A Systematic Literature Review Protocol for Access Control in the Internet of Medical Things (IoMT) Data and Services

Fahmida Hossain
Faculty of Information Technology,
Monash University, Melbourne, Victoria, Australia.
Email: fahmida.hossain@moansh.edu

March 17, 2025

1 Rationale

In recent years, the use of IoT devices has been rising exponentially across various application domains, including the healthcare sector [1]. The **I**nternet of **M**edical **T**hings (IoMT) is experiencing a similar surge in development and usage due to their need for remote medical interventions, improved data-driven clinical decisions, demand from healthcare professionals for enhanced monitoring, education, and care plan implementation[2]. Then, IoMT's influence in current medical research, disease management, drug administration and relative education has further facilitated their growth [3].

The IoMT systems deal with sensitive and personal data. Hence, their effectiveness, reliability, robustness and acceptance largely depend on their capability to handle security and privacy-related challenges [4]. An appropriate access control mechanism for IoMT systems can ensure authorized access to data and services, especially preserving privacy and integrity [5]. However, to our knowledge, no rigorous review was conducted considering the contexts (i) IoMT, (ii) Access Control, and (iii) Data and Services. Therefore, we plan to perform a **S**ystematic **L**iterature **R**eview (SLR) focusing on access control in IoMT data and services to gain a comprehensive understanding of the current state and future needs of these integrated fields. The SLR will be beneficial in the following key ways:

- It will allow us to systematically review the existing literature on IoMT access control data and services, ensuring a comprehensive, unbiased review based on established SLR guidelines [6].
- It will enable a thorough understanding of the existing methods, strategies and technologies currently being used for access control in IoMT data and services.
- It will help identify limitations in this integrated domain and determine areas that require further exploration and improvement.
- It will lead to a journal publication, contributing to the body of knowledge for the community audiences.

Conducting an SLR on access control in IoMT data and services will offer a compact but comprehensive view of the current state, challenges, and future directions in relative aspects, ultimately contributing to more efficient healthcare systems for their users.

