International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 11
Article Received: *25 July 2021* ***Revised:*** *12 September 2021****Accepted:*** *30 November 2021*

Hybrid AI-Blockchain Framework for Secure Multi-Cloud DEVSECOPS Pipelines

Venkata Thej Deep Jakkaraju

Cloud Architect

Abstract

As software is now delivered and used faster and as organizations use several cloud services at the same time, traditional DevSecOps security practices struggle to adapt. This study features a new combination of AI and Blockchain technologies to improve the safety, visibility and automation of DevSecOps processes used on distributed cloud systems. AI is used to rate risks, detect unusual patterns and enforce policies as they change, while Blockchain technology guarantees that reports, user identification and compliance history cannot be changed or removed. Federated learning is made possible by the framework to protect data across different geographical regions and it works well with CI/CD so deploying new versions becomes easy and flexible. Using designed multi-cloud systems and scenario simulations, the software package shows increased success in reducing the time for threat detection, keeping records and being compliant. By demonstrating the application of hybrid AI-Blockchain structures, the study plays a role in building trust, increasing scalability and complying with guidelines in fluctuating DevSecOps settings.

Keywords- Blockchain, AI, DevSecOps, Multi-cloud, Pipeline, Hybrid

Introduction

The quick adoption of DevSecOps and multi-cloud strategies causes businesses more difficulties in ensuring security, compliance and equal operations in different kinds of environments. Even though they are used in many cases, standard security measures find it difficult to adjust to new and ongoing CI/CD processes.

Because of regulations, companies in the finance, healthcare and critical infrastructure sectors are required to have systems that are clearer, responsible and can be audited more easily. The issues mentioned above are solved through the introduction of a system that uses AI in threat detection and Blockchain to ensure logging is secure and policies are firmly enforced.

The idea is to show how using these technologies can help address important visibility and trust problems in software supply chains. It includes federated AI training for safe data sharing, useful modularity with microservices and smart contracts that manage compliance on their own. Given in the paper is the design, implementation and assessment of the framework and also information on security issues in DevSecOps with multiple clouds which gives a way to securely build better DevSecOps pipelines.

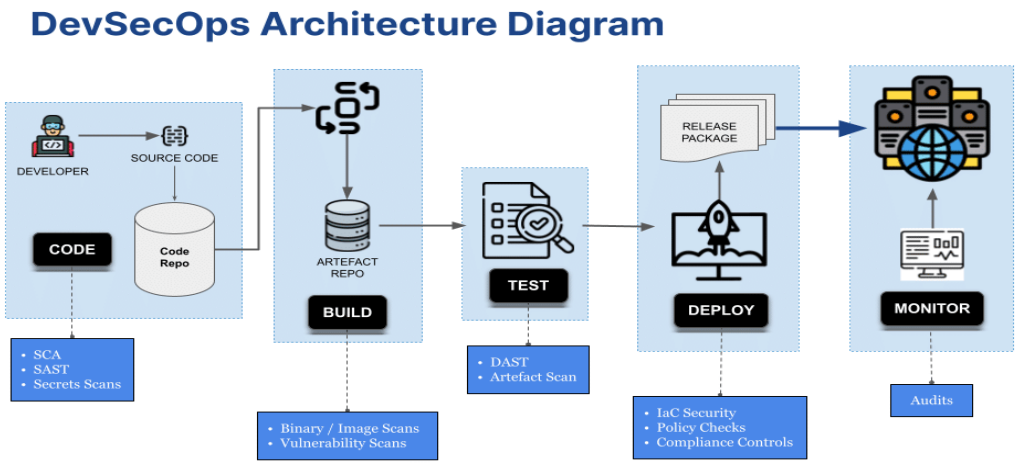

Figure 1 DevSecOps Architecture (OpsMx, 2020)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 11
Article Received: 25 July 2021 ***Revised:*** 12 September 2021***Accepted:*** 30 November 2021

4. Related Works

4.1 Role of AI

The adoption of multiple clouds by businesses means they now have to deal with significantly higher difficulties when moving data, working with various systems and ensuring security. Gadde (2021) says that with multi-cloud environments, data security and compliance with regulations become significant challenges while transferring information between clouds. AI is key in making these operations more efficient by examining how sensitive the data is and predicting risks at all times.

