# Article information:

A Systematic Review of Digital, Cloud and IoT Forensics | SpringerLink
<https://link.springer.com/chapter/10.1007/978-981-15-9317-8_2>

# Article summary:

1. The proliferation of high-end devices with cloud-based services has modernized and eased our lives, but also made it easier for criminals to carry out their activities.

2. Digital forensics is an easier task compared to cloud forensics, as the segregation and collection of evidence in a cloud forensic investigation is a mammoth task due to the distributed and multi-tenant nature of cloud computing.

3. The review aims to create a thorough understanding of the current state of research on digital, cloud, and IoT forensics and identify research gaps to help fellow researchers.

# 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 titled "A Systematic Review of Digital, Cloud and IoT Forensics" provides an overview of the current state of research on digital forensics, cloud forensics, and IoT forensics. The authors highlight the importance of these fields in investigating criminal activities carried out using modern devices and technologies. They also discuss the challenges associated with cloud forensic investigation due to the distributed and multi-tenant nature of cloud computing.

Overall, the article provides a comprehensive review of the literature on digital, cloud, and IoT forensics. However, there are some potential biases and limitations that need to be considered. For example, the authors focus primarily on the benefits of digital forensics in investigating criminal activities but do not explore any potential risks or negative consequences associated with this field.

Additionally, while the authors provide a thorough review of existing research on digital, cloud, and IoT forensics, they do not present any counterarguments or alternative perspectives. This one-sided reporting may limit readers' understanding of the broader context surrounding these fields.

Furthermore, some claims made in the article are unsupported by evidence or require further clarification. For instance, when discussing blockchain in forensics, the authors state that "blockchain technology can be used to create tamper-proof records." However, they do not provide any evidence to support this claim or explain how blockchain technology achieves this goal.

Finally, it is worth noting that some sections of the article contain promotional content for specific technologies or companies. For example, when discussing cloud computing services provided by Microsoft Azure and Amazon Web Services (AWS), the authors mention these companies by name without providing any justification for their inclusion.

In conclusion, while "A Systematic Review of Digital, Cloud and IoT Forensics" provides a useful overview of existing research on these topics, readers should approach it with a critical eye. The article's potential biases and limitations should be taken into account when evaluating its claims and conclusions.

# Topics for further research:

* Risks and negative consequences of digital forensics
* Alternative perspectives on cloud and IoT forensics
* Limitations of blockchain technology in creating tamper-proof records
* Criticisms of Microsoft Azure and Amazon Web Services in cloud forensics
* Ethical considerations in digital
* cloud
* and IoT forensics
* Future directions and emerging trends in digital forensics research

# Report location:

<https://www.fullpicture.app/item/a1724e830c510b32b97cb5f26eee9996>