

Digital Forensics in Internet of Things (IoT) Ecosystems

Towards a Comprehensive Framework for Digital Evidence Acquisition, Preservation, and Analysis



MD Monsuruzzaman | 2504658



MSc Cyber Security and Digital Forensics



University of Wales Trinity Saint David



ACCA7004 Research Methods and Professional Development



Dr. Suresh Shanmugasundaram



10th August 2026



Background

Internet of Things

Billions of connected devices



Smart homes



Healthcare



Smart cities



Industry 4.0



Challenges



Cyber attacks



Distributed evidence



Volatile data



Cloud storage



Multiple devices

Why Digital Forensics?



Incident investigation

Identify timeline, source and impact of incidents



Evidence collection

Gather digital evidence from diverse and distributed sources



Legal admissibility

Ensure evidence integrity and support court proceedings

Research Problem



Challenges



Heterogeneous
devices



Cloud
computing



Edge
computing



Proprietary
hardware



Lack of standard
framework



RESEARCH GAP

No comprehensive forensic investigation framework exists for heterogeneous IoT ecosystems.

Research Aim & Objectives

Research Aim

Develop a **conceptual digital forensic investigation framework** for IoT ecosystems.

Objectives

01



Literature
Review



02



Identify
Challenges



03



Compare
Frameworks



04



Develop
Framework

Literature Review

Existing Research

- ✓ IoT Forensics
- ✓ Cloud Forensics
- ✓ Edge Forensics
- ✓ AI
- ✓ Blockchain

Research Gap

- ✗ Limited validation
- ✗ Lack of interoperability
- ✗ No standard framework
- ✗ Domain specific
- ✗ Insufficient integration

Comparison Matrix

Frameworks	Validation	Interoperability	Scope	Standardization	Integration	Real-world Applicability
IoT Forensics Framework [A]	✓	✗	✓	✗	~	~
Cloud Forensics Framework [B]	✓	✗	✓	~	~	✓
Edge Forensics Framework [C]	~	✗	~	✗	~	~
AI-based Approach [D]	~	~	✓	~	✗	~
Blockchain-based Approach [E]	~	✗	~	~	~	✓
Proposed Framework (This Study)	✓	✓	✓	✓	✓	✓



Addressed / Good



Partial / Limited



Not Addressed / Poor

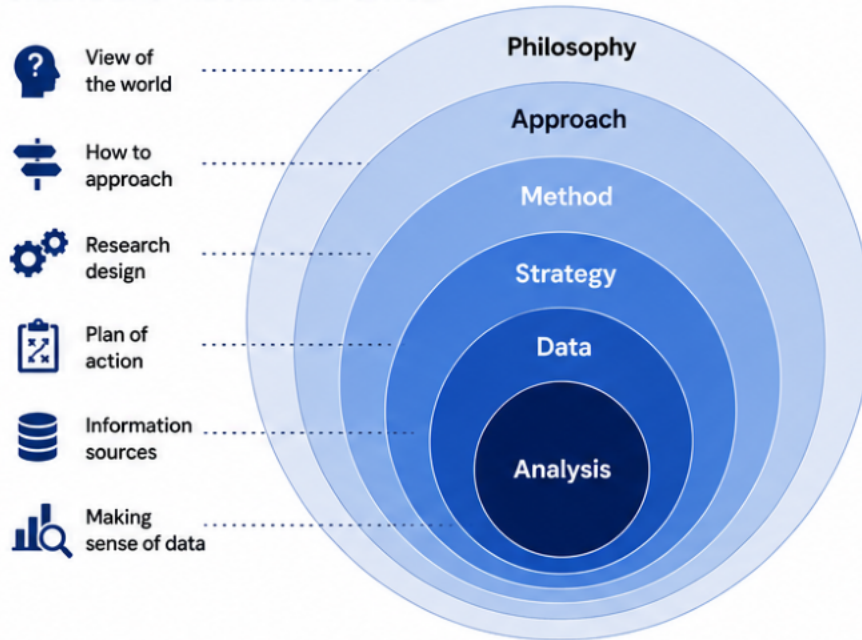


Therefore,
New framework required.