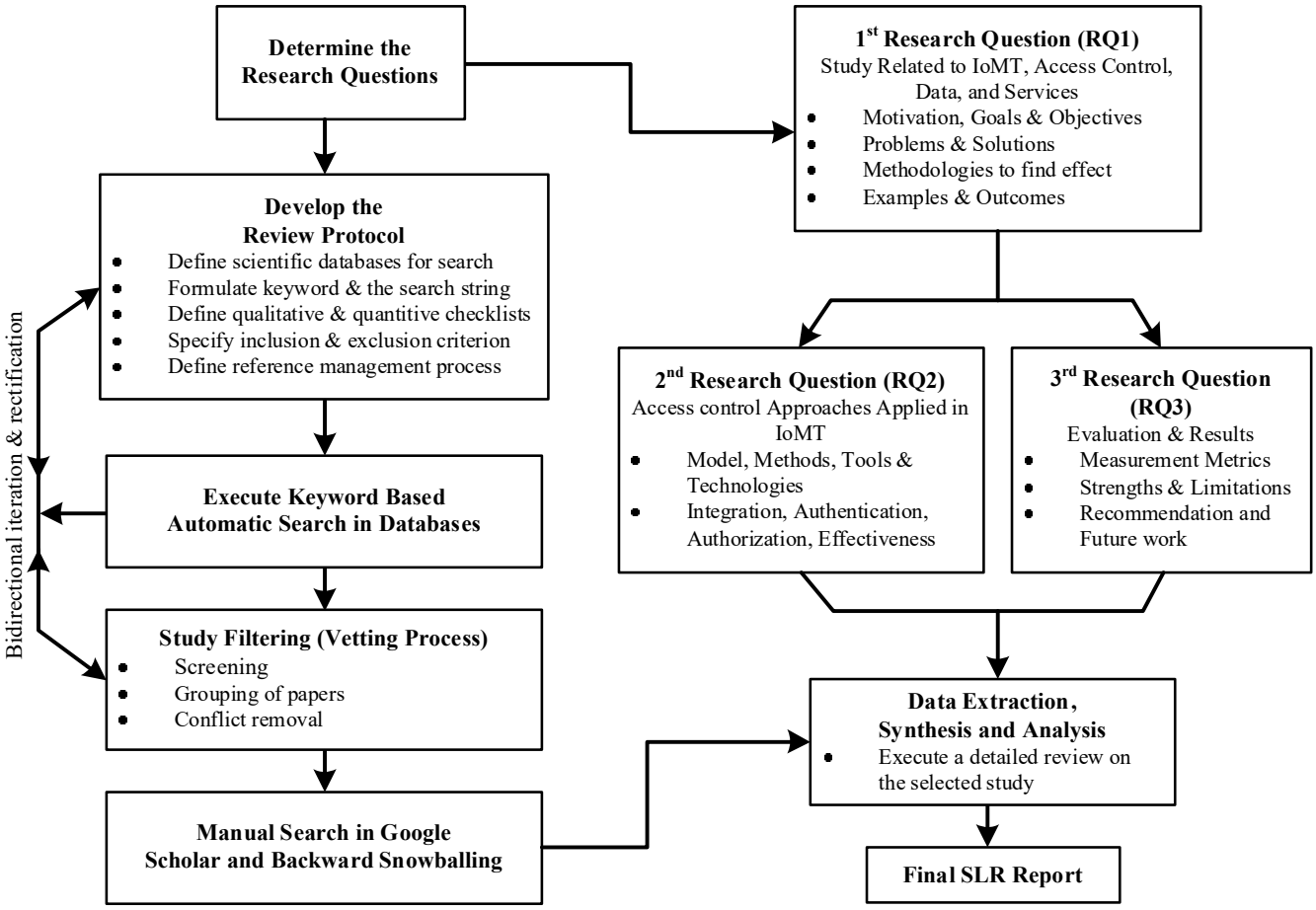

Figure 1: Architectural block diagram for this SLR

2 Research Methodology, Research questions and PICOC

A high level workflow diagram of this SLR is shown in Figure 1 following the guidelines provided by Kitchenham et al. [6]. In this work, our objective is to analyze existing research on the 'why' and 'how' access control mechanisms impact the overall IoMT system, its deployment, and usage, particularly in the context of data and services. We are also interested in identifying what research gaps exist in these integrated domains. To achieve this, we have formulated three key **R**esearch **Q**uestions (RQs). We used the work from Petticrew et al.[7] and adapted it according to **I**nformation **T**echnology (IT) taxonomies[6] to define the **P**opulation, **I**nterventions, **C**omparison, **O**utcomes, and **C**ontext (PICOC) of this SLR, as shown in Table 1. This PICOC guides the formation of RQs for this SLR as follows:

RQ1 What are the goals and objectives of access control approaches in IoMT data and services?

SubRQ$_{1A}$ What motivated the research in each study?
(Motivation, examples, scenario, societal needs, technological advancements, regulatory changes)

SubRQ$_{1B}$ What are the goals and objectives of each research paper reviewed?
(What they want to achieved in the paper)

Table 1: PICOC for this SLR

Population	The literature on IoMT, Access Control, Data and Services
Intervention	Access control method, policy, tool, technology, device
Comparison	Comparison among interventions for analysis
Outcomes	The consequence of access control for IoMT data and services
Context	**Include:** Access control approaches specifically for IoMT with a data and service component. **Exclude:** Explicitly IoT access control approaches, enhancements of the access control process, Malware identification, approaches not specifically designed for IoMT, research not including data and service components, approaches not accessible in English, general cybersecurity topics not focusing on access control, and theoretical proposals without implementation or evaluation.

SubRQ$_{1C}$ What problems do the studies solve, and what benefits do they offer?
(Usually for the target users, manufacturer, medical practitioner and service provider)

SubRQ$_{1D}$ What are the methodologies used by the researchers to identify the effect of access control in IoMT data and services?

