International Journal of Core Engineering & Management
Volume-8, Issue-02, 2025 ISSN No: 2348-9510

A QUALITATIVE RESEARCH DESIGN FOR INVESTIGATING CLOUD SECURITY CONCERNS USING REFLEXIVE THEMATIC ANALYSIS

Dr. Sonal Sagar Boda
University of the Cumberlands
sboda59203@ucumberlands.edu

Abstract

This study presents a replicable exploratory qualitative methodology designed to investigate cloud security concerns in enterprise SaaS environments. Grounded in an interpretivist paradigm, the research followed a structured five-phase design including problem identification, research question development, methodological construction, expert sampling, and reflexive data analysis. Participants were recruited through a multi-step expert sampling process using professional networks and strict eligibility criteria. Data were collected via semi-structured interviews and analyzed using a six-phase reflexive thematic analysis framework that supported both inductive and deductive coding approaches. The study incorporated trustworthiness strategies through credibility, dependability, confirmability, and transferability, with emphasis on ethical compliance, informed consent, and anonymization protocols. Reflexivity and bracketing were maintained throughout to reduce researcher bias. This methodological blueprint offers a practical and transferable guide for scholars seeking to explore complex cloud security challenges through rigorous qualitative inquiry.

Keywords: Qualitative research, reflexive thematic analysis, cloud security, expert interviews, research trustworthiness, interpretivist paradigm, research design.

I. INTRODUCTION

Qualitative research plays an essential role in understanding complex, context-dependent issues within enterprise environments, particularly in domains like cloud computing where socio-technical factors shape implementation outcomes. As cloud-based systems become increasingly embedded in digital transformation initiatives, there is a need for methodological frameworks that can capture expert insight, organizational dynamics, and embedded knowledge systems related to cloud security practices [1]. This study responded to that need by presenting a rigorously designed qualitative research methodology aimed at investigating security architecture concerns in Software as a Service (SaaS) environments.

The research was grounded in an interpretivist paradigm, which acknowledged that meaning is constructed through human experiences, social contexts, and organizational interactions. This philosophical orientation supported in-depth engagement with domain experts to explore how they interpreted, managed, and responded to cloud security risks in real-world enterprise

settings [2]. Unlike positivist approaches that seek generalizable truths through quantifiable variables, the interpretivist stance applied in this study prioritized contextual understanding, participant subjectivity, and knowledge co-construction—principles well-suited to exploring emerging and nuanced security concerns in cloud-based architectures [3].

To support this interpretive lens, the study was designed using a structured qualitative research framework comprising five interrelated phases: identifying the research problem, formulating research questions, constructing the methodology, conducting expert interviews, and analyzing the data through reflexive thematic analysis. The structured design enhanced procedural clarity and made the methodology suitable for replication in other enterprise-focused information systems research [1], [4]. Transparency across each phase—especially in participant recruitment, data collection, and analysis—further supported trustworthiness and reproducibility, two critical standards in qualitative scholarship [5].

A central objective of this paper is to provide a detailed and replicable account of the research design process, particularly as it relates to expert sampling and data interpretation in high-stakes cloud environments. Fifteen experts were recruited through professional networks using purposive sampling methods tailored for niche enterprise domains. The process emphasized inclusion criteria tied to experience in SaaS implementation and security oversight, while maintaining rigorous protocols for informed consent and confidentiality [4], [6]. This methodological transparency is especially vital in fields where access to qualified participants is limited and where expert input provides contextual depth not attainable through surveys or observational studies.

Data were analyzed using Braun and Clarke's reflexive thematic analysis, a six-phase approach that emphasized researcher subjectivity, iterative engagement, and theoretical alignment throughout the coding process. This form of analysis supported both inductive and deductive coding, enabling researchers to surface emergent insights while also mapping those insights to existing conceptual frameworks where appropriate [7]. The use of reflexivity and bracketing further ensured that researcher assumptions were acknowledged and addressed throughout the analytic process [2], [7].

The methodology presented in this paper was originally developed and implemented as part of the author's doctoral dissertation in information technology. Ethical protocols, data collection instruments, and analytic strategies were approved through an institutional review board and applied consistently throughout the study.

