
Département de génie informatique

# Comparative Critique of Three Scientific Papers


| *Auteur* | *Email* | *Matricule* |
|---|---|---|
| Ilias Bettayeb | ilias.bettayeb@polymtl.ca | 2092408 |


Présenté à :
M. Armstrong Foundjem

20 novembre 2023

# Table des matières

# 1 Comparative Critique of Three Scientific Papers

## 1.1 Overview

The three papers under consideration delve into the topic of the abuse of cloud computing. Each paper explores various facets of this issue, shedding light on its importance. Comparative critique in research is crucial for contextualizing findings, evaluating methodologies, validating results, identifying trends, improving research design and enhancing critical thinking skills. This critique will help have a better understanding of the abuse of cloud computing.

## 1.2 Research Questions/Objectives

— Paper 1 : Explore and investigate the scope and magnitude of the security threat "abuse and nefarious use of cloud computing."
— Paper 2 : To investigate the prevalence and characteristics of cryptojacking, specifically focusing on the development of CMTracker as a behavior-based detector
— Paper 3 : The primary objective is to propose an economic measure to deter attacks and service abuses in cloud computing applications through the use of digital currency

## 1.3 Methodologies

— Paper 1 : The paper does not explicitly detail the methodology used. But cloud deployment models, cloud computing threats and attacks related to abuse use of cloud computing are treated on this paper. This paper defines in detail a bunch of notions that might be useful for the projet. [HO13]
— Paper 2 : The paper employs CMTracker, a behavior-based detector with two runtime profilers, to automatically track cryptocurrency mining scripts and their related domains. The two profilers include a hash-based profiler and a stack structure-based profiler. [Hon+18]
— Paper 3 : The paper proposes the BitDeposit scheme, where users make a small deposit in digital currency before using a service, and this deposit is refunded if no abuse or attack is detected. The use of Bitcoin and its ecosystem is explored as a solution, leveraging micropayments and currency exchanges. [SL13]

## 1.4 Key Findings

— Paper 1 : The paper identifies "abuse and nefarious use of cloud computing" as the top security threat. It emphasizes weak registration processes and the potential misuse of cloud services by cybercriminals.
— Paper 2 : The study provides insights into the impact, distribution mechanisms, obfuscation, and attempts to evade detection in cryptojacking attacks. Notably, organizations benefit from cryptojacking, leveraging unique wallet IDs, and frequently updating their attack domains.

— Paper 3 : The BitDeposit scheme utilizes Bitcoin to require users to make deposits, deterring potential attackers. The digital currency allows for low transaction costs, and the deposits withheld from attackers can be exchanged for real-world currency.

## 1.5 Strengths and Limitations

— Strengths
  * Shared strengths among the papers : The three papers give examples of attacks related to the abuse of cloud computing. Also, the papers explain quite complicated concepts in a simple way which is really helpful.
  * Unique strengths of individual papers :
    — Paper 1 : The paper emphasizes the importance of understanding and addressing security threats in cloud computing. Also, the focus on the specific threat of abuse and nefarious use provides depth.
    — Paper 2 : This study really goes in-depth and the result sections is comprehensive. The INFRASTRUCTURE OF MALICIOUS MINERS section has infrastructures that are very well explained and that we could recreate in our project.
    — Paper 3 : The paper introduces an innovative economic approach, the BitDeposit scheme, using digital currency (Bitcoin) to deter attacks and service abuses in cloud computing applications. Also, the paper discusses the applicability of the BitDeposit scheme to various cloud computing applications beyond email spam
— Limitations
  * Common limitations or shortcomings : Two of the papers are too much focused on cryptocurrency and don't really talk about the other types of attacks of abuse of cloud computing.
  * Unique issues pertaining to individual papers :
    — Paper 1 : The paper lacks explicit details on the methodology used, making it challenging to assess the rigor of the research.
    — Paper 2 : The study relies on behavior-based profiling, potentially missing some evasion techniques not accounted for by CMTracker. The detection approach may have false negatives, as some cryptojacking pages might escape detection.
    — Paper 3 : The paper acknowledges challenges, such as determining the appropriate deposit value and addressing transaction costs. Potential issues related to breaking pseudonymity and key reuse are identified.

## 1.6 Discussions and Implications

— Paper 1 : The authors interpret their results by highlighting the vulnerabilities of cloud computing, especially in terms of insider threats and the potential for cybercriminals to exploit weak registration processes. The implications suggest a need for more proactive security measures
— Paper 2 : The authors highlight the importance of their behavior-based detection approach compared to existing solutions, emphasizing the need for more sophisticated

detection methods.
— Paper 3 : The authors emphasize the benefits of using digital currency, specifically Bitcoin, for its decentralized nature, low transaction costs, and the ability to convert deposits into real-world money.

There are no differences in how the authors of the three papers relate their findings to existing literature or real-world implications. Also, there isn't any contrasting viewpoints or interpretations among the papers

### 1.7 Recommendations and Future Directions

Future research in the field of cloud computing abuse should focus on integrated solutions that combine proactive security measures, enhanced behavior-based detection mechanisms, and innovative approaches like the BitDeposit scheme. This approach can address the multifaceted challenges identified in the papers, including unauthorized access, evolving evasion techniques, and issues related to deposit values and transaction costs. By integrating these elements, researchers can develop more comprehensive and effective strategies to guard cloud computing environments from abuse activities.

## 2 General Observations :

The papers highlights the importance of a comprehensive and multi-faceted approach to address cloud computing abuse. While Paper 1 emphasizes the need for transparent methodologies in security research, Paper 2 highlights the pervasive impact of cryptojacking and the effectiveness of advanced tracking tools like CMTracker. Paper 3 introduces an economic perspective, emphasizing the BitDeposit scheme's potential benefits. Integrating these insights could lead to effective mitigation strategies against diverse threats in cloud computing.

## 3 Conclusion :

This critique highlights the importance of a comparative approach in understanding cloud computing abuse, emphasizing strengths, limitations, and implications across three papers. It highlights the significance of behavior-based detection mechanisms, as seen in Paper 2's examination of cryptojacking. Additionally, Paper 3 introduces a pioneering economic perspective with the BitDeposit scheme. Paper 1 also helped introducing the attacks related to the abuse of cloud computing. Those three papers provides notions that will be helpful for the project.

# Références

[HO13] Yasir Ahmed Hamza et Marwan Dahar Omar. « Cloud computing security : abuse and nefarious use of cloud computing ». In : *Int. J. Comput. Eng. Res* 3.6 (2013), p. 22-27.

[Hon+18] Geng Hong et al. « How you get shot in the back : A systematical study about cryptojacking in the real world ». In : *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018, p. 1701-1713.

[SL13] Jakub Szefer et Ruby B Lee. « Bitdeposit : Deterring attacks and abuses of cloud computing services through economic measures ». In : *2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*. IEEE. 2013, p. 630-635.