SubRQ$_{1E}$ What are the types of examples used by the researchers in their studies?
(Target, system domain, academic and industry)

SubRQ$_{1F}$ What are the final outcomes of the study?
(The outcomes of a study can include one or more of the following: framework, guidelines, method, techniques, tools, models, platform, evaluations results of an access control approach)

RQ2 What access control approaches have been applied to IoMT data and services?

SubRQ$_{2A}$ What specific access control models exist?
(Types of access control models applied in IoMT e.g., DAC, MAC, RBAC, ABAC)

SubRQ$_{2B}$ What technologies and tools have been used for implementation?
(Applied technologies, languages, tools, platforms to implement the access control mechanism)

SubRQ$_{2C}$ How have these access control mechanisms been integrated with existing systems?
(Integration approach of access control mechanisms with the current environment)

SubRQ$_{2D}$ What types of authentication and authorization have been applied?
(Password-based, Two-Factor, Biometric, Certificate-based, Token-based authentication; Role-Based, Attribute-Based, Discretionary, Mandatory Access Control Authorization Methods)

SubRQ$_{2E}$ How effective have these approaches been in maintaining the security and privacy of IoMT data and services?
(Efficiency and acceptance)

Table 2: Concepts and search terms explanation

Main Terms	Supportive Search Terms
Concept 1(Co1): IoMT	Healthcare IoT (HIoT), Medical devices, Connected medical devices, Wearable medical devices, Connected health devices, Medical sensors, Healthcare sensors, Medical monitoring devices, Healthcare monitoring devices, Medical telemetry devices, Health telemetry devices, Medical cyber-physical systems (MCPS), Healthcare cyber-physical systems (HCPS), Medical embedded systems, Health embedded systems.
Concept 2 (Co2): Access Control	Authorization, Authentication, Security policy enforcement, Permission management, User permissions, Identity and Access Management (IAM), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC), Multifactor Authentication (MFA), Biometric Authentication, Access Governance, Access Management, Access Rights, Access Privileges, Access Restrictions, Access Enforcement.
Concept 2 (Co3): Data and Services	Information, Resources, Assets, Service-Oriented Architecture (SOA), Data Management, Data Governance, Data Security, Data Privacy, Data Protection, Data Confidentiality, Data Integrity, Data Availability, Data Storage, Data Transmission.

RQ3 How have the approaches been evaluated and what results have been obtained?

SubRQ$_{3A}$ What metrics have been used to measure performance and effectiveness?
(This can include security metrics, efficiency metrics, discussion on the reported results)

SubRQ$_{3B}$ What are the primary strengths, challenges, and limitations reported?
(Identified strength, drawbacks, limitations, or challenges that came up during the evaluations)

SubRQ$_{3C}$ What potential solutions or improvements have been suggested to overcome the identified challenges and limitations?
(Discussions on proposed enhancements, mitigation strategies, or future research directions to address these challenges and limitations)

SubRQ$_{3D}$ What are our recommendations for future work in this area?
(Understanding the implications of the findings, what can be done, and our future works)

3 Search strategy

We developed a strategy to search for papers that target Access control in IoMT data and services. The goal is to find as many primary study papers as possible. Our strategy consisted of three parts: search string identification, automatic search in electronic database and snowballing using google scholar. We identified relevant primary studies for this SLR were identified based on the RQs defined in Table 1. With the assistance of the PICOC approach (Table 1), our search terms were divided into three primary concepts, as shown in Table 2. These concepts helped us to set a well-formulated search string as shown below:

'IoMT' OR 'Healthcare IoT' OR 'Medical devices' OR 'Connected medical devices' OR 'Wearable medical devices' OR 'Connected health devices' OR 'Medical sensors' OR 'Healthcare sensors' OR 'Medical monitoring devices' OR 'Healthcare monitoring devices' OR 'Medical telemetry devices' OR