The remainder of the paper is structured as follows: Section II outlines the philosophical alignment and rationale for the chosen research design; Section III describes the data collection and expert sampling procedures; Section IV details the data analysis procedures used; Section V discusses trustworthiness and ethical considerations; Section VI presents methodological limitations and recommendations; and Section VII concludes with reflections on the study's contribution to qualitative research in information systems.

International Journal of Core Engineering & Management
Volume-8, Issue-02, 2025 ISSN No: 2348-9510

II. RESEARCH DESIGN AND PARADIGM ALIGNMENT

The study employed a structured qualitative research design to investigate security concerns in Software as a Service (SaaS) cloud environments. This design was selected to explore how experienced enterprise professionals interpret, describe, and respond to architectural and operational risks associated with cloud service delivery. The research design was purposefully aligned with the interpretivist paradigm, which supports contextual, meaning-centered inquiry rather than hypothesis testing or statistical generalization [8]. As cloud security involves deeply embedded organizational practices, an exploratory and interpretive approach was best suited to uncover how these practices are understood and enacted by domain experts in their real-world settings [9].

The interpretivist orientation of the study positioned reality as socially constructed, shaped by human interaction, institutional knowledge, and lived organizational experience. This epistemological stance guided all aspects of the research—from sampling and instrumentation to interview interaction and analytical interpretation [10]. The research design rejected the notion of a single objective truth in favor of capturing multiple, coexisting realities from participants directly engaged in SaaS implementation and security oversight. By focusing on expert perspectives, the study sought to explore both the conscious strategies and tacit knowledge that inform enterprise responses to persistent and emergent cloud security challenges [11].

To implement this philosophical approach, the study followed a five-phase qualitative research design. These phases included: (1) identifying the research problem, (2) formulating research questions, (3) designing the methodological framework, (4) collecting data through expert interviews, and (5) analyzing data using reflexive thematic analysis. This design enabled an iterative inquiry process, where data collection and analysis informed one another, and early insights could be refined as understanding deepened [8], [12]. The goal was not to produce predictive models or quantifiable metrics, but to construct a conceptual understanding grounded in participant narratives and security practice environments.

The qualitative design was further justified by the exploratory nature of the research questions, which were open-ended and developed to investigate the "how" and "why" behind cloud security concerns. Rather than starting with a predefined hypothesis, the study allowed research questions to evolve through a recursive and reflexive engagement with participants and data [13]. This flexibility is a hallmark of qualitative research, particularly in under-theorized or rapidly evolving domains such as cloud-based architecture and cybersecurity governance [10], [13]. By avoiding rigid protocol-driven methods, the design maintained openness to emerging constructs and relational patterns that might otherwise be constrained in quantitative or positivist frameworks.

The research design also accounted for the researcher's role as an instrument of inquiry, consistent with interpretivist principles. To minimize bias and maximize rigor, the researcher engaged in reflexivity throughout the design and data collection phases. Reflexive practices included bracketing personal assumptions, maintaining analytic memos, and documenting decisions related to methodological adjustments. These strategies contributed to the

transparency, accountability, and trustworthiness of the research design [9], [14].
Finally, the chosen research design responded to the need for methodological clarity in qualitative studies of enterprise security. While much of the existing cloud computing literature remains dominated by technical or quantitative perspectives, this study demonstrated how interpretive, expert-centered methods can produce insights that are both academically rigorous and practically relevant. The following sections document the operationalization of this design across participant recruitment, interview development, thematic coding, and trustworthiness strategies, establishing a detailed and replicable process for future research in this space.

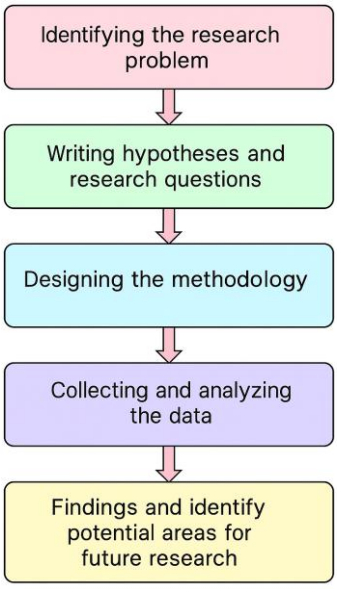

Fig. 1. Five-step exploratory qualitative research design

Figure 1. illustrates the five-phase research design developed and executed in this study. Each stage represents a key methodological milestone: identifying the research problem, writing hypotheses and research questions, designing the methodology, collecting and analyzing data, and identifying areas for future research. The diagram visually reinforces the logical sequence and procedural transparency essential to replicable qualitative inquiry in cloud security contexts. Color-coded pastel segments help distinguish each phase for clarity and readability.