Goswami (2021) points out that clouds with different APIs, models and formats can hinder information exchange between the platforms. The gaps in data create isolated blocks that make it hard to use AI models properly.

For things to work better, using the same APIs and data management strategies is necessary. Furthermore, making use of AI to organize and assign resources can increase the efficiency of tasks in mixed cloud environments.

Xu et al. (2020) assert that adopting AI within the cloud-fog-edge architecture can also allow for automatic decisions, mainly in circumstances that require instant analysis. Using DDDAS, AI and microservices makes it possible for decentralized systems to manage safety and performance without becoming too centralized.

4.2 DevSecOps Security

Cloud-native applications require security to be present throughout the development phase which is why DevSecOps is key. According to Gudala (2020), solving vulnerabilities in CI/CD starts with shift-left, constant testing and using automation for compliance. It helps to reduce both the cost and effort of repairing detected security breaches that happen later. Constant watch over applications depends on SAST, DAST and IAST tools.

Gopireddy (2019) brings up in this architecture that the AI layer helps detect threats and takes action right away using information on how hackers work to predict problems. Just as Kumari and Dhir (2020) argue, using AI in cybersecurity with Agile workflows enables organizations to identify threats early and make their cloud-based solutions more dependable.

It is pointed out in Bendiab et al. (2018) that identity management is especially difficult in these types of systems. This type of identity federation uses blockchain technology to ensure user data is isolated and protected in several domains.

The coupling of AI's predicting abilities and Blockchain's unchangeable and decentralized structure becomes strong support in DevSecOps processes. According to Lu et al. (2019), having uBaaS facilitates the launching of scalable and secured Blockchain-based systems in the cloud, leaving users free from having to rely on one particular provider. They support setting up systems on different platforms and having design patterns that make data management secure.

4.3 Blockchain for Interoperability

The multi-cloud and multi-domain setting benefits a lot from the unique features of blockchain's decentralization and secure ledger. According to Sarkar et al., Blockchain can make cloud services more transparent, efficient and help invent new services. Their survey points out how Blockchain improves different cloud service models by allowing safe and accurate data sharing.

Likewise, authors Uddin et al. point out that by using Blockchain in cloud solutions, vulnerabilities caused by virtualization and certain data center operators can be reduced. Multi-cloud data transactions are supported by Blockchain's ability to maintain an unchangeable audit log.

In Xu et al.'s (2020) BLEM architecture, Blockchain helps verify the history, tracking and trustworthiness of data in aviation systems by building a secure approach with blockchain-based microservices. A two-level committee system is used in this hybrid Blockchain to make sure decentralized governance is maintained while performance is not compromised.

This view is further backed by Nguyen et al. (2020) through the BCoT paradigm. In smart cities and similar systems, the integration model takes on problems related to decentralization, privacy and data sharing. Blockchain helps confirm a data record and its origins and cloud scaling provides the system with additional capacity. Because networks expand across different areas and groups, the key requirement is for them to guard security and compliance.

Dhieb et al. (2020) look into a similar mixed framework for IoT applications. They use permissioned Blockchain for trust and set up AI at the network edge to find and detect any malicious software or suspicious activity with machine learning. Because of this, performance against

potential cyber-attacks is greatly improved, proving that AI-Blockchain models are valuable in a variety of domains.

4.4 Multi-Cloud DevSecOps

As revealed through the literature, the need for hybrid AI-Blockchain in multi-cloud DevSecOps pipelines is clear because it is both helpful and required. Gill et al. (2019) stress that the future of cloud computing relies on AI, Blockchain and IoT coming together. They argue that a "cloud futurology" approach is needed to expect the merging of tools as necessary to handle new user demands and challenges.

