# Article information:

Electronics | Free Full-Text | Proactive Forensics in IoT: Privacy-Aware Log-Preservation Architecture in Fog-Enabled-Cloud Using Holochain and Containerization Technologies
<https://www.mdpi.com/2079-9292/9/7/1172>

# Article summary:

1. Cloud computing and IoT devices have brought numerous benefits to various fields, but security and privacy concerns remain a significant issue.

2. The proposed Proactive Forensics in IoT, Privacy-Aware Log-preservation Architecture in Fog-enabled-cloud using Holochain and Containerization Technologies (PLAF) aims to ensure the security and privacy of logs generated by IoT devices in a fog-enabled cloud environment.

3. The PLAF architecture includes features such as log preservation, privacy preservation automation, and tackling multi-stakeholder problems through ownership non-repudiation and trust admissibility. It also uses state-of-the-art technologies such as Docker containers and Holochain for log preservation.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article "Proactive Forensics in IoT: Privacy-Aware Log-Preservation Architecture in Fog-Enabled-Cloud Using Holochain and Containerization Technologies" discusses the challenges of securing log data generated by IoT devices in a fog-enabled cloud environment. The authors propose a three-layered architecture called PLAF that ensures log integrity, verifiability, provenance, and temper resistance while preserving privacy and tackling multi-stakeholder collusion problems.

Overall, the article provides a comprehensive overview of the challenges faced by digital forensics in fog-enabled cloud environments. The authors highlight the importance of proactive forensic data collection and preservation to improve forensic capability and reduce incident response costs. They also discuss the limitations of existing cloud logging schemes that use encryption to secure log data.

However, there are some potential biases and missing points of consideration in the article. For example, the authors do not discuss the potential risks associated with using non-malicious botnets for automated log collection. Botnets can be used for malicious purposes such as launching DDoS attacks or stealing sensitive information. Additionally, the authors do not explore counterarguments or alternative solutions to their proposed architecture.

Furthermore, some claims made in the article are unsupported or lack evidence. For instance, the authors state that fog computing expands the computing and storing properties of cloud computing for network edge without providing any empirical evidence to support this claim.

In conclusion, while the article provides valuable insights into proactive forensics in IoT environments, it is important to consider potential biases and missing points of consideration when evaluating its claims. Further research is needed to validate the effectiveness of PLAF architecture and explore alternative solutions to securing log data in fog-enabled cloud environments.

# Topics for further research:

* Risks associated with using non-malicious botnets for automated log collection
* Alternative solutions to securing log data in fog-enabled cloud environments
* Empirical evidence supporting the claim that fog computing expands the computing and storing properties of cloud computing for network edge
* Potential limitations of PLAF architecture
* Multi-stakeholder collusion problems in digital forensics
* Incident response costs in fog-enabled cloud environments

# Report location:

<https://www.fullpicture.app/item/2e7e1339942c0eb0a247af048751e875>