

Survey on Cryptojacking Detection and Prevention in Cloud Systems

Dr. Pradeep Laxkar

Associate Professor

Department of Computer Science and Engineering

ITM(SLS) University, Vadodara, Gujarat

pradeep.laxkar@gmail.com

Corresponding Author: * Pradeep Laxkar (pradeep.laxkar@gmail.com)

Received: 18 August 2026 | Revised: 22 August 2026 | Accepted: 25 August 2026

Abstract—Cryptojacking is one of the major threats that has come about in the area of cloud computing, and it refers to the secret mining of cryptocurrency through the use of an exploitation of computing resources. The said hacking method combines existing web and host methods, thus utilizing JavaScript, WASM, advertising, phishing, rootkits, and process obfuscation for avoiding detection. As such, AWS EC2, Azure VMs, Kubernetes, and Docker are some of the popular cloud platforms that are heavily targeted by this threat. Defending tactics currently employed heavily rely on behavioral scrutiny, anomaly detection, monitoring of network traffic, and also the employment of ML algorithms such as deep learning, reinforcement learning, and adversarial autoencoders. Unfortunately, issues with scalability, false alarm reduction, real-time monitoring, and threat response at an adaptive level persist among these solutions' privacy-preserving learning over distributed data, multi-modal input data, as well as cloud-native SIEM & DevSecOps integration to support the security teams in being proactive rather than reactive. IAM, encryption and key management, and threat detection with Active Responder APIs are the indispensable building blocks for IaaS, PaaS, and SaaS model security. A smart, interpretable, as well as automated defense framework is the weapon of multi-cloud and serverless environments in winning the fight against cryptojacking, which keep on evolving.

Keywords—Cryptojacking, cloud security, anomaly detection, machine learning, runtime protection, adaptive defense, reinforcement learning.

I. INTRODUCTION

Cloud computing is one of the major components of Modern Information and Communication Technology (ICT) systems [1]. It facilitates virtualized data storage, processing, and management through web-based services. Being highly scalable, flexible, cost-effective, and simple to use, one of the reasons cloud computing has been embraced so thoroughly by various sectors such as healthcare, finance, education, and government [2][3][4]. Nevertheless, with the growth of cloud infrastructure, the issue of securing data and services has become quite a challenge [5][6]. Data breaches, Distributed Denial of Service (DDoS) attacks, and Advanced Persistent Threats (APTs) are just a few examples of the increasingly

sophisticated cyber threats that illustrate why strong security models for the cloud are essential.

Cryptojacking has become a stealthy and major problem for cloud systems. The term "cryptojacking" refers to the practice of secretly mining cryptocurrencies using another person's computer system, sometimes without their knowledge or permission. Such a malicious act causes the energy consumption to rise, the system efficiency to lower, and the attackers to have the possibility of further intrusions into the victim's network [7]. Cryptojacking typically occurs when users visit websites that contain mining scripts, infected software, compromised browser extensions, or malicious links [8][9]. The attacker takes advantage of the trustworthiness and anonymity of cryptocurrency transactions to execute the malicious code [10][11][12]. Since blockchain technology and cryptocurrency are becoming popular, attackers are more than ever tempted to take advantage of cloud infrastructures.

Traditional security mechanisms like rule-based IDS and payload inspection are frequently unable to effectively counter modern [13][14] Cryptojacking attacks, especially when encryption or disguise is applied to network traffic [15]. While learning-based and behavior-based detection methods provide potential solutions, they still need to overcome practical obstacles, including the presence of unlabeled and highly imbalanced traffic in cloud gateways. As a result, strong detection and prevention measures become indispensable for the protection of cloud environments from Cryptojacking [16]. The relatively low volume of mining traffic requires efficient detection algorithms.

A. Structure of the Paper

The organization of the paper is as follows: Section II describes the operational mechanism of Cryptojacking in a cloud system. Section III describes crypto mining techniques. Section IV presents cloud security solutions and mitigation. Section V presents cloud security and mitigation strategies. Section VI highlights advanced AI- and ML-driven defence models. Section VII summarizes the outline, conclusions, and future directions.

II. OPERATIONAL MECHANISM OF CRYPTOJACKING IN CLOUD SYSTEMS

Cryptojacking is a type of cyberattack in which someone uses someone else's computer to mine Bitcoin without their permission or knowledge. It is different from ransomware or data theft in that it is a silent and permanent attack that aims to stay unnoticed for a long time while it keeps using the CPU, GPU, memory, or cloud resources for cryptojacking. Traces from 12 families were included; features were browser, mining, load, and network-based; SVM achieved 97.9% TPR and 1.1% FPR. Out guard detected 6,302 sites, mostly low-popularity or through ads, classified into 14 families, with 35 campaigns using libraries. Fig 1 shows an overview of cryptojacking, illustrating how websites deliver mining code, victim browsers execute mining tasks, and blocks are added to the blockchain [17][18].