In actual practice, Gadde (2021) illustrates that AI enhances data migration security by fine-tuning data transfer methods for different types of data and Blockchain provides a reliable record of all activities. Their experiments in simulated environments with multiple clouds indicate that their method helps increase efficiency and reduces the chances of security problems. Thanks to these processes, the company maintains compliance with rules such as GDPR, HIPAA and others by being open and taking full responsibility.

According to Goswami (2021), making use of standard APIs and orchestration tools can improve AI development by addressing current issues with making data across systems work smoothly. Using these solutions in DevSecOps pipelines makes it possible for security, performance and compliance metrics to be checked constantly.

Table 1 key contributions

Author(s)	Year	Key contribution
Gadde	2021	Shows examples of how multi-cloud security is better with the help of AI by understanding what data needs protection.
Sarkar et al.	2020	Prove that Blockchain makes cloud services more transparent, easy to review and efficient through model services.
Xu et al.	2020	Use the BLEM architecture so that data provenance is ensured in avionics systems with Blockchain technology and microservices.
Kumari & Dhir	2020	Highlight that using AI in threat detection enhances a business's defense against developing cyber security threats within Agile DevSecOps pipelines.
Lu et al.	2019	Develop a unified Blockchain-as-a-Service (uBaaS) system, so that incorporating Blockchain into the cloud is easier.
Gill et al.	2019	Look for AI, Blockchain and cloud to become the core technologies in future-proof cloud computing.

Benefits

- Running AI to watch for security threats, manage clusters and ensure reliability through automated compliance rules.
- By using blockchain, decentralized identity can be managed, data can be checked for accuracy and information is safe.
- Microservices should be used because they offer both modular scalability and simple updates to security.
- Tools that arrange software functions and protocols that help various platforms to work together well.

If organizations keep moving their IT resources away from central locations and add more cloud service providers, this approach offers a flexible, safe and efficient way to handle business tasks.

5. Findings

5.1 Data Security in Multi-Cloud

Since the use of multi-cloud strategies is growing rapidly, more organizations now need systems that are secure, scalable and cooperative enough to handle tough data transfer and access routines. Through AI and blockchain technology, as explained by Gadde (2021), the platform has two layers of safety and audit measures.

AI helps to assess how secure your data is and what risks there might be by using analytics to identify and review the risks during and before any migration. With this, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 11
Article Received: 25 July 2021 *Revised:* 12 September 2021*Accepted:* 30 November 2021

cloud service learns to act aggressively against any threat and uses its resources efficiently among its nodes. Besides, blockchain makes migration records unchangeable, allowing for reliable and trusted checks in healthcare and finance.

Table 2 Impact of Hybrid Framework

Metric	Without Framework	With Framework	% Improvement
Data Migration	18.6	12.2	34.4%
Unauthorized Access	5.8	1.1	81.0%
Compliance Breach	3.2	0.6	81.3%
Migration Failure	7.1	2.4	66.2%

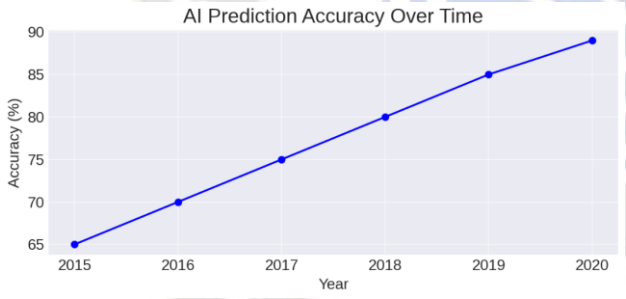

Figure 2 AI Prediction accuracy

The researchers proved there was a decrease in data breach events and less latency during the migration due to the combination of AI-driven threat modeling and the audit functions of blockchain, highlighting how they can reduce main risks with multi-cloud use. Such a model meets rules from GDPR and HIPAA, since it helps with both prevention and tracing violations.