Research Methodology

SAUNDERS' RESEARCH UNION

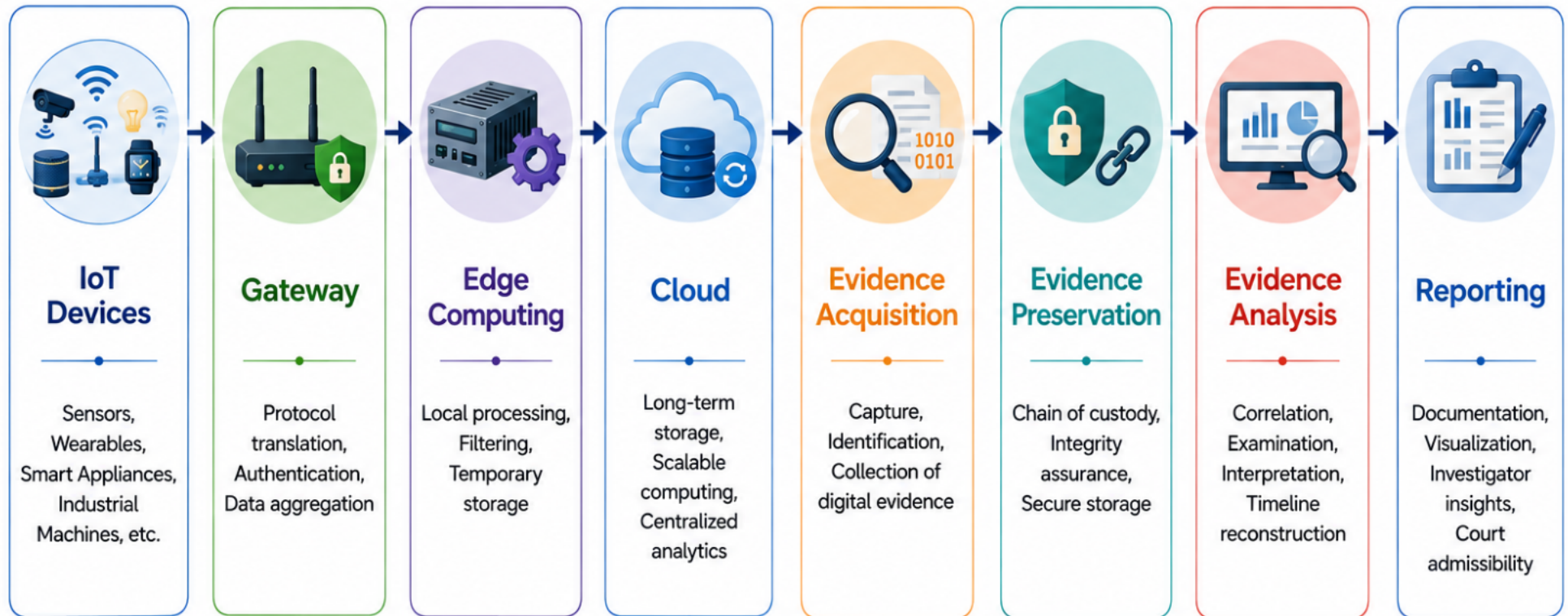


ITEM	SELECTION
 Philosophy	Positivism
 Approach	Deductive
 Method	Qualitative
 Strategy	SLR + Comparative Analysis
 Data	Secondary
 Analysis	Thematic Analysis

ACADEMIC DATABASES



Proposed Conceptual Framework



Expected Outcomes



ACADEMIC



Contributes to the body of knowledge in IoT forensics.



Provides a novel conceptual framework for research.



Opens avenues for interdisciplinary collaboration.



FUTURE RESEARCH



Provides a foundation for empirical validation.



Enables extension to specific IoT domains.



Encourages development of tools and datasets.



PROFESSIONAL & SOCIETAL



Supports investigators in handling IoT-related incidents.



Enhances digital evidence admissibility and reliability.



Strengthens cyber resilience in IoT ecosystems.



12-week research plan



Conclusion



- IoT creates new forensic challenges.



- Existing frameworks remain limited.



- Research addresses identified gap.



- Proposed framework supports future investigations.

Thank You

Questions?