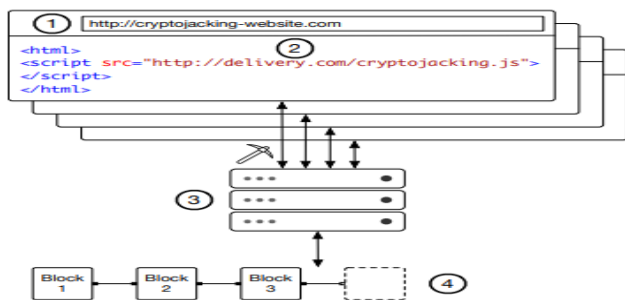


Fig. 1. Cryptojacking overview

A. Nature and Mechanics of Cryptojacking

Cryptojacking is an information technology term that describes the unauthorized appropriation of a computer's resources and processing power to mine cryptocurrencies, thereby exploiting the unwitting proprietor of the device. Cryptojacking constitutes a malicious form of cryptocurrency mining [19]. The overarching purpose of cryptojacking and the theft practices of miners-hackers is to obtain "free computing power" for "cost-free" mining of the so-called fossil cryptocurrencies through the development of a unique mining rig that can process data from foreign devices without the proper authorization.

B. Attack Vectors in Cloud Serverless Platforms

A serverless platform is an ecosystem that is both dynamic and complicated, consisting of many different parts. Considering the security offered by each component and how they interact is essential when designing a secure serverless ecosystem [20]. In most cases, attackers from outside the cloud launch attacks by exploiting fields that users can alter in one of the available APIs for event handling. When an attacker is based inside the cloud and has complete command over a function or functions, they are considered an internal adversary. Attackers in this category can try to build covert channels, escalate privileges, steal or alter sensitive data, learn about infrastructure and runtime environments, or launch a Denial-of-Service attack.

C. Vulnerabilities in Cloud

The three main service models that make up cloud computing are IaaS, PaaS, and SaaS.

- **Infrastructure as a Service (IaaS):** Virtual machines, storage, servers, and networking infrastructure are all part of the basic computing resources that this service model makes available [21].

- **Platform as a Service (PaaS):** Platform as a service (PaaS) offers an ecosystem for creating and managing applications. Applications for end users are provided by the PaaS. Platform as a Service simplifies the development cycle.
- **Software as a Service (SaaS):** There is no longer any need to install software on client computers thanks to software as a service (SaaS). SaaS does provide easy access and quick setup.

D. Web-Based and Host-Based Attacks

Cloud-based Cryptojacking attacks have two main types: web Cryptojacking and host Cryptojacking [22]. Both want to use the computational resources for secret cryptocurrency mining, but their differences are very significant in the execution strategies, stealth mechanisms, and the way they can be detected.

- **Web-based attack:** Internet-based cryptojacking is carried out via evil scripts that are hidden in a site or a browser add-on, and they are launched when a user opens the infected page [23]. The mining program is written for the browser and uses languages like JavaScript and Web Assembly (WASM) so that no local malware has to be installed. Malvertising, phishing emails, hacked websites, and third-party JavaScript libraries are frequently used to spread web-based Cryptojacking [24][25].
- **Host-based attack:** Host-based Cryptojacking is much more aggressive and can go on for a long time without being detected as it works at the level of the operating system. The attackers implant the mining malware right on the physical machine or a virtual one in the cloud. To avoid detection, this malware usually disguises the processes that it uses via process obfuscation, rootkits, and API hooking. Cloud platforms like AWS EC2, Azure Virtual Machines, Kubernetes (K8s) clusters, and Docker containers are often the target of host-based attacks.

III. DETECTING MALICIOUS CRYPTOMINING ACTIVITIES

Detection of crypto mining attacks has been approached through browser-based and host-based analyses, examining traffic patterns, executable files, and dynamic behaviors to identify mining activities. Techniques include monitoring network traffic to detect communication with mining servers, opcode analysis of non-executable files, and passive-active flow monitoring to uncover hidden mining pools. Machine learning models leverage features derived from these network characteristics, enabling accurate identification of compromised devices and mitigation of crypto-mining attacks.

A. Behavioral and Resource-Based Detection Approaches:

The repetitive and consistent nature of crypto-mining behavior creates network traffic with clear trends. There is a high degree of self-similarity since the computational process of mining causes traffic to increase periodically [26]. In contrast to the more erratic patterns seen in typical traffic, the Hurst exponent of mining traffic is typically larger than 0.5. Therefore, behavioral and resource-based detection methods can use traffic statistics, temporal features, and resource utilization metrics as inputs to identify crypto mining activities.

