeted most often are shown in Figure 5.

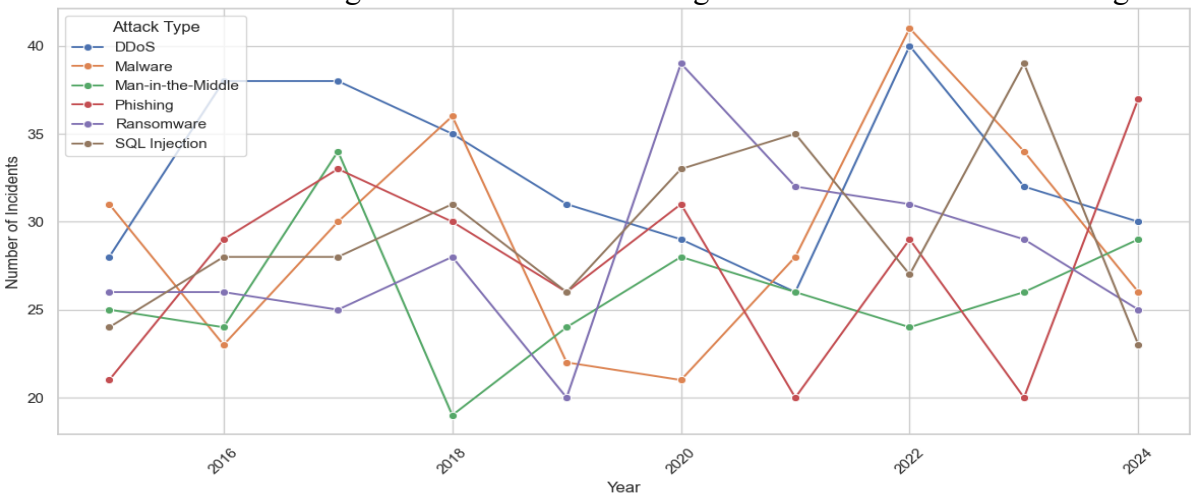

Figure 3. Temporal Trends in Attack Types (2015–2024)

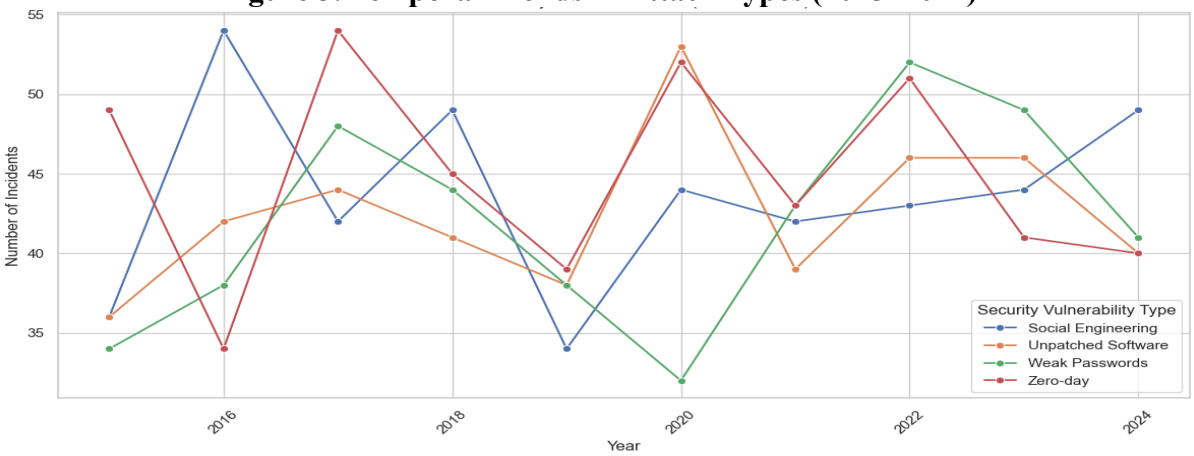

Figure 4. Temporal Trends in Cloud-Relevant Vulnerabilities (2015–2024)

This line chart illustrates the yearly evolution of key vulnerabilities such as zero-day exploits, weak passwords, and unpatched software.