III. DATA COLLECTION AND SAMPLING PROCEDURES

The data collection phase of the study was structured to support methodological transparency, ethical rigor, and thematic saturation. Semi-structured interviews were used to elicit detailed accounts from expert participants with practical experience in SaaS security architecture. The interview method was chosen to allow open-ended exploration of individual perspectives,

while maintaining a consistent framework of core questions related to cloud security challenges, decision-making processes, and organizational dynamics [15]. All interviews were conducted by the researcher and recorded with participant consent, enabling transcription and detailed analysis.

Participant selection followed a five-step expert sampling process designed to reach highly qualified individuals in the enterprise cloud computing domain. The sampling strategy began with targeted outreach to LinkedIn groups relevant to SaaS architecture, cybersecurity, and enterprise technology. Additional recruitment efforts involved direct messaging on LinkedIn and personalized invitations to professionals who met the study's criteria. From this initial pool, participants were selected based on relevance to the research topic, depth of implementation experience, and willingness to engage in a semi-structured interview process [16]. This approach ensured alignment between research objectives and participant qualifications while maintaining ethical recruitment practices.

The final sample consisted of fifteen participants who met predefined inclusion and exclusion criteria. To be eligible for the study, participants had to be at least 18 years of age and have demonstrable experience with SaaS implementation projects, particularly those involving architectural decision-making and security governance. Individuals without relevant experience or who declined to participate after receiving the study overview were excluded [16]. This criteria-driven approach contributed to data integrity by focusing on participants who possessed both technical and contextual knowledge of cloud service environments.

Demographic data were collected during the onboarding process to contextualize participant responses. These data included gender, age range, professional role, and specific expertise in SaaS implementation and cloud security. The sample included individuals across various industries and organization types, enhancing the relevance and applicability of the qualitative insights. While the study did not seek to generalize findings to a population, diversity in participant background supported a broader range of perspectives related to architectural, operational, and governance-related concerns in cloud computing [17].

Prior to participation, all individuals received a detailed information sheet outlining the purpose of the study, the nature of participation, and data protection procedures. Informed consent was obtained through signed documentation, and participants were informed of their right to withdraw at any time without consequence. The research protocol was reviewed and approved by the Institutional Review Board of the University of the Cumberlands to ensure compliance with ethical standards for human subject's research [18]. Confidentiality measures were implemented through anonymization of interview transcripts and removal of identifiable information during data processing.

To ensure qualitative rigor, the study applied the principle of data saturation as a guide for sample size adequacy. While the total recruited sample comprised fifteen participants, saturation was observed after twelve interviews, with no new concepts emerging in the final transcripts. This approach combined iterative questioning with thematic saturation principles to determine when sufficient data had been collected to support credible and transferable insights [19]. The next section describes the analytic procedures used to examine these data, including

International Journal of Core Engineering & Management
Volume-8, Issue-02, 2025 ISSN No: 2348-9510

coding frameworks, analytical transparency, and the role of reflexivity.

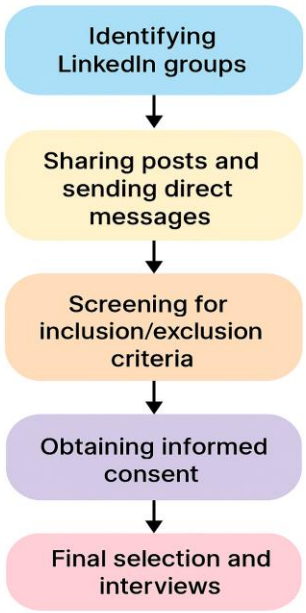

Fig. 2. Expert Sampling and Recruitment Process

Figure 2 illustrates the five-step participant recruitment process used in this study. The flow began with identifying relevant LinkedIn groups in the enterprise cloud domain, followed by sharing recruitment posts and sending personalized direct messages. Screening for inclusion and exclusion criteria ensured that participants met the minimum threshold of SaaS implementation and security experience. Informed consent was then obtained from eligible participants, after which final selection and interview scheduling were completed. The color-coded flow highlights the procedural rigor applied to the purposive expert sampling strategy used for this study.

