DST481

Research Methodology

Kamogelo Phiri(577418)

Belgium Campus iTversity

Introduction

The methodology chapter describes the research design, the theoretical basis for research, the collection of data, analysis, and ethical aspects of this dissertation. Because this study is a theoretical and best-practice study of cybersecurity for IoT, it does not conduct primary experiments or develop systems because it is studying cybersecurity regarding IoT from both theoretical and best-practice perspectives. This is a systematic literature review (SLR) method to review, analyse, and synthesize existing academic contributions, ensuring transparency, reliability, and replicability, and aligning with the goals of the dissertation to explore the security challenges, strategies, and frameworks of IoT. (Derek Cabera, 2023)

Research Design

A qualitative, exploratory research design based on a thorough analysis of scholarly literature is suitable since:

- IoT security is a rapidly evolving field, requiring synthesis of multiple perspectives.
- The aim is to evaluate **theories, strategies, and best practices** rather than to test new algorithms or build systems.
- The qualitative design allows critical reflection on gaps, limitations, and future directions in IoT cybersecurity research.

The design is structured around thematic coding of studies into categories aligned with dissertation chapters:

1. IoT Architecture & Security Issues
2. Threats & Attack Vectors
3. Cybersecurity Strategies (encryption, anomaly detection, protocols)
4. Security Frameworks & Regulations
5. Gaps & Challenges in Research

Research Approach

Given that cybersecurity knowledge is context-specific and is created as humans interact with each other, develop policies and build technology, this dissertation adopts an interpretivist philosophy and a constructivist lens.

Since this study moves between conceptual frameworks and previous research, the study takes an abductive approach rather than a pure inductive (build theory) or deductive (test theory) approach, enabling the study to address IoT security from a technical, legal, and social perspective.

Research Strategy

The research methodology is a Systematic Literature Review (SLR) that follows the guidelines for structured reporting and selection as outlined in PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). (Rafael Sarkis-Onofre, 2021) Keywords like: *"IoT security," "lightweight encryption IoT," "IoT anomaly detection," "secure IoT communication protocols," and "resource-constrained devices."*

The stages of the SLR are as follows:

1. **Identification** – Gathering articles from peer-reviewed journals and conference proceedings across databases (IEEE Xplore, SpringerLink, ScienceDirect, MDPI, Wiley).
2. **Screening** – Removing duplicates and excluding studies older than 2020 or not peer-reviewed.
3. **Eligibility** – Reviewing abstracts to confirm relevance to IoT cybersecurity.
4. **Inclusion** – Finalising sources aligned with themes (20+ papers selected).

IoT cybersecurity could be studied using a variety of research designs, including surveys, case studies, and controlled experiments, but the Systematic Literature Review (SLR) was determined to be the most suitable. Alongside response bias and the challenge of obtaining a sizable and representative sample of IoT professionals from various industries limit the usefulness of surveys and questionnaires in assessing expert or user perspectives, they can still be helpful. Contrarily, case studies offer in-depth understandings of a single theme or system, but their conclusions are frequently context-specific and not generally applicable. Although controlled experiments are useful for testing prototypes or algorithms, they necessitate a substantial infrastructure and technical implementation that is outside the purview of this study

By contrast, the SLR approach enables the researcher to synthesise evidence from a wide body of peer-reviewed studies published over the past five years, ensuring the findings reflect the state-of-the-art in IoT cybersecurity. It provides a structured and reproducible process for evaluating diverse strategies (e.g., lightweight encryption, anomaly detection, blockchain frameworks), allowing comparisons across multiple fields. Moreover, the use of PRISMA ensures transparency, minimizes researcher bias and enhances the reliability of the review. This range and systematic care make the SLR particularly suited to answering the dissertation's central research question without requiring direct experimentation or organisational access.

Data Analysis and Collection

Standards, book chapters and peer-reviewed articles published in the previous five years were the only secondary sources from which data was gathered. Data will be systematically collected from reputable academic sources; for e.g., IEEE Xplore, Springer, ScienceDirect, Wiley, and MDPI etc.

Following the SLR process, this will be documented in a PRISMA flowchart to show the transparency.