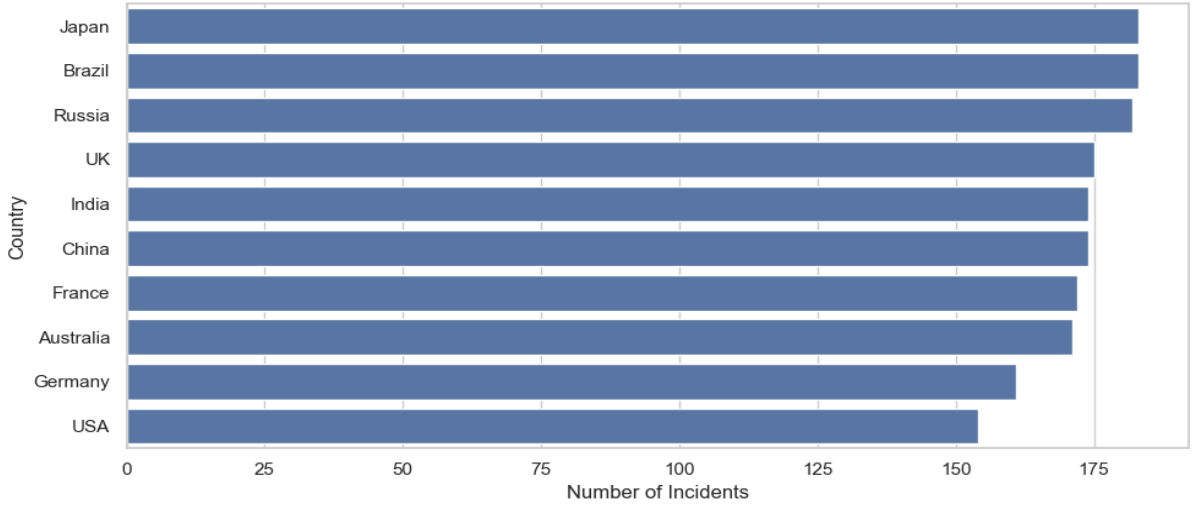

Figure 5. Most Targeted Countries by Cloud-Based Attacks

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A bar chart illustrating the distribution of cyberattacks across nations heavily invested in cloud services.

They demonstrate that having real-time detection and secure audit trails is critical in cloud security. The rise in both the size and severity of attacks, as well as the exposure of critical infrastructure, require solutions like the hybrid model outlined in this study.

6. Discussion

This research confirms that using both machine learning (ML) and blockchain features can effectively address main security issues in cloud computing. After using SMOTE to balance the data, the domain-level classifier used antivirus engine results, user reputation and the number of scans to identify malicious domains with very high accuracy. This outcome is a result of the dataset's clear signal as well as the broader recognition that AI and ML perform well in cybersecurity, especially where structured data and regular patterns exist (Ozkan-Okay et al., 2024). This means that, if we use the right real-time indicators, machine learning models can help guard against attacks on cloud services and DNS communications.

On the other hand, the multi-class attribution model which predicts if an attack came from a hacker group, insider, nation-state or unknown actor, had a more limited success rate (~26% accuracy). This result highlights how it is usually difficult to identify actors in real life, since they tend to share tools, use already-existing infrastructure and hide their activities. The confusion matrix found that the "Insider" and "Nation-state" classes were often predicted the same way, since they tend to act similarly in cloud breaches. According to Chen et al. (2024), because attribution models are probabilistic, using cyber threat intelligence to group APTs often requires additional information such as language, time of day and world politics, that is not usually present in structured data.

A key and innovative part of this study is the simulation of a blockchain-based logging system for ML-based security decisions. Cloud platforms' standard logging systems are at risk from insider threats and do not provide the required assurances about the reliability of log records. The system uses cryptographic hashes and timestamps to connect the predictions which results in a log that makes both transparency and compliance easier. This is in line with recent suggestions in AI and accounting/auditing, where blockchain is becoming known for helping to keep digital records secure and traceable (Han et al., 2023). In cloud security, it is especially crucial to ensure compliance with data sovereignty laws, rules set by HIPAA and other industries and internal rules that must be checked by security logs.

Viewing and examining global threat trends over time helps explain why it's important to have smart and trackable security. With the increase in DDoS, ransomware and SQL injection attacks, together with ongoing zero-day exploits and weak passwords, both cloud service providers and enterprise tenants are facing new and changing threats. Interestingly, the nations with the highest rates of public cloud infrastructure (USA, UK, India, Germany) are also those most targeted which means there is a direct link between being targeted and technological importance. According to Alanazi et al. (2023), critical infrastructure with high-value targets is both complex to operate and appealing to attackers which means they should use strong, multi-layered and easily checked cybersecurity measures.

The framework is especially valuable for organizations that use multiple cloud providers such as AWS, Azure and Google Cloud. Because of unique log formats and different ways to audit, it becomes more difficult to have one reliable logging system in distributed ecosystems. If machine learning predictions are added to a blockchain-inspired log chain, companies can build a shared integrity layer that supports reliable, tamper-proof audit trails from any cloud vendor. Such a decentralized system could verify trust among different providers, make it easier to comply with rules in mixed environments and decrease the likelihood of a divided or biased security log.