IV. DATA ANALYSIS PROCEDURES

The data analysis phase followed Braun and Clarke's reflexive thematic analysis framework, which provided a structured yet flexible approach to interpreting qualitative interview data. This six-phase model was selected for its suitability in capturing patterns of meaning across participants' narratives while supporting iterative and reflexive engagement. The six phases included (1) familiarization with the data, (2) initial coding, (3) generating candidate themes, (4) reviewing themes in relation to coded extracts and the full dataset, (5) defining and naming themes, and (6) producing the final analytic narrative [20]. Each phase was applied systematically to preserve analytic rigor and traceability.

Data familiarization involved reading and re-reading each interview transcript in full. During this phase, the study documented early impressions and analytic memos, which supported

reflexivity and informed the direction of subsequent coding. This immersion enabled a deep understanding of the nuances in participant language, tone, and contextual framing. All transcripts were anonymized and formatted prior to analysis to ensure participant confidentiality [21].

Initial coding was conducted using ATLAS.ti qualitative analysis software, which allowed systematic organization of data excerpts and supported code mapping. Both inductive and deductive coding strategies were employed. Inductive codes emerged directly from the data, grounded in participant descriptions of real-world challenges, decision-making contexts, and organizational conditions. Deductive codes were aligned with the conceptual literature and theoretical framework which guided the study, including concerns related to governance, architecture, security controls, and domain-specific analytic categories [22]. The dual approach enhanced analytic completeness and ensured relevance to both practice and theory.

Candidate themes were generated by clustering conceptually related codes into overarching categories. During this process, the study reviewed all initial codes for consistency, relevance, and depth. Visual mapping tools in ATLAS.ti supported this process by highlighting relationships among codes, co-occurrence frequencies, and code density across participants. These outputs informed the identification of patterns of meaning that extended beyond individual transcripts [23].

The theme refinement phase involved critically reviewing all themes against both coded data extracts and the full dataset. The study tested the coherence, internal consistency, and boundary clarity of each theme to ensure analytic soundness. Overlapping themes were either merged or further differentiated, depending on their conceptual distinction and interpretive value. Themes that lacked adequate support or clarity to answer the research questions were excluded [20], [23].

In the defining and naming phase, each finalized theme was articulated in a concise analytic descriptor that captured the central idea of the theme in relation to the research questions. The naming process emphasized alignment with participants' phrasing while also ensuring interpretive clarity and abstraction. Definitions were documented in analytic memos and reviewed for fit with the overarching research questions and objectives. These definitions served as anchors for reporting, ensuring consistency from coding to interpretation [24].

The final analytic phase involved synthesizing the defined themes into a coherent narrative structure. This phase bridged participant data with methodological transparency, allowing the final interpretation to reflect both empirical grounding and theoretical insight. The output was not limited to descriptive categorization but offered an interpretive account of the latent meanings embedded in expert discourse. These interpretations were later integrated with existing literature to close the analytic loop, though that stage is addressed in a separate publication [24].

Throughout all phases, the study maintained a reflexivity journal to document methodological decisions, emerging assumptions, and analytic uncertainties. This record served as an audit trail and contributed to trustworthiness by making the analytic process transparent and reproducible [25].