1. Identification

Records identified through database searching (n = 90)

Additional records identified through other sources (n = 0)

----

2. Screening

Records after duplicates removed (n = 70)

Records screened (n = 70)

Records excluded (n = 25)

----

3. Eligibility

Full-text articles assessed for eligibility (n = 45)

Full-text articles excluded, with reasons (n = 15)

----

4. Included

Studies included in qualitative synthesis (n = 30)

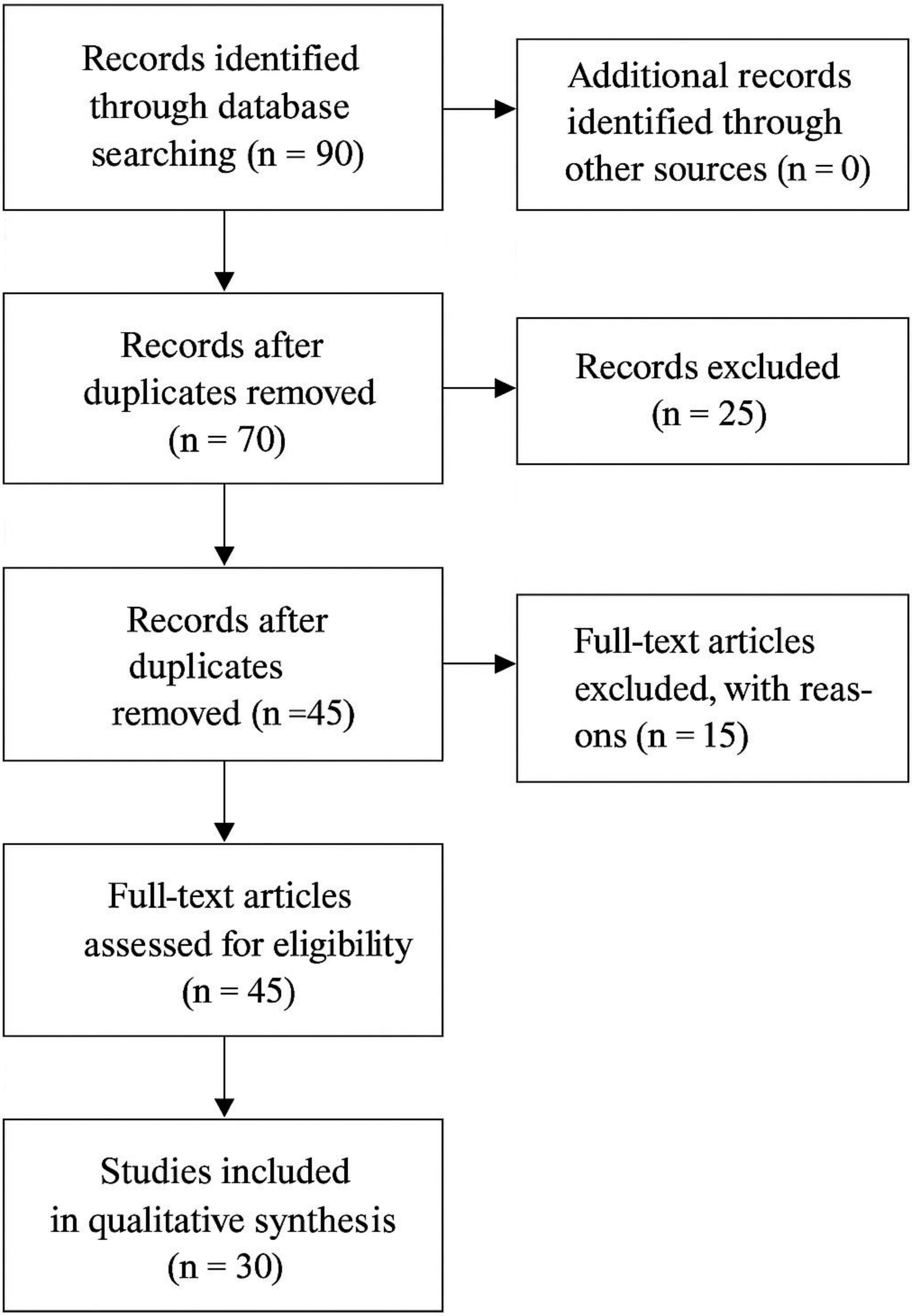
Records identified through database searching (n = 90)
Additional records identified through other sources (n = 0)
Records after duplicates removed (n = 70)
Records excluded (n = 25)
Records after duplicates removed (n =45)
Full-text articles excluded, with reasons (n = 15)
Full-text articles assessed for eligibility (n = 45)
Studies included in qualitative synthesis (n = 30)