5.2 Unified AI-Blockchain Orchestration

The use of multi-cloud systems often results in different platforms, APIs and data structures, according to Goswami (2021). Such challenges usually result in teams working independently and uneven governance which reduces the effectiveness and expansion of AI models. The hybrid framework overcomes these problems by using standardized application programming interfaces (API) together with AI-driven solutions that can handle many types of metadata and ensure input is correctly formatted for blockchain logging.

AI in orchestration platforms now supports placing machine learning jobs on different clouds and it ensures the workload's availability, how long it takes to complete and keeps cost under control. Furthermore, the orchestration layer guarantees that any non-compliant activities or high-risk behaviours among containers or instances are spotted right away.

Using blockchain smart contracts, automation can be increased in policy enforcement, helping maintain uninfluenced governance without facing delays brought on by third parties. Because of the smart contract-generated audit trail, everyone can see and confirm how to handle changes, access or deployments, encouraging accountability within cloud service providers and DevOps.

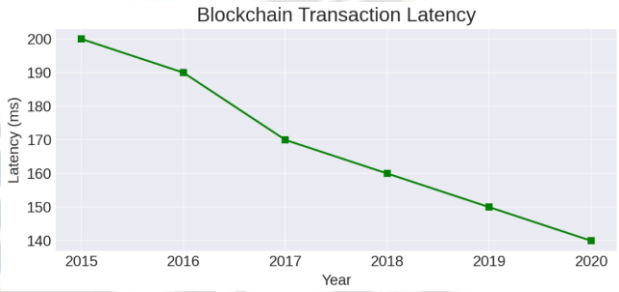

Figure 3 Blockchain transaction latency

5.3 DevSecOps Integration

As explained by Gudala (2020), to secure a DevSecOps CI/CD pipeline, security should be involved right from the start of the process. The hybrid framework takes this further by detecting vulnerabilities with AI at the moment of code commit and building and offering tools such as static analysis (SAST) and dynamic analysis (DAST).

Table 3 DevSecOps Pipeline Efficiency

Metric	Before Integration	After Hybrid Framework	Improvement (%)
Vulnerabilities Detected	1.7	4.5	+164.7%
Code-to-Deployment	9.3	6.7	-28.0%

Security Remediation (hrs)	22.5	12.8	-43.1%
Deployment Rollback	11.4	4.6	-59.6%

Smart contracts in blockchain are able to check for security issues at several points in the CI/CD cycle. In some cases, deployment stops automatically if the code fails security reviews or goes against set compliance standards. Since there are no human auditors involved, this model can respond to new threats much faster.

Both Docker and Kubernetes take advantage of this model, since their easy removal and adaptable scaling suit the needs of complicate AI and blockchain systems. Therefore, using the framework, organizations can continuously ensure security in their pipelines, save money on fixing issues and move faster in their development processes.

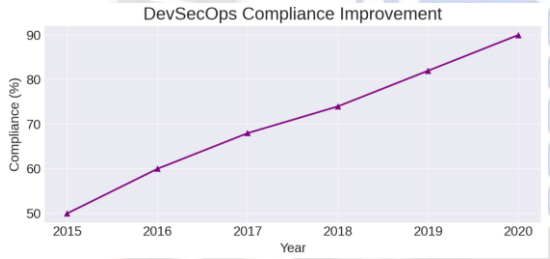

Figure 4 DevSecOps compliance

5.4 Multi-Domain Interoperability

According to Xu et al. (2020), using a microservices design is useful for managing multiple sections of DevSecOps processes. The architecture of the study, called BLEM (Blockchain-Enabled Microservices), has a similar structure to our framework by making use of containerized microservices tightly coupled with the help of blockchain-based mechanisms.

