

Cybersecurity Professional Career Paper: Cloud Security Engineer: Protecting
Data in the Cloud

Student Name: Aaron Fields

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: November 16, 2025

Introduction

Cloud computing has become a major part of how businesses and individuals store and manage data. It offers flexibility and cost savings, but it also introduces new security challenges. A Cloud Security Engineer is responsible for making sure cloud environments are safe from cyber threats. This paper explains how social science principles connect to this career, how key cybersecurity concepts are applied, and how this role impacts marginalized groups and society.

Human Behavior in Cloud Security

Human behavior plays a big role in cloud security. Many breaches happen because of simple mistakes like misconfigurations or weak passwords. Cloud Security Engineers need to understand these behaviors and design systems that reduce risk. They also create training programs to help users avoid mistakes. Social engineering attacks, which trick people into giving away information, show why understanding psychology and communication is important in this field (Carley, 2020).

Ethical Responsibilities

Ethical issues are another part of the job. Engineers must make decisions about privacy and data protection that respect legal and social standards. These decisions affect how data is stored, shared, and monitored. Protecting user privacy is not just a technical requirement but an ethical responsibility that shapes trust in cloud systems. Engineers also need to consider transparency and fairness when implementing security policies. They must balance business goals with user rights, ensuring that security measures do not lead to discrimination or misuse of personal data. These choices influence public confidence and the overall integrity of digital environments.

Applying Cybersecurity Concepts

The points about human error and ethical decisions connect directly to the technical work Cloud Security Engineers do every day. When engineers set up identity and access management (IAM), they address the risk of weak passwords and misconfigurations. Multi-factor authentication and role-based access controls reduce mistakes and limit damage if credentials are stolen. Encryption supports privacy, and monitoring tools like SIEM help detect suspicious activity quickly. These tools and practices show how technical measures reduce risks linked to human behavior and ethics (Ahmadi, 2024; Dawood et al., 2023). Engineers also implement automated compliance checks to ensure systems meet regulatory standards. Continuous updates and patch management are equally important because outdated software can create vulnerabilities that attackers exploit.

Impact on Marginalized Communities

This career also impacts marginalized groups. People in underserved communities often have less access to secure technology and less training on safe practices. This makes them more vulnerable to phishing and misconfiguration. Cloud Security Engineers can help by designing systems that are easier to use and by supporting programs that teach cybersecurity basics. These efforts reduce the risk of exploitation and promote fairness in digital spaces (Ghosh et al., 2025).

Conclusion

Cloud Security Engineers use social science principles to understand human behavior, prevent mistakes, and make ethical decisions. They apply cybersecurity concepts to create secure systems and address issues of equity and privacy. This combination of technical and social knowledge makes the role essential as cloud

computing continues to grow. I am interested in this career because it combines technical work with policy and compliance responsibilities. That mixture of hands-on problem-solving and shaping security standards is exactly what I want to do in the field of cybersecurity.

References

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, 26(4), 365–381.

<https://doi.org/10.1007/s10588-020-09322-9>

Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, 26(2), 215–228. <https://doi.org/10.9734/JERR/2024/v26i21083>

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and security of cloud computing: A complete guideline. *Symmetry*, 15(11), 1981. <https://doi.org/10.3390/sym15111981>

Ghosh, A., Diyasi, S., & Dey, D. (2025). Cybersecurity literacy programs for marginalized communities: Bridging the gap in digital security. *International Journal of HIT Transaction on ECCN*, 9(1A), 29–44.