B. Network, Log, and Anomaly-Driven Monitoring Techniques

The software and hardware components that make up NIDSs can function as either standalone devices inside a local administration domain or as an integrated part of RegSOC [27]. Various types of cyber-attacks, both signature-based and non-signature-based, can be detected by this NIDS by monitoring network traffic between ISPs and their customers' network infrastructures. Different from signature-based detection, which uses unique identifiers to identify known threats, behavioral analysis and anomaly detection look for unusual network activity that could be a sign of zero-day attacks or other undiscovered dangers [28]. Machine learning methods are employed to detect anomalies in network traffic, distinguishing between atypical user operations and potential attack symptoms [29]. The anomaly detection module operates autonomously and can integrate with SIEM systems, analyzing traffic in real time or from historical CSV files, with feature vectors extracted from TCP/IP headers aggregated by IP addresses and port pairs.

IV. CLOUD SECURITY SOLUTIONS AND MITIGATION STRATEGIES

A lot of different ideas and actions have been taken to deal with cloud security issues and lower the risks that come with them. Essential security measures include encryption and key management, which prevent unauthorized parties from accessing data while it is in transit or at rest and handle cryptographic keys correctly [30]. By using the principle of least privilege, Identity and Access Management (IAM) systems allow for the necessary management of user identities, roles, and permissions, hence minimizing security risks [31] [32]. Amazon Web Services (AWS) GuardDuty and Microsoft Azure Security Centre are cloud-specific security solutions that monitor cloud environments in real-time to improve threat detection and response capabilities. Furthermore, by integrating threat intelligence, constant monitoring, and log analysis, comprehensive security monitoring systems allow for the prompt detection and resolution of security events. Fig 2 shows the overall design of various mitigation measures and tiered security mechanisms. Regular security assessments, penetration testing, and vulnerability scanning supplement proactive defence strategies, while industry-recognized certifications and standards like FedRAMP, CSA STAR, and ISO 27001 offer frameworks for evaluating and assuring the security capabilities of cloud service providers.

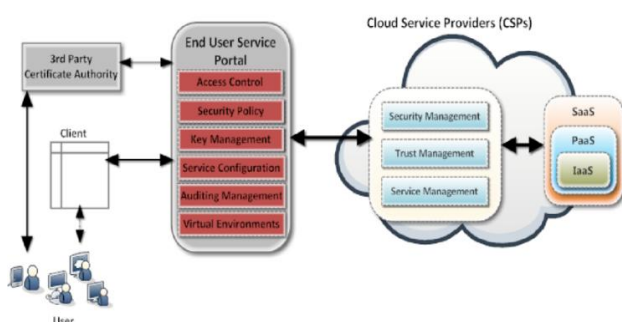


Fig. 2. Framework for Cloud Security Solutions and Mitigation Strategies.

A. Identity Access Management

Identity access management includes making it easier for outside users to access applications, using cloud-based [33]

services more, and using social networking sites more, all of which need access [34]. In order to prevent a cyberattack, it is imperative that data that is currently being transmitted or transmitted soon be encrypted. Businesses are required to standardize their security practices in accordance with the General Data Protection Regulation (GDPR).

B. Data Protection, Encryption, and Key Management

To protect sensitive data from unwanted access, cloud data protection mostly depends on robust encryption methods and secure key management. Organizations may preserve data security to legal requirements by making sure encryption keys are properly stored, rotated, and controlled some discussed below:

- **Symmetric Encryption:** The symmetric encryption algorithm used by all public CSPs is AES-256, which has a key length of 256 bits and uses just one key for encryption and decryption.
- **Asymmetric Encryption:** Cryptography that uses two independent but mathematically related cryptographic keys is called asymmetric encryption or public key cryptography. The two pieces of information are known as a "public and private key pair."
- **Key management service:** Azure, AWS, and Google Cloud Platform all provide key management services [35] making them the three most popular CSPs. Customers may store and organize all of their encryption keys in one convenient location with a key management service. Key management services provide their users with a dashboard where they can generate, assign, remove, and rotate their encryption keys.

C. Threat Detection and Incident Response

Multiple brute-force attacks can compromise cloud resources, including APIs and platforms for cloud management. In Fig 3, buckets show how CSBAuditor warnings match attack attributes in cloud logs.

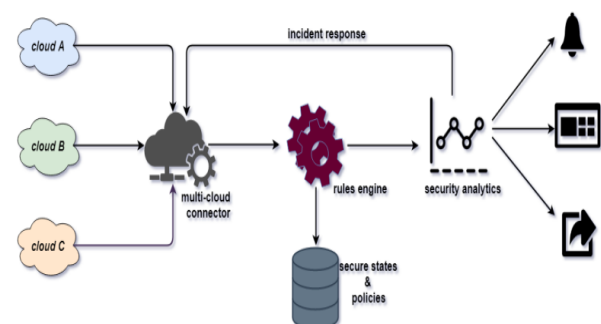


Fig. 3. Threat Detection of an Incident in the Cloud

A human agent can take action, or the Active Responder can revoke the API key of the suspicious user to suspend him immediately.