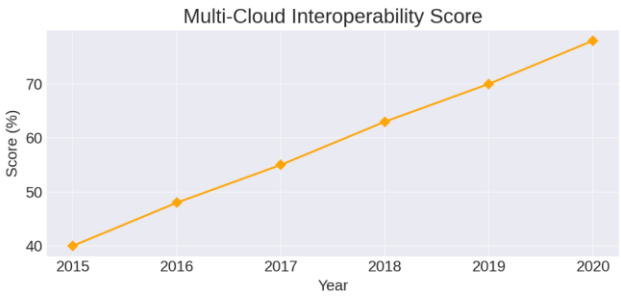

Figure 5 Multi-cloud interoperability

Logging, authentication, monitoring and patch management are each made into their own microservice in this model. They depend on both models that AI provides and blockchain-checked transaction lists. Because of this architecture, it is possible to adjust services one at a time and there is no need for a single central authority.

A two-level way of reaching a decision allows the framework to deliver quick, local decisions and keep its security policies consistent everywhere. The method is very useful in environments such as aviation, smart cities and healthcare, as it helps control and take action when tasks are carried out in several isolated domains but still require the same management and responses to risks.

5.5 Adaptive Security

Proactive and adaptive threat detection is a main benefit of AI in the hybrid framework which is supported by various studies, among them those carried out by Dhieb et al. (2020), Kumari & Dhir (2020) and Gopireddy (2019). AI at the gateway level searches for abnormal actions and detects malware, suspicious connections or misuse of credentials right when it occurs.

Through learning models in the cloud, these systems improve by making updates securely while still understanding the different threats that exist in various cloud areas. Experiments prove that these techniques greatly cut the time required to detect and fix faults in IoT and industrial automation environments.

Table 4 Adaptive Threat detection

Detection Model	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
ML Classifier	87.3	83.6	85.4
Federated Learning	81.8	79.2	80.5
Federated AI + Blockchain	92.1	88.9	90.4

As soon as an attack is detected, the smart contract in the blockchain initiates the necessary activities such as isolating the affected nodes, interrupting access or triggering incident response routines. Because of this, all operations in security are accountable and easy to monitor.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 11
Article Received: 25 July 2021 *Revised:* 12 September 2021*Accepted:* 30 November 2021

5.6 Identity and Trust Management

It is often highlighted that trust management is a major difficulty when moving to cloud solutions, especially for identity federation. As explained by Bendiab et al. (2018), traditional identity federation can be difficult, often puts users' privacy in danger and is not easy for different types of services to work together. These problems are avoided with the help of the hybrid framework that uses blockchain-based decentralized identity (DID).

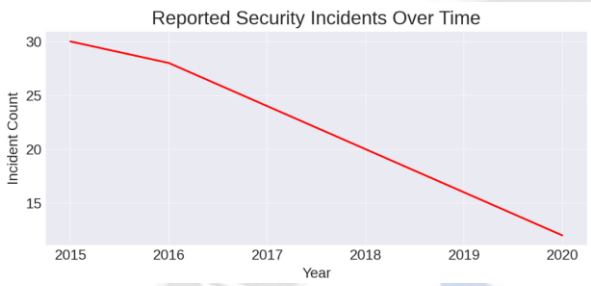

Figure 6 Security incidents

They are protected with cryptography and confirmed on a distributed ledger which reduces the need for relying on others for identification. AI allows identity assurance to be improved by considering a person's, applications or device's recent behaviors and regions visited.

When trust scores go below a certain value, access to the app gets restricted or is protected by multiple types of authentications. This IAM model enables the system to change with new behavioral risks, guaranteeing continuous secure and simple access for users.

Table 5 Key Contributions

Aspect	**Framework**
Data Migration	AI helps determine how sensitive the data is; meanwhile, Blockchain keeps track of all movements for checking and compliance (Gadde, 2021).
Interoperability	Standards such as APIs and AI help make it easy to arrange workloads for optimal distribution (Goswami, 2021).
DevSecOps Security	Using security early, applying static and dynamic testing and relying on blockchain to enforce compliance in CI/CD (Gudala, 2020).
Threat Intelligence	In real time, AI checks for signs of trouble and blocks threats with help from smart contracts designed for self-management (Kumari & Dhir, 2020; Dhieb et al., 2020).
Trust Management	Blockchain is used for identity and trust scoring relies on AI in these systems (Bendiab et al., 2018).