'Health telemetry devices' OR 'Medical cyber-physical systems' OR 'Healthcare cyber-physical systems' OR 'Medical embedded systems' OR 'Health embedded systems") AND ("Access Control' OR 'Authorization' OR 'Authentication' OR 'Security policy enforcement' OR 'Permission management' OR 'User permissions' OR 'Identity and Access Management' OR 'Role-Based Access Control' OR 'Attribute-Based Access Control' OR 'Mandatory Access Control' OR 'Discretionary Access Control' OR 'Multifactor Authentication' OR 'Biometric Authentication' OR 'Access Governance' OR 'Access Management' OR 'Access Rights' OR 'Access Privileges' OR 'Access Restrictions' OR 'Access Enforcement") AND ("Data and Services' OR 'Information' OR 'Resources' OR 'Assets' OR 'Service-Oriented Architecture' OR 'Data Management' OR 'Data Governance' OR 'Data Security' OR 'Data Privacy' OR 'Data Protection' OR 'Data Confidentiality' OR 'Data Integrity' OR 'Data Availability' OR 'Data Storage' OR 'Data Transmission'

4 Selection of papers: Inclusion and exclusion criterion

Tables Table 3 and Table 4 present the **I**nclusion **C**riteria (IC) and **E**xclusion **C**riteria (EC) that have been used to identify the studies of this SLR, respectively.

Table 3: Inclusion criteria

ID	**Detail Criterion**
IC_1	Full text of Conference papers, Journal articles and Book chapters that comply with three concepts defined in Table 2.
IC_2	Entire papers are written in English and use references.
IC_3	Studies that propose a solution or partial solution for access control in IoMT, including design, model, development, guidelines and tools.
IC_4	Papers available in an electronic format i.e., doc, docx, pdf, HTML, ps.

Table 4: Exclusion criteria

ID	**Detail Criterion**
EC_1	Gray literature, workshop articles, posters, books, work in-progress proposals, key notes, editorial, secondary or review studies, vision papers with no concrete implementation.
EC_2	Discussions papers and opinion papers, as well as Surveys that do not include any solution defined is IC_3
EC_3	Short papers less than three pages, irrelevant and low quality studies that do not contain considerable amount of information to extract
EC_4	Papers discussing on IoT or similar terms but not regarding IoMT and access control e.g., bug fixing
EC_5	Access control without relevant IoMT, beyond the scope, no real work or implementation
EC_6	Conference or workshop papers if an extended journal version of the same paper exists.
EC_7	Papers with inadequate information to extract (Irrelevant Papers).
EC_8	Non-primary studies (Secondary or Tertiary Studies).
EC_9	Papers about access control but not use IoMT as point of concern.

5 Quality assessment

We used a 1-to-5 numeric score – Very Poor, Inadequate, Moderate, Good, and Excellent – **Q**uality **C**hecking (QC) applied to each study using following eight questions (QC_1 to QC_8).

QC_1: Is the study highly relevant to the research and concepts defined in Table 1 and Table 2.

QC_2: Does the study clearly explain the methodology that accomplishes its goals?

QC_3: Does the study provide sufficient information on data collection, prototyping and/or algorithms used?

QC_4: Does the study adhere to data privacy and security in the context of IoMT?

QC_5: Does the study detail how it has validated or evaluated its results, e.g., through user studies, experiments, simulations, or theoretical proofs?

QC_6: Is there a clear outcome and results analysis reported?

QC_7: Are study limitations and possible future work adequately described?

QC_7: What is the citation count and quality of the venue where the study was published?

QC_8: Are the implications and significance of the research findings discussed in the study?

QC_9: Is the study's writing and presentation clear and understandable?

QC_{10}: How much is the work presented in the study practically usable?

6 Qualitative information to be extracted from each paper

We extracted the following a set of key information items from each primary selected paper, forming its **Q**ualitative **I**nformation (QI):

QI_1: Publication detail – Authors, title, demographics, year, venue, citation count, publisher.

QI_2: What is the motivation/goal of this study?

QI_3: What is the benefit of this study in the context of IoMT?

QI_4: What type of IoMT devices or systems are considered in the study?