V. ADVANCED SECURITY FRAMEWORKS AND INTELLIGENT DEFENSE IN CLOUD ENVIRONMENTS

Intelligent protection mechanisms and sophisticated frameworks are increasingly used. These cutting-edge methods guarantee proactive defense against changing threats, improve threat identification, and automate response. Cloud-native security is discussed below:

A. Current Mitigation Tools and Cloud-Native Protections

Cloud-native applications in the real-world context should be continued since the technology and cyber threats keep changing. Microservices, containers, and orchestration platforms are the foundation of cloud-native applications, introducing new issues that need analysis and mitigation, such as identity, access control, and security of communication between services.

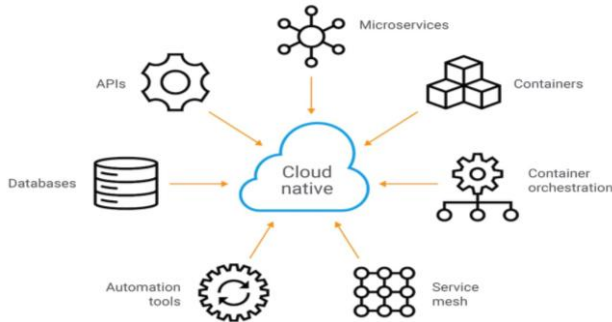


Fig. 4. Cloud-Native Architecture and Its Core Components

Continuous investigation is required to use innovative approaches to threat detection, response to incidents, and compliance, whereas the existing security tools consist of runtime protection capabilities, DevSecOps pipelines, cloud-native SIEM, IAM systems, AI-based threat detection technology, and blockchain-based access control [36]. The industry viewpoints illuminate open-source tools such as Falco and Clair and community projects such as CNCF Security and Kubernetes Security Audit to ensure solid security positions on a case-by-case application, network, infrastructure, and compliance [37][38]. In Fig 4, the core components of a cloud-native architecture, including microservices, containers, orchestration, automation tools, and service mesh, form the foundation for implementing these security protections.

B. Machine Learning-Based Adaptive Security Models

Reinforcement Learning in Security: Intelligent cybersecurity systems could benefit from reinforcement learning, a method that focuses on agents learning from their interactions with their environments. Deep RL has been used in network intrusion detection and attack mitigation. In Fig 5, the SDN architecture serves as a foundation for implementing RL-based adaptive security models.

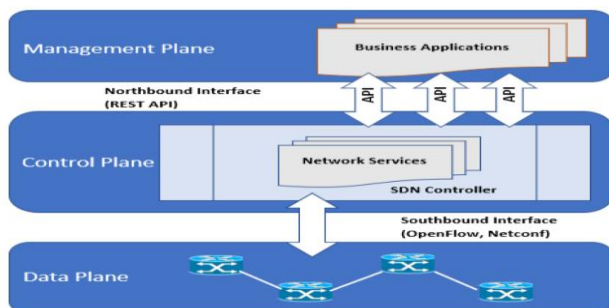


Fig. 5. Layered Architecture of Software-Defined Networking (SDN) for Adaptive and Intelligent Security Management

Automated threat detection and response across AWS, Azure, and GCP was accomplished by a multicloud security orchestration system that made use of a deep RL agent. Different research suggested a cognitive hierarchy DQN model for SOC in the cloud, simulating the dialogue between

human analysts and an RL-inspired attacker to find the best defenses. In contrast to static techniques, RL agents are able to respond to adaptive adversaries and improve data protection by developing complicated strategies. To enable adaptive threat detection and mitigation across the management, control, and data planes in real-time, reinforcement learning techniques can be efficiently integrated into a software-defined networking (SDN) environment [39].

VI. LITERATURE REVIEW

In this section, recent studies demonstrate the growing role of AI and ML in cloud security, from detecting cryptojacking and malware to automating anomaly detection and threat response:

A. Chakravorty and N. Elsayed (2026) present a thorough, methodical study of the literature on AI-based methods for identifying cryptojacking in cloud systems. Machine learning, deep and hybrid models, transfer learning, and federated detection frameworks spanning host, network, hypervisor, and container runtime levels are all covered in the analysis of 41 peer-reviewed research. It looks at how well detection works against contemporary threats like file less mining, encrypted Stratum communication, and container misuse. Additionally, the study assesses operational overhead, repeatability, scalability, class imbalance, and dataset availability. Additionally, typical machine learning models based on preprocessing decisions are validated using publicly accessible datasets [40].

R. Marbel et al. (2026) A Graph Neural Network (GNN) is used in a time-based embedding method for Cloud Services Graph-based Anomaly Detection (CS-GAD) to identify abnormal user behavior. It suggests a dynamic tripartite graph that models how people, activities, and cloud services interact over time. A unique dataset that simulates five real-world attacks—cryptojacking, billing abuse, lateral movement, monitor exploitation, and service targeting—is used to assess the method. The dataset includes 107,116 API requests from 79 AWS services during 32 days, with assaults mixed in with regular cloud traffic [41].