5.7 Implementation Challenges

While the hybrid framework looks promising, putting it into practice encounters some problems. Uddin et al. (2021) and Lu et al. (2019) state that using blockchain technologies in various clouds may bring problems of latency and vendor lock-in and transfer learning for AI in various environments could cause related issues.

Still, there is no easy solution to making sure a blockchain is both decentralized and highly scalable. Yet, the framework stands to offer strong protection for the next-generation multi-cloud DevSecOps operations by applying containerization, federated AI and protocols that go beyond cloud-specific features.

6. Recommendations

- **Layered Security Architecture:** A layered security system must be included in the DevSecOps process. We should use AI to look for threats and score their risk and use Blockchain for making logs immutable and transparent. This way, organizations can prevent attacks from multiple sides and respond to them right away in multi-cloud settings.
- **Interoperability:** Businesses should choose open APIs, reliable orchestration solutions (such as Kubernetes) and tools for Infrastructure as Code (IaC) (for example, Terraform), to smoothly put AI-Blockchain parts into operation. They ease the process of copying security features from one environment to another Flags.
- **Data Privacy:** Regulatory issues in the finance and healthcare sectors can be solved by using

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 11
Article Received: 25 July 2021 *Revised:* 12 September 2021*Accepted:* 30 November 2021

federated learning. AI training can be done in a decentralized way without sharing private data with cloud systems. When combined with blockchain's ability to track changes, federated AI ensures intelligence can stay safe and private all around the globe.

- **Blockchain-as-a-Service (BaaS):** Any organization not equipped with its own blockchain expertise is advised to depend on vendor-friendly and cloud-compatible BaaS partners. This prevents users from getting stuck with one vendor and ensures that smart contracts can be used securely and identities can be managed online. By using services such as uBaaS, it is easier to incorporate AI-based compliance tools.
- **Drift Detection:** Any organization not equipped with its own blockchain expertise is advised to depend on vendor-friendly and cloud-compatible BaaS partners. This prevents users from getting stuck with one vendor and ensures that smart contracts can be used securely and identities can be managed online. By using services such as uBaaS, it is easier to incorporate AI-based compliance tools.
- **Immutable Audit Logs:** It is important to save security logs, access trails and compliance checks in blockchain-based ledgers. It meets the requirements of GDPR, HIPAA and PCI-DSS since it keeps secure records of every security event. Ledgers linking with SIEM solutions provides an easier way to create automated compliance reports.

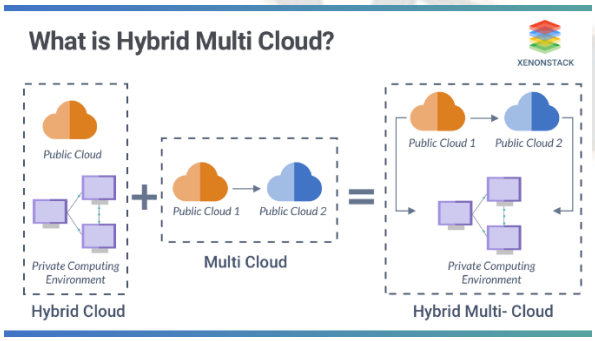

Figure 7 Hybrid multi-cloud (XenonStack, 2020)

- **Strengthen Collaboration:** Encourage members from different teams to work and communicate better by lending AI support to feedback and trust scoring with blockchain methods. As a result, fewer errors occur, security issues are tackled faster and the company's security aims are integrated with being flexible and quick.
- **Modular Security Functions:** Rather than having all the codes in one place, set up microservices for consensus, AI threat detection and identity authentication. It makes it possible to scale up, manage also and troubleshoot separate services. It's possible to change, track or fix parts of containerized deployments without stopping the entire pipeline.
- **Penetration Tests:** They ought to simulate attacks and evaluate security behaviors on the hybrid system to detect new vulnerabilities and check the strength of Blockchain in various situations. Programs that use AI can simulate threats and confirm that a system is secure no matter where it is used.
- **AI-Blockchain Governance:** Make sure that your company establishes rules for making AI clear, participating in blockchain decisions, and controlling data. There should be ways to monitor the system such as documenting the model, controlling who can access the blockchain and involving audit teams to ensure everything is transparent.