Figure 1: PRISMA Flowchart

Inclusion Criteria:

- Published between 2020– current year
- Peer-reviewed journal or conference paper
- Direct relevance to IoT cybersecurity
- Written in English
- Accessible in full text

Exclusion Criteria:

- Grey literature (blogs, news articles, non-peer-reviewed reports)
- Studies unrelated to IoT (general cybersecurity only)
- Duplicate publications

Analysis

The data will be analysed using **thematic coding** to identify recurring security issues, proposed solutions, and gaps. The thematic coding process is as follows:

1. **Initial coding:**

- Read through each paper carefully.
- Highlight or note down key points related to your research question (e.g., "IoT encryption issues," "anomaly detection approach").
- Each of these points becomes a short label summarizing a concept, papers/concepts can be under the same label.

2. **Categorization:**

- Group similar codes together into broader categories.
- Example: Codes like "lightweight AES encryption," "blockchain-based encryption," and "energy-efficient encryption" can be grouped under the category "Encryption strategies."

3. **Theme development:**

- Identify overarching patterns or insights that emerge from the categories.

- Example: From the Encryption strategies and Protocol efficiency categories, there could be a theme like “Trade-offs between security strength and resource efficiency in IoT devices.”

4. **Analysis & reporting:**

- Use these themes to summarize findings, discuss trends, gaps, best practices, and support your conclusions.
- You can also tabulate quantitative results (like encryption times or detection accuracy) alongside these themes for more robust comparison.

Where possible, **quantitative measures** reported in studies (e.g., encryption time, detection accuracy, latency rates) will be in table format for cross-study comparison.

Validity, Reliability and Trustworthiness

To strengthen validity, multiple measures were applied:

- **Triangulation** – Using at least five credible sources of (IEEE, Springer, MDPI, ScienceDirect, Wiley). Most article sources
- **Recency Filter** – Only including studies from the past five years.
- **Peer Review Filter** – Ensuring quality and reliability of data sources.
- **Transparent Methodology** – PRISMA framework ensures replicability.

Consistent screening and documentation of inclusion/exclusion criteria supported reliability, and an audit trail will be maintained throughout the research process, including detailed documentation of search queries, inclusion and exclusion decisions, and synthesis of findings, ensuring that the research can be reproduced by others and that best practices in SLR methodology are being followed.

Ethical Considerations

Although the study does not involve human participants, ethical considerations remain critical. They include:

- **Academic Integrity** – Correct citation of all sources to avoid plagiarism.
- **Respect for Intellectual Property** – Using only licensed, accessible academic papers.
- **Anti-Plagiarism Software** – Final dissertation will be checked for originality in compliance with institutional requirements.

Methodology Limitations

This methodology is limited by:

- **Exclusion of grey literature** (which may contain industry best practices).
- **Publication bias** – Studies with negative results are less likely to be published.
- **Rapidly evolving field** – Some findings may become outdated quickly. For example (Amandeep Singh Sohal, 2018) is a way older article than (Olukunle Oladipupo Amoo 1, 2023), but it helps creates a foreground to the updated paper written by another author
- **Dataset unavailability** – Limits empirical testing of ML-based strategies.

Conclusion

It is justifiable to use an SLR because it offers both breadth and depth, and conclusions are not restricted to a single environment, dataset, or case, whereas experimental methods may be costly and require infrastructure, and surveys may not capture technical details but merely perceptions. It is a great way to directly address the research objectives in a saleable and evidence-based manner.

This methodology, which is based on interpretivism and abductive reasoning, used systematic literature review, triangulation and recency filtering to validate data that were collected through structured database searches and thematic analysis. This methodology ensures the dissertation can achieve its objectives to critically appraise IoT cybersecurity strategies, identify gaps, and present future research directions.

References

Cabrera, D., Cabrera, L. and Cabrera, E. (2023). The Steps to Doing a Systems Literature Review (SLR). *Journal of Systems Thinking Preprints*, 23(3). doi: https://doi.org/10.54120/jost.pr000019.v1

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S. and McGuinness, L.A. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *British Medical Journal*, 372(71). doi: https://doi.org/10.1136/bmj.n71

Sarkis-Onofre, R., Catalá-López, F., Aromataris, E. and Lockwood, C. (2021). How to Properly Use the PRISMA Statement. *Systematic Reviews*, [online] 10(1). doi: https://doi.org/10.1186/s13643-021-01671-z