Cao et al. (2025) proposed an unsupervised manner-enabled detection mechanism, only using legitimate applications' magnetic signatures from GPU side channels for model construction. MagInspector innovates in training an unsupervised autoencoder network in an adversarial manner that well learns the stable signature patterns of legitimate applications, while incompatible with mutable cryptojacking ones. In the process of model training, it elaborately extracts mutual energy cumulation distribution features to represent legitimate applications to overcome the impact of their inter-type; a locality sensitive hashing-driven outlier removal algorithm is designed to enhance MagInspector's robustness to noise samples [42].

Nissar et al. (2024) studied cryptojacking attacks on cloud infrastructure, focusing on hacker groups. It analyzes how attackers deploy mining software and malware in the cloud, leading to performance degradation, resource consumption, and financial loss. Typically, these attacks target specific cloud resources like AWS EC2 or Lambda, involving using an EC2 instance as an internal command-and-control (C2) server to coordinate the provisioning of AWS ECS, LightSail, and EKS services for mining purposes. System specifications are exfiltrated through DNS tunneling [43].

Almurshid et al. (2024) purpose of this intelligent cryptojacking malware detection system is to: analyses the lifecycle of both host-based and web-based cryptojacking malware in detail; compare and contrast existing solutions, pointing out their shortcomings; apply deep static analysis to identify key indicators crucial for cryptojacking analysis; execute thorough dynamic analysis to demonstrate the real-world impact of cryptojacking; and use a new, large, and robust cryptojacking dataset (CJDS) with over 100,000 samples, the details of which are provided. (f) builds vision-based prediction models with 23 CNN algorithms, which are thoroughly tested with extensive metrics [44].

Kwedza and Chindipha (2023) A method to acquire bitcoin through the completion of computationally difficult

puzzles for a reward is known as cryptomining. In most cases, it is not feasible to invest in the costly specialized gear needed to accomplish this. An attacker commits cryptojacking when he or she unlawfully exploits a device to mine cryptocurrency. One possible extension of this attack is to leverage cloud infrastructure and networks to create a model that can automatically detect cryptojacking in a cloud setting. This model would analyses network traffic from an attacked cloud server and use machine learning techniques [45].

Table I presents a consolidated summary of recent research on the application of Cryptojacking detection in cloud systems, highlighting the major findings, existing challenges, and prospective future directions.

TABLE I. SUMMARY OF RECENT STUDIES ON AI AND ML APPLICATIONS IN CLOUD SECURITY AND MALWARE DETECTION

Author(s)	Key Findings	Approach	Application	Limitations	Future Work
A. Chakravorty and N. Elsayed (2026)	Reviews AI-based cryptojacking detection techniques and identifies challenges in deployment and evaluation.	Systematic literature review of 41 peer-reviewed studies, supplemented by machine-learning validation experiments.	Cryptojacking detection across cloud hosts, networks, hypervisors, and container environments.	Dataset availability, class imbalance, reproducibility, scalability, and computational overhead remain challenges.	Develop scalable detection models, improve dataset diversity, and validate performance against evolving attacks in real-world cloud environments.
R. Marbel et al. (2026)	Demonstrates the use of temporal graph embeddings and GNNs for early detection of anomalous cloud-user behavior.	Dynamic tripartite graph modeling of users, actions, and cloud services; evaluation using simulated AWS API traffic.	Cloud anomaly detection, including cryptojacking, billing abuse, lateral movement, and other attacks.	Cryptojacking is not the exclusive focus; evaluation relies on simulated traffic, and explicit prevention mechanisms are not established in the provided abstract.	Validate the model using real-world cloud workloads, improve cryptojacking-specific detection, and investigate integration with automated mitigation mechanisms.
Cao et al. (2025)	GPU side-channel magnetic signatures used to detect cryptojacking with high accuracy.	Unsupervised Autoencoder (MagInspector) using adversarial training & LSH-based outlier removal.	Detection of cryptojacking and malicious GPU activities.	Limited to GPU-based attack detection; may fail on CPU cryptojacking.	Extend to multi-dimensional hardware metrics; apply to real cloud deployments.
Nissar et al. (2024)	Identified real hacking groups and cloud resource exploitation (AWS EC2, Lambda, EKS).	Analysis of cryptojacking behaviors, cloud mining strategies & DNS tunneling.	Real-world cryptojacking behavior analysis in cloud infrastructures.	Focused mainly on AWS; lacks detection/prevention mechanism.	Integrate ML-based detection & monitoring tools for cloud platforms.
Almurshid et al. (2024)	Developed an intelligent holistic detection system using the CJDS dataset & CNN-based vision models.	Static & dynamic malware analysis + CNN-based cryptojacking detection.	Host-based & web-based cryptojacking analysis with large dataset (>100k samples).	High computational cost; CNN requires powerful infrastructure.	Optimize CNN models & integrate hybrid ML approaches for real-time use.
Kwedza & Chindipha (2023)	ML model detects cryptojacking automatically using network traffic in cloud systems.	Machine Learning classification using network traffic dataset.	Detection of cryptojacking in cloud server traffic.	Dataset limited to specific attacks; lacks generalization.	Extend dataset & test on multiple cloud platforms (AWS, Azure, GCP).

