



Analysis of sample size, type, and statistical method in cybersecurity research.

Prepared by

ALI MMADI, PhD student - Midocean University



Research Skills (2)

Task 5

ALI MMADI

PhD student - Midocean University

www.midocean.ae

1. Introduction

Hello,

My name is Ali Mmadi, a PhD student in Information Technology, specializing in Cybersecurity.

In this fifth task of the Research Skills 2 course, I will present the methodological part related to sampling and the statistical method in scientific research.

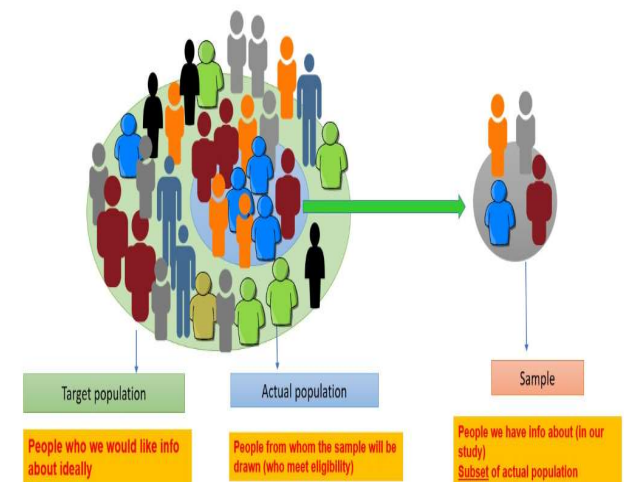
My example is based on a study applied to the security of hybrid Cloud environments and intrusion detection using artificial intelligence.

2. Definition of the research framework and community

The **research community**, or **study population**, represents all the individuals or systems concerned by the research.

In my study, the **research community corresponds to cybersecurity professionals and system administrators** working in organizations using hybrid cloud infrastructures.

This population is chosen because it possesses the knowledge and operational practices related to network and data security.



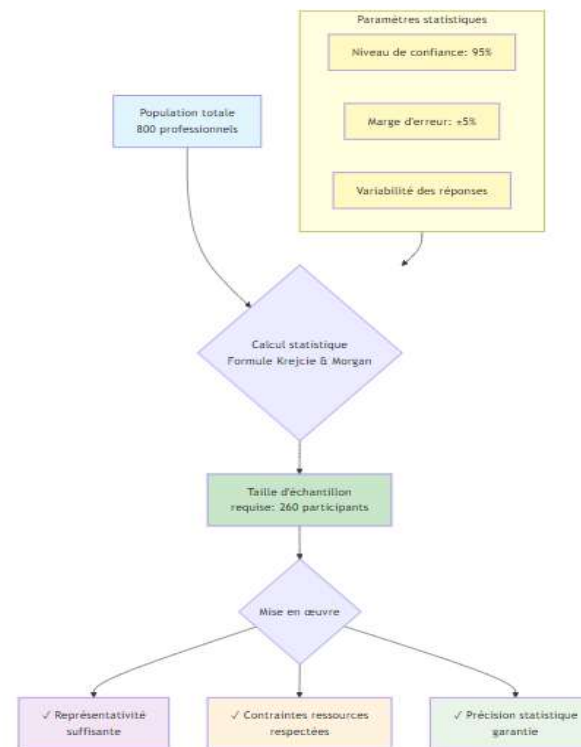
3. Sample size

The sample size depends on several criteria:

- ❑ The total population size;
- ❑ The confidence level (often 95%);
- ❑ The tolerated margin of error (often $\pm 5\%$);
- ❑ And the variability of the expected responses.

In my example, for a population estimated at **800 professionals**, the statistical calculation using the Krejcie & Morgan (1970) formula determined a sample size of **260 participants**.

This size ensures sufficient representativeness while respecting time and resource constraints.



4. Sample type

To select the respondents, I used a **probabilistic sampling method**, more specifically the stratified random sampling method.

This method involves dividing the population into homogeneous sub-groups, called strata, for example:

- Network administrators,
- Security analysts,
- Cloud engineers.

Then, a **proportional random sample** was selected from each stratum.

This type of **sampling allows for better representativeness** of the different roles in the field of cybersecurity.

5. Statistical method used

After data collection using a structured questionnaire, statistical analyses were carried out using SPSS software and the Python language (pandas, statsmodels). Three levels of analysis were applied:

Descriptive analysis:

- ❑ Means, standard deviations, and frequencies to describe respondents' perceptions.
- ❑ Example: the average score for 'trust in Cloud security policies' was 3.8 out of 5.

Correlation analysis (Pearson):

- ❑ To measure the relationship between cybersecurity awareness and compliance with security policies.
- ❑ Result: $r = 0.72$, $p < 0.01$, indicating a strong positive correlation.



Multiple regression analysis:

- ☐ To identify predictive variables of security performance.
- ☐ Significant factors include cybersecurity training and organizational maturity.

These analyses made it possible to empirically validate the research hypotheses while ensuring the scientific rigor of the model.

5. Conclusion

In summary:

- ✓ The research community consisted of cybersecurity professionals in Cloud environments.
- ✓ The sample, composed of 260 participants, was determined according to the statistical rules of Krejcie & Morgan.
- ✓ The type of sampling adopted was stratified random sampling, ensuring the representativeness of the groups.
- ✓ Finally, statistical analyses were conducted using SPSS and Python, combining descriptive, correlational, and regression analyses.

These steps demonstrate **the methodological validity and reliability of scientific research** in the field of **cybersecurity**.

Thank you for your attention.

Bibliographic reference

1. Krejcie, R. V., & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, 30(3), 607–610.
2. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate Data Analysis* (8th ed.). Pearson.
3. Creswell, J. W. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage.
4. ISO/IEC 27032:2023. *Cybersecurity Guidelines for Information Security*.
5. Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach for Intrusion Detection in Cloud Environments. *Future Generation Computer Systems*, 89, 347–359.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