International Journal of Core Engineering & Management
Volume-8, Issue-02, 2025 ISSN No: 2348-9510

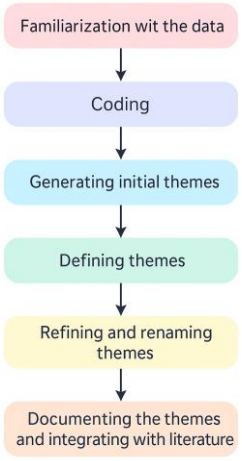

Fig. 3. Six-Phase Reflexive Thematic Analysis (Braun & Clarke)

Figure 3 visualizes the six-phase reflexive thematic analysis framework used in this study, adapted from Braun and Clarke's model. The process included familiarization with the data, coding, generating initial themes, defining themes, refining and renaming themes, and documenting the themes while integrating them with existing literature. The vertically aligned flowchart offers a color-coded depiction of how analytic depth was developed through iterative interpretation. This figure reinforces transparency and helps readers understand the recursive structure that underpinned the analytic process used in this research.

V. TRUSTWORTHINESS AND ETHICAL CONSIDERATIONS

To ensure methodological integrity, the study adopted Lincoln and Guba's trustworthiness framework as the foundation for evaluating qualitative rigor. This framework comprises four essential criteria: credibility, dependability, confirmability, and transferability. Each was operationalized through specific strategies during the research design, data collection, and analysis phases [20]. These criteria were selected for their alignment with interpretivist research and their widespread acceptance in information systems and organizational research involving human participants [21].

Credibility was established by ensuring that the research design accurately represented the perspectives of expert participants. This was achieved through prolonged engagement with the data, detailed memoing during transcription and coding, and the triangulation of participant responses through iterative question refinement. The use of inductive and deductive coding also contributed to credibility by enabling data-driven insights while maintaining alignment with the study's conceptual framework [22]. Thick descriptions and verbatim quotations were prepared during the reporting phase to enhance authenticity, though not included in this paper.

Dependability was addressed by maintaining a systematic audit trail of research activities. This included timestamped memos, coding logs in ATLAS.ti, and reflective notes written during and

after each interview session. All analytic decisions—from theme formation to exclusion—were documented to allow external reviewers or future researchers to trace how conclusions were reached. The structured five-phase design also reinforced procedural consistency across participants [23].

Confirmability focused on avoiding investigator's bias and ensuring that findings emerged from the data rather than personal assumptions. Reflexivity was practiced throughout the project by maintaining a journal that captured methodological choices, evolving interpretations, and uncertainties encountered during coding. These records were periodically reviewed against the coded data to maintain alignment with participants' perspectives [24]. Use of qualitative software further enabled traceability by linking each analytic code to its corresponding raw data extract.

Transferability was supported through deliberate participant selection and the provision of contextual detail about participants' organizational settings, roles, and expertise in SaaS implementation. While generalization was not the study's objective, capturing a diverse range of perspectives allowed for conceptual transferability to similar enterprise security environments. The inclusion and exclusion criteria ensured that all participants had relevant and recent experience with SaaS architecture and security concerns [25].

Ethical rigor was maintained by following formal institutional protocols for human subjects research. All study procedures were reviewed and approved by the Institutional Review Board of the University of the Cumberlands. Participants received an information sheet outlining the purpose of the study, voluntary participation, and data confidentiality protocols. Signed informed consent was obtained prior to each interview. Pseudonyms were used in interview transcripts to protect identities, and real participant names were avoided to maintain confidentiality. Data were anonymized during transcription and stored on a secure, password-protected drive. Access was limited solely to the researcher, and no identifiable information was retained in the final dataset [18], [26].

By applying these strategies, the study established a transparent, replicable, and ethically grounded process suitable for future qualitative investigations in cloud security contexts.

VI. LIMITATIONS AND FUTURE METHODOLOGICAL RECOMMENDATIONS

As with all qualitative studies, this research was subject to certain methodological limitations that may affect the scope and generalizability of its findings. While the study was designed to ensure rigor through reflexive thematic analysis and trustworthiness protocols, limitations related to sampling, researcher positioning, and analytic boundaries must be acknowledged to support transparency and future replication [20].

One key limitation was the use of expert purposive sampling. Although this strategy enabled the recruitment of highly experienced participants, it inherently limited the diversity of perspectives by focusing exclusively on individuals involved in SaaS implementation and security governance. The results of the study are therefore contextually bound and may not fully reflect the views of broader organizational roles or industries outside the participants'

experience [21]. Future studies could address this limitation by incorporating a more heterogeneous sampling frame, such as stratified purposive or maximum variation sampling, to capture a wider range of professional viewpoints.