VII. CONCLUSION AND FUTURE WORK

Cryptojacking poses a critical and evolving threat in the domain of cloud security due to its stealthy nature, distributed execution, and economic motivation. This survey explored the mechanisms, detection methodologies, and mitigation strategies employed against cryptojacking attacks in cloud ecosystems. The reviewed literature highlights that while traditional rule-based intrusion detection systems provide limited defense against emerging cryptojacking variants, ML and DL techniques such as DBNs, CNNs, and autoencoders offer promising capabilities for identifying subtle behavioral deviations and encrypted traffic patterns. Additionally, reinforcement learning-based adaptive frameworks and cloud-native SIEM integrations are advancing automated threat response across multi-cloud infrastructures. Future research should emphasize the development of hybrid AI-based models

that combine static, dynamic, and network-layer features for end-to-end detection, as well as federated learning for privacy-preserving model sharing across organizations. Establishing standardized cryptojacking benchmarks, enhancing interpretability through explainable AI, and deploying real-time, autonomous mitigation pipelines represent critical steps toward achieving resilient and intelligent cloud defense systems.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of interest.

How to cite this article:

P. Laxkar, "Survey on Cryptojacking Detection and Prevention in Cloud Systems," *Journal of Global Research in Electronics and Communication*, vol. 2, no. 8, pp. 22–28, Aug. 2026, Doi: XXXX.