QI_5: What access control mechanisms does the study explore or propose?

QI_6: What is the domain of the study (e.g., healthcare, homecare, hospital management)?

QI_7: Who are the target end users of the approach presented in the paper?

QI_8: What are the final outcomes of the study?

QI_9: What specific IoMT data types or services are addressed in the study?

QI_{10}: What access control models or frameworks are used in the study?

QI_{11}: How are the proposed solutions implemented (e.g., hardware, software platforms, protocols)?

QI_{12}: What are the performance metrics considered in the study for evaluating the proposed solutions?

QI_{13}: What methodologies are used for testing and validating the proposed solutions?

QI_{14}: What are the results and findings of the evaluations?

QI_{15}: How does the study deal with issues related to data transmission, storage, data privacy, security and availability in IoMT?

QI_{16}: How does the study address the unique challenges of IoMT, such as real-time data processing, device heterogeneity, scalability, etc.?

QI_{17}: What are the strengths and contributions of the study?

QI_{18}: What are the limitations or drawbacks of the study?

QI_{19}: What are the proposed solutions or future directions to address these limitations or challenges?

QI_{20}: What are the implications of the study for practitioners and researchers?

QI_{21}: Does the study provide any tools, datasets, or other resources for the community?

QI_{22}: What are the metrics used for the evaluation of the proposed IoMT solutions or access control mechanisms?

QI_{23}: What are the research gaps and future challenges/opportunities reported in the study?

7 Data Synthesis

Quantitative data synthesis will be carried out to find patterns and trends in the research, such as the percentage of studies that employ existing frameworks versus those that devise their own solutions for IoMT. This analysis will cover factors such as the number of studies published per year, the types of IoMT devices or systems investigated, and the various access control mechanisms proposed, among other relevant data obtained from the studies.

Important findings that are reasonable highlighting to the wider research community will be presented as qualitative data. This might include noteworthy papers from each domain (IoMT, Access Control, and Data and Services), which will be discussed in detail. For instance, we will identify intriguing correlations, major discoveries, gaps in current research, and any particularly innovative or effective solutions proposed in the selected studies studies as per the workflow discuss earlier (shown in Figure 1.

References

[1] A. Chowdhury, G. Karmakar, J. Kamruzzaman, The co-evolution of cloud and iot applications: Recent and future trends, in: Handbook of Research on the IoT, Cloud Computing, and Wireless Network Optimization, IGI Global, 2019, pp. 213–234. doi:https://doi.org/10.4018/978-1-5225-7335-7.ch011.

[2] G. J. Joyia, R. M. Liaqat, A. Farooq, S. Rehman, Internet of medical things (iomt): Applications, benefits and future challenges in healthcare domain, J. Commun. 12 (4) (2017) 240–247. doi:http://dx.doi.org/10.12720/jcm.12.4.240-247.

[3] S. Razdan, S. Sharma, Internet of medical things (iomt): Overview, emerging technologies, and case studies, IETE Technical Review 39 (4) (2022) 775–788. doi:http://doi.org/10.1080/02564602.2021.1927863.

[4] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. Tsatsoulis, Review of security and privacy for the internet of medical things (iomt), in: 2019 15th international conference on distributed computing in sensor systems (DCOSS), IEEE, 2019, pp. 457–464. doi:http://doi.org/10.1109/DCOSS.2019.00091.

[5] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, D. Lymberopoulos, A survey on security threats and countermeasures in internet of medical things (iomt), Transactions on Emerging Telecommunications Technologies 33 (6) (2022) e4049. doi:https://doi.org/10.1002/ett.4049.

[6] B. A. Kitchenham, S. Charters, Other Keele Staffs, Guidelines for performing systematic literature reviews in software engineering (version 2.3), Tech. rep., Keele University and Durham University Joint Report (2007).
URL https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

[7] M. Petticrew, H. Roberts, Systematic reviews in the social sciences: A practical guide, John Wiley & Sons, 2008.
URL https://doi.org/10.1002/9780470754887