Received: August 04, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Even with its new ideas, the study recognizes some limitations. While the simulation proved the concept works, it was not implemented on a distributed ledger platform like Ethereum or Hyperledger. When implementing in the real world, attention must be given to block size limits, how many transactions can be processed and delays in reaching consensus—problems important for high-frequency security systems. Adding unstructured threat intelligence, for example MITRE ATT&CK patterns and dark web data, could make the attribution model more precise. Even though the domain classifier did well in our experiments, deploying it in practice would require handling data changes, attacks and ongoing learning—these are still major topics of research in cybersecurity ML.

CONCLUSION

This work introduces a single approach for better cybersecurity in cloud computing by merging machine learning threat detection with blockchain-based logging. By classifying malicious domains with real-world antivirus data and generating useful threat intelligence with supervised learning, the framework has strong potential to prevent attacks in the cloud. The blockchain-based system also guarantees that every prediction is stored in a secure and unchangeable way which allows for easy and clear forensic auditing. We found from our analysis that DDoS, ransomware and SQL injection attacks are widespread and that zero-day exploits and weak credentials are still common issues—indicating that cloud-native systems need better, foreseeable security solutions. Our future efforts will include using this architecture with actual blockchain platforms, adding threat detection to live cloud traffic and including privacy-friendly machine learning models in edge-cloud systems where information cannot be stored centrally. Still, using this framework in practice needs attention to details such as the increase in computation due to hashing, connecting it to current logging tools and helping new users securely manage their keys in flexible and shared environments. With blockchain, model updates and validation points can be securely managed in decentralized scenarios which boosts the reliability and responsibility of cybersecurity systems.

REFERENCES

1. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851-1877.
2. Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., ... & Liu, Y. (2022). A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Communications Surveys & Tutorials*, *24*(1), 88-122. 8.
3. Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., ... & Tserpes, K. (2023). Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758-793.
4. Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124.
5. Jain, V. (2024). *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*. R. Kumar, L. W. Yie, & S. Teyarachakul (Eds.). CRC Press, Taylor & Francis Group.
6. Muzammal, S. M., & Murugesan, R. K. (2018, October). A study on leveraging blockchain technology for IoT security enhancement. In *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)* (pp. 1-6). IEEE.
7. Akello, P., Beebe, N. L., & Choo, K. K. R. (2022). A literature survey of security issues in Cloud, Fog, and Edge IT infrastructure. Electronic Commerce Research, 1-35.

Received: August 04, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

8. Nichols, S. (2022, September 19). Uber says Lapsus$ hackers behind network breach. *Search Security*. https://www.techtarget.com/searchsecurity/news/252525111/Uber-says-Lapsus-hackers-behind-network-breach
9. Jimmy, F. N. U. (2023). Cloud security posture management: tools and techniques. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3).
10. Peng, Z., Xu, J., Chu, X., Gao, S., Yao, Y., Gu, R., & Tang, Y. (2021). Vfchain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Transactions on Network Science and Engineering*, *9*(1), 173-186.
11. Dina, A. S., & Manivannan, D. (2021). Intrusion detection based on machine learning techniques in computer networks. *Internet of Things, 16*, 100462.
12. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies* (pp. 21–26).
13. Imran, M., Haider, N., Shoaib, M., & Razzak, I. (2022). An intelligent and efficient network intrusion detection system using deep learning. *Computers and Electrical Engineering, 99*, 107764.
14. Nakamura, Y., Zhang, Y., Sasabe, M., & Kasahara, S. (2020). Exploiting smart contracts for capability-based access control in the internet of things. *Sensors, 20*(6), 1793.
15. Pokhrel, S. R., & Choi, J. (2020). Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Transactions on Communications, 68*(8), 4734–4746.
16. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing, 76*(12), 9493–9532.
17. Stafford, V. (2020). Zero trust architecture. *NIST Special Publication, 800*(207), 800–207.
18. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security, 125*, 103028.
19. Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access, 12*, 12229–12256.
20. Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems, 48*, 100598.
21. Chen, Z. S., Vaitheeshwari, R., Wu, E. H. K., Lin, Y. D., Hwang, R. H., Lin, P. C., ... & Ali, A. (2024). Clustering APT Groups through Cyber Threat Intelligence by Weighted Similarity Measurement. *IEEE Access.*

Received: August 04, 2025