REFERENCES

- [1] E. Idowu, "Cybersecurity Challenges in Cloud- Based ICT Systems," *ArXiv*, vol. 2, no. 1, pp. 0–17, Apr. 2025, doi: 10.20944/preprints202504.1651.v1.
- [2] V. Pal and S. K. Chintagunta, "Transformer-Based Graph Neural Networks for RealTime Fraud Detection in Blockchain Networks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1401–1411, Jul. 2023, doi: 10.48175/IJARSCT-11978Y.
- [3] Y. Macha, "A Review of Cloud-Based CRM Systems in Healthcare: Advances, Tools Challenges, and Best Practices," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 848–856, Nov/Dec, 2022, doi: 10.14741/ijcet/v.12.6.20.
- [4] N. K. Prajapati, "Cloud-based serverless architectures: Trends, challenges and opportunities for modern applications," *World J. Adv. Eng. Technol. Sci.*, vol. 16, no. 1, pp. 427–435, Jul. 2025, doi: 10.30574/wjaets.2025.16.1.1225.
- [5] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijrmt.v4i5.542.
- [6] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 09, no. 03, pp. 205–212, March, 2025, doi: 10.47001/IRJIE/2025.903027.
- [7] E. Tekiner, A. Acar, A. S. Uluagac, E. Kirda, and A. A. Selcuk, "SoK: Cryptojacking Malware," in *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, Vienna, Austria: IEEE, Sep. 2021, pp. 120–139. doi: 10.1109/EuroSP51992.2021.00019.
- [8] A. Hernandez-Suarez *et al.*, "Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks," *Appl. Sci.*, vol. 12, no. 7, pp. 1–28, Mar. 2022, doi: 10.3390/app12073234.
- [9] T. Babenko *et al.*, "Risk Assessment of Cryptojacking Attacks on Endpoint Systems: Threats to Sustainable Digital Agriculture," *Sustainability*, vol. 17, no. 12, pp. 1–36, Jun. 2025, doi: 10.3390/su17125426.
- [10] B. R. Cherukuri, "AI-Driven Security Solutions: Combating Cyber Threats with Machine Learning Models," *Int. J. Multidiscip. Res.*, vol. 6, no. 5, pp. 1–17, Oct. 2024, doi: 10.36948/ijfmr.2024.v06i05.29317.
- [11] H. Kapadia and K. C. Chittoor, "Quantum Computing Threats to Web Encryption in Banking," *Int. J. Nov. Trends Innov.*, vol. 2, no. 12, pp. a197–a204, 2024.
- [12] D. Patel and R. Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.
- [13] S. Amrale, "A Novel Generative AI-Based Approach for Robust Anomaly Identification in High- Dimensional Dataset," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, 2024, doi: 10.48175/IJARSCT-19900D.
- [14] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *Tijer – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.
- [15] S. Xi *et al.*, "MineShark: Cryptomining Traffic Detection at Scale," in *Proceedings 2025 Network and Distributed System Security Symposium*, Reston, VA: Internet Society, 2025, pp. 1–20, February. doi: 10.14722/ndss.2025.230402.
- [16] C. Jansi Sophia Mary, K. Mahalakshmi, and B. Senthilkumar, "Deep Dive On Various Security Challenges, Threats And Attacks Over The Cloud Security," in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, Mar. 2023, pp. 2089–2094. doi: 10.1109/ICACCS57279.2023.10113125.
- [17] A. Kharraz *et al.*, "Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild," in *2019 IW3C2 (International World Wide Web Conference Committee)*, San Francisco, CA, USA: ACM, May 2019, pp. 840–852. doi: 10.1145/3308558.3313665.
- [18] I. A. Khoso, M. A. Khoso, A. Ali, M. Mureed, M. H. Subhpoto, and A. S. Khaskheli, "Detection Of Cryptojacking Threats By Using Machine Learning Within Cloud Server Environments," *Spectr. Eng. Sci.*, vol. 4, no. 5, pp. 2391–2401, May, 2026.
- [19] T. Hetmańczuk, "Cryptojacking: Definition, Implementation, Effects and Protection Against That Form of Cyberattack. Is Malicious Cryptomining a Manifestation of the Crisis Behaviour of Individual Miners During Cryptocurrency Rush?," in *Reactions of Market Entities to Crisis Situations*, Wroclaw University of Economics and Business, 2023, pp. 73–96. doi: 10.15611/2023.96.1.05.
- [20] S. Kumar Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *Tech. Int. J. Eng. Res.*, vol. 9, no. 10, pp. 49–55, 2022, doi: 10.56975/tijer.v9i10.159996.
- [21] M. Dawood, S. Tu, C. Xiao, H. Alasmay, M. Waqas, and S. U. Rehman, "Cyberattacks and Security of Cloud Computing: A Complete Guideline," *Symmetry (Basel)*, vol. 15, no. 11, 2023, doi: 10.3390/sym15111981.
- [22] W. El-Shafai, A. T. Azar, and S. Alshathri, "Vision transformer framework for host based cryptojacking malware detection," *Sci. Rep.*, vol. 16, no. 1, pp. 1–28, Jul. 2026, doi: 10.1038/s41598-025-14378-1.
- [23] P. Shital and C. R., "Web Browser Security: Different Attacks Detection and Prevention Techniques," *Int. J. Comput. Appl.*, vol. 170, no. 9, pp. 35–41, Jul. 2017, doi: 10.5120/ijca2017914938.
- [24] N. N. Gadani, H. Kapadia, and S. Sivasamy, "Deep Belief Networks (Dbn) for Cloud-Based Malware Detection and Analysis," in *2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMO)*, IEEE, Jun. 2025, pp. 400–406. doi: 10.1109/ICCMO67468.2025.00076.
- [25] B. Singh, H. Singh, M. A. Augie, and T. Banerjee, "Strengthening Modern IAM Authentication with Quantum Cryptography and Anti-Phishing Techniques," *Sarcouncil J. Eng. Comput. Sci.*, vol. 04, no. 10, pp. 17–31, October, 2025, doi: 10.5281/zenodo.17260292.
- [26] L. Dong, Z. Li, X. Li, X. Wang, and Y. Liu, "Identification technique of cryptomining behavior based on traffic features," *Front. Phys.*, vol. 11, pp. 1–11, Sep. 2023, doi: 10.3389/fphy.2023.1269889.
- [27] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, pp. 209–218, September, 2024, doi: 10.56472/25832646/JETA-V4I3P122.
- [28] N. D. Bhandarwar, "Generative AI-Driven Framework for Zero-Day Attack Prediction in Next-Gen Cybersecurity Using FusionGuardNet with DualInstinct Optimizer," in *2026 IEEE International Conference on Emerging Computing and Intelligent Technologies (ICoECIT)*, Hyderabad, India: IEEE, Jan. 2026, pp. 1–9. doi: 10.1109/ICoECIT68303.2026.11496755.
- [29] J. Paramesh, K. P. Sriram, E. Anbalagan, S. Sasikumar, and M. G. Vimal Kumar, "Developing an Adaptive Security Framework for Real-Time Threat Detection and Response in Cloud-Network Systems," in *2024 International Conference on Cybernation and Computation (CYBERCOM)*, 2024, pp. 644–648. doi: 10.1109/CYBERCOM63683.2024.10803141.
- [30] P. Mahalle, P. H. Desai, and P. Chandre, "Model Confidentiality in AI-as-a-Service: Challenges and Cryptographic Solutions," in *World Conference on Information Systems for Business Management*, vol. 1748, Springer, 2026, pp. 369–381. doi: 10.1007/978-3-032-12990-1_34.
- [31] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 6–18, Mar. 2025, doi: 10.48175/ijarsct-23902.
- [32] M. R. R. Deva and N. Jain, "Utilizing Azure Automated Machine Learning and XGBoost for Predicting Cloud Resource Utilization in Enterprise Environments," in *2025 International Conference on Networks and Cryptology (NETCRYPT)*, IEEE, May 2025, pp. 535–540. doi: 10.1109/NETCRYPT65877.2025.11102235.