Another limitation relates to the scope of the research questions and interview framework. The study prioritized depth over breadth by focusing specifically on architectural security concerns within enterprise SaaS implementations. While this facilitated rich data collection within a defined focus area, it limited exploration of adjacent factors such as end-user training strategies or post-deployment auditing practices, which could be relevant in a more expansive enterprise context [22]. Future methodological extensions could incorporate follow-up interviews or organizational case studies to deepen context-specific interpretation.

The study's interpretivist stance also introduces limitations related to subjectivity and reflexivity. Although reflexive journaling and analytic traceability measures were maintained, the interpretation of participant narratives remains influenced by the researcher's academic background and theoretical lens. However, to strengthen confirmability and reduce potential bias, the research design and coding strategy were reviewed by the dissertation chair, the full doctoral committee, the university's writing center, and the Institutional Review Board's quality team [23], [26], [27].

In addition, the study relied on synchronous virtual interviews as the sole data collection method. While this medium facilitated accessibility and scheduling, it may have constrained the depth of rapport or nonverbal context compared to in-person interviews [24]. Incorporating asynchronous follow-up methods such as participant reflections or diary-based engagement could support greater depth and flexibility in future designs.

Finally, the study adhered to the scope and ethical constraints approved by the Institutional Review Board of the University of the Cumberlands. This ensured methodological soundness but may have limited certain adaptive techniques such as longitudinal tracking or mixed-methods triangulation. Future research could explore extended timelines or integrated data modalities to enrich qualitative depth while upholding ethical safeguards [25], [26], [27].

By acknowledging these limitations and offering directions for future methodological refinement, the study supports ongoing replication and improvement of qualitative inquiry into SaaS security challenges within enterprise contexts.

VII. CONCLUSION

This paper presented a rigorously structured qualitative research methodology designed to investigate security challenges in enterprise SaaS environments. Grounded in an interpretivist paradigm, the study employed a five-phase exploratory research design supported by expert sampling, reflexive thematic analysis, and established trustworthiness protocols. Each stage of the process—from research question development to data analysis—was systematically aligned with the principles of qualitative inquiry and tailored to the context of cloud security research.

The study demonstrated how Braun and Clarke's six-phase reflexive thematic analysis could be implemented in a replicable and ethically grounded manner. Key methodological choices,

including the use of ATLAS.ti software, dual-mode coding strategies, and reflexivity journals, contributed to the analytic transparency and reliability of the findings. The structured application of Lincoln and Guba's trustworthiness criteria further enhanced credibility, dependability, confirmability, and transferability, providing a foundation for methodological rigor consistent with interpretivist standards [20], [28].

The approach detailed in this paper illustrated how methodological depth was achieved without compromising transparency or procedural clarity. By documenting the complete research process—including data collection, participant selection, coding logic, and ethical safeguards—the study provided a blueprint for researchers aiming to examine complex, socially embedded phenomena within enterprise technology contexts. The emphasis on methodological reflexivity and auditability supported future applications in adjacent domains, including cybersecurity governance, digital transformation, and organizational resilience in cloud environments.

This methodological contribution was developed and implemented as part of the author's doctoral dissertation at the University of the Cumberlands. The full study was reviewed and approved by the dissertation chair, committee, university writing center, and the Institutional Review Board quality team, ensuring the research adhered to academic, ethical, and methodological standards [26], [27].

By providing a transparent and transferable methodological framework, this paper offered a replicable design that can inform future qualitative studies investigating information systems challenges in dynamic and security-sensitive enterprise settings.