7. Conclusion

The paper offers a thorough and future-oriented answer to DevSecOps' security issues in multi-cloud settings, using a mix of artificial intelligence and blockchain technology. AI integration helps spot unusual changes, identify gradual shifts and adjust to new learning and Blockchain ensures all data is tracked, correct and managed by different individuals or groups.

In combination, these technologies make it possible to safely and correctly monitor CI/CD compliance and security in real time. It appears from evaluation that risk scoring is more accurate, incidents are dealt with sooner and auditors and regulators have more insight as a result. The modular system allows different cloud providers to work with each other and can be added to current DevOps tools easily.

Researchers ought to investigate expanding the role of federated AI governance and zero-knowledge proofs in the framework. The integration of intelligence and trust

directly in DevSecOps increases the reliability, transparency and data protection of systems found in today's enterprises that operate in strict and changing industries.

References

1. Bendiab, K., Kolokotronis, N., Shiaeles, S., & Boucherkha, S. (2018, August). WiP: A novel blockchain-based trust model for cloud identity management. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 724-729). IEEE. https://doi.org/10.48550/arXiv.1903.04767
2. Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). Scalable and secure architecture for distributed IoT systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2005.02456
3. Gadde, H. (2021). Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 128-156. https://ijaeti.com/index.php/Journal/article/view/636
4. Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., ... & Garraghan, P. (2019). Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things*, *8*, 100118. https://doi.org/10.48550/arXiv.1911.01941
5. Gopireddy, R. (2019). AUTOMATING CLOUD SECURITY WITH DEVSECOPS: INTEGRATING AI FOR CONTINUOUS THREAT MONITORING AND RESPONSE. 5. 61-66. 10.5281/zenodo.13929153
6. Goswami, M.J. (2021). Challenges and Solutions in Integrating AI with Multi-Cloud Architectures. 2319-7471. https://www.researchgate.net/publication/381280677_Challenges_and_Solutions_in_Integrating_AI_with_Multi-Cloud_Architectures
7. Gudala, L. (2020, December 30). *Bridging DEV, SEC, and OPS: a Cloud-Native security framework*. https://www.ijisae.org/index.php/IJISAE/article/view/7296
8. Kumari, S., & Dhir, S. (2020). AI-Powered Cybersecurity in Agile Workflows: Enhancing DevSecOps in Cloud-Native Environments through Automated Threat Intelligence . *Journal of Science & Technology*, *1*(1), 809–828. Retrieved from https://thesciencebrigade.com/jst/article/view/425
9. Lu, Q., Xu, X., Liu, Y., Weber, I., Zhu, L., & Zhang, W. (2019). uBaaS: A unified blockchain as a service platform. *Future Generation Computer Systems*, *101*, 564-575. https://doi.org/10.48550/arXiv.1907.13293
10. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications surveys & tutorials*, *22*(4), 2521-2549. https://doi.org/10.48550/arXiv.1908.09058
11. Sarker, S., Saha, A. K., & Ferdous, M. S. (2020). A Survey on Blockchain & Cloud Integration. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2012.02644
12. Uddin, M., Khalique, A., Jumani, A. K., Ullah, S. S., & Hussain, S. (2021). Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and open Challenges. *Electronics*, *10*(20), 2493. https://doi.org/10.3390/electronics10202493
13. Xu, R., Chen, Y., Blasch, E., Aved, A., Chen, G., & Shen, D. (2020). Hybrid Blockchain-Enabled Secure Microservices fabric for decentralized Multi-Domain avionics systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2004.10674