- [33] V. Prajapati, "Cloud-Based Database Management: Architecture, Security, challenges and solutions," *J. Glob. Res. Electron. Commun.*, vol. 01, no. 1, pp. 07–13, 2025, doi: doi.org/10.5281/zenodo.14934833.
- [34] M. Uddin and D. Preston, "Systematic Review of Identity Access Management in Information Security," *J. Adv. Comput. Networks*, vol. 3, no. 2, pp. 150–156, January, 2015, doi: [10.7763/JACN.2015.V3.158](https://doi.org/10.7763/JACN.2015.V3.158).
- [35] T. L. Moore, S. S. Conlon, A. U. Hewarathna, T. B. M. Dissanayaka, and A. B. Mailewa, "Encryption methods and key management services for secure cloud computing: A review.," *Comput. Syst. Sci. Eng.*, vol. 46, no. 3, pp. 967–984, 2022.
- [36] S. Srinivasan, R. Sundaram, K. Narukulla, S. Thangavel, and S. B. Venkata Naga, "Cloud-Native Microservices Architectures: Performance, Security, and Cost Optimization Strategies," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 16–24, 2023, doi: [10.63282/3050-9246.IJETCSIT-V4I1P103](https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P103).
- [37] B. R. Ande, "Enhancing Cloud-Native AEM Deployments Using Kubernetes and Azure DevOps," *Int. J. Commun. Networks Inf. Secur.*, vol. 15, no. 8, pp. 33–41, 2023.
- [38] S. K. Malaraju, G. C. Kakaraparthi, and R. C. Bondalapati, "Efficient Deployment of Scalable AI Models via Kubernetes Orchestration in Hybrid Cloud Setups," in *2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)*, IEEE, Aug. 2025, pp. 1450–1454. doi: [10.1109/CISES66934.2025.11265182](https://doi.org/10.1109/CISES66934.2025.11265182).
- [39] M. Saqib, D. Mehta, F. Yashu, and S. Malhotra, "Adaptive Security Policy Management in Cloud Environments Using Reinforcement Learning," in *2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC)*, IEEE, Apr. 2025, pp. 1–10. doi: [10.1109/ICMCTC62214.2025.11196240](https://doi.org/10.1109/ICMCTC62214.2025.11196240).
- [40] A. Chakravorty and N. Elsayed, "Detecting Cryptojacking in Cloud Environments: A Systematic Review of AI-Based Defenses, Deployment Challenges, and Research Gaps," Mar. 02, 2026. doi: [10.21203/rs.3.rs-8627518/v1](https://doi.org/10.21203/rs.3.rs-8627518/v1).
- [41] R. Marbel, Y. Cohen, R. Dubin, A. Dvir, and C. Hajaj, "Cloudy with a Chance of Anomalies: Dynamic Graph Neural Network for Early Detection of Cloud Services' User Anomalies," in *2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC)*, 2026, pp. 1–7. doi: [10.1109/CCNC65079.2026.11366510](https://doi.org/10.1109/CCNC65079.2026.11366510).
- [42] H. Cao *et al.*, "Unveiling the Superiority of Unsupervised Learning on GPU Cryptojacking Detection: Practice on Magnetic Side Channel-Based Mechanism," *IEEE Trans. Inf. Forensics Secur.*, vol. 20, pp. 4874–4889, 2025, doi: [10.1109/TIFS.2025.3563069](https://doi.org/10.1109/TIFS.2025.3563069).
- [43] N. Nissar, S. Arjun, K. Siddartha, and S. M. Raheman, "Novel Attack Vector to Abuse AWS for Cryptojacking," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2024, pp. 1369–1374. doi: [10.1109/ICAAIC60222.2024.10575628](https://doi.org/10.1109/ICAAIC60222.2024.10575628).
- [44] H. A. Almurshid, I. Almomani, M. A. Khalifa, and W. El-Shafai, "A Holistic Intelligent Cryptojacking Malware Detection System," *IEEE Access*, vol. 12, pp. 161417–161439, 2024, doi: [10.1109/ACCESS.2024.3488192](https://doi.org/10.1109/ACCESS.2024.3488192).
- [45] P. Kwedza and S. D. Chindipha, "Cryptojacking Detection in Cloud Infrastructure Using Network Traffic," in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2023, pp. 1–6. doi: [10.1109/ICECET58911.2023.10389593](https://doi.org/10.1109/ICECET58911.2023.10389593).