REFERENCES

1. J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed. Thousand Oaks, CA, USA: SAGE Publications, 2018.
2. L. H. Hennink, I. Hutter, and A. Bailey, Qualitative Research Methods, 2nd ed. London, U.K.: SAGE Publications, 2020.
3. V. Braun and V. Clarke, "Using thematic analysis in psychology," Qual. Res. Psychol., vol. 3, no. 2, pp. 77–101, 2006.
4. N. K. Denzin and Y. S. Lincoln, The SAGE Handbook of Qualitative Research, 5th ed. Thousand Oaks, CA, USA: SAGE Publications, 2018.
5. Y. S. Lincoln and E. G. Guba, Naturalistic Inquiry. Beverly Hills, CA, USA: SAGE Publications, 1985.
6. V. Braun and V. Clarke, Thematic Analysis: A Practical Guide. Thousand Oaks, CA, USA: SAGE Publications, 2021.
7. J. A. Maxwell, Qualitative Research Design: An Interactive Approach, 3rd ed. Thousand Oaks, CA, USA: SAGE Publications, 2013.
8. M. B. Miles, A. M. Huberman, and J. Saldaña, Qualitative Data Analysis: A Methods Sourcebook, 4th ed. Thousand Oaks, CA, USA: SAGE Publications, 2020.

9. J. W. Creswell and C. N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 4th ed. Thousand Oaks, CA, USA: SAGE Publications, 2018.
10. M. Q. Patton, Qualitative Research and Evaluation Methods, 4th ed. Thousand Oaks, CA, USA: SAGE Publications, 2015.
11. L. H. Hennink and N. Kaiser, "Sample sizes for saturation in qualitative research: A systematic review of empirical studies," Qual. Health Res., vol. 27, no. 4, pp. 591–608, 2017.
12. A. T. Cannon, S. R. Rosenthal, and R. T. Houston, "Expert sampling for applied qualitative research: Lessons from the field," Qual. Market Res., vol. 25, no. 2, pp. 240–256, 2022.
13. K. Charmaz, Constructing Grounded Theory, 2nd ed. Thousand Oaks, CA, USA: SAGE Publications, 2014.
14. C. Marshall and G. B. Rossman, Designing Qualitative Research, 6th ed. Thousand Oaks, CA, USA: SAGE Publications, 2016.
15. J. Saldaña, The Coding Manual for Qualitative Researchers, 3rd ed. Thousand Oaks, CA, USA: SAGE Publications, 2016.
16. C. Seidman, Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences, 4th ed. New York, NY, USA: Teachers College Press, 2013.
17. A. Strauss and J. Corbin, Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 2nd ed. Thousand Oaks, CA, USA: SAGE Publications, 1998.
18. B. D. Miller, "Protecting human subjects in qualitative research," Qual. Health Res., vol. 14, no. 3, pp. 377–387, 2004.
19. V. Braun, V. Clarke, and D. Hayfield, "Thematic analysis," in Handbook of Research Methods in Health Social Sciences, P. Liamputtong, Ed. Singapore: Springer, 2019, pp. 843–860.
20. A. Gibbs, "Analyzing qualitative data," in The SAGE Encyclopedia of Social Science Research Methods, M. S. Lewis-Beck, A. Bryman, and T. F. Liao, Eds. Thousand Oaks, CA, USA: SAGE Publications, 2004, pp. 13–17.
21. B. Tracy, Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact, 2nd ed. Hoboken, NJ, USA: Wiley-Blackwell, 2019.
22. N. King and C. Horrocks, Interviews in Qualitative Research, 2nd ed. London, U.K.: SAGE Publications, 2016.
23. D. Silverman, Doing Qualitative Research, 5th ed. Thousand Oaks, CA, USA: SAGE Publications, 2017.
24. L. Yardley, "Demonstrating validity in qualitative psychology," in Qualitative Psychology: A Practical Guide to Research Methods, J. Smith, Ed., 3rd ed. London, U.K.: SAGE Publications, 2015, pp. 257–272.
25. J. Morse, "Critical issues in qualitative research methods," in Qualitative Nursing Research, 2nd ed., Thousand Oaks, CA, USA: SAGE Publications, 1995, pp. 315–329.

26. S. S. Boda, Exploring Software as a Service Security Architecture Challenges and Considerations, Ph.D. dissertation, University of the Cumberlands, Williamsburg, KY, USA, 2024. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Y097WfQAAAAJ&citation_for_view=Y097WfQAAAAJ:u-x6o8ySG0sC
27. Institutional Review Board Quality Assurance Committee, "IRB standards and review protocol," Univ. of the Cumberlands, Williamsburg, KY, USA, Internal Report, 2024.
28. V. Clarke, "Reflexive thematic analysis: A practical framework for qualitative researchers," presented at the Qualitative Research Conference, 2021.