Marwadi University
Marwadi Chandarana Group

NAAC
A+

Major Project-I (01CE0716)

Review 2

(23/08/2025)

TITLE: Advance digital forensic investigation tool for iot device

Team ID: 7CE_082

Team Member 1: JEET JOSHI (92310103088) (TC1)

Team Member 2: HITEKSHA THAKER (92310103102) (TC4)

Guided By

Internal Guide Name: HANSA VAGHELA

Department of Computer Engineering,

Faculty of Engineering & Technology

OUTLINE

- Abstract
- Introduction
- Problem Statement
- Technical Features And Elements
- Working Of Forensic Tools
- Applications Of the forensic tool
- Advantages of the invention
- Result
- Flowchart of the investigations tool
- Research Paper
- Comparison
- Reference
- Conclusion

ABSTRACT

ABSTRACT

The sudden explosion of Internet of Things (IoT) devices particularly in today's homes has brought forth essential challenges around data security, digital privacy, and forensic traceability. Of all the devices, smart thermostats are particularly noted because they engage perpetually with user activity, environmental information, and remote access, which makes them vulnerable to cyberattacks and malicious access. This study introduces an Advanced Digital Forensic Investigation Tool for IoT Devices, with a special focus on smart thermostats, to tackle these new issues. The proposed tool is a modular, lightweight, and privacy-aware forensic framework for secure data acquisition, real-time monitoring, and intelligent evidence analysis. It combines the process of encrypted communication, anti-forensic resistance, and machine learning-based anomaly detection with captured data to ensure authenticity and integrity. The structuring of the tool is done to seamlessly operate within resource-constrained IoT settings and is cross-platform compatible for forensic investigators and security analysts. This paper presents a new solution that, in addition to enabling post-incident forensics, enables proactive forensic preparedness in IoT environments. The instrument enables legal admissibility of cyber evidence, meets privacy laws, and is easily extendible to many other IoT architectures beyond thermostats. Through the use of secure protocols, automated forensic capability, and modularity, this study fills the current gap between traditional forensics and the ongoing needs of intelligent environments.

Keywords: IoT forensics, smart thermostat, cybercrime investigation, forensic automation, digital evidence, anti-forensics, privacy-aware systems, real-time monitoring, forensic readiness

INTRODUCTION

INTRODUCTION

- The widespread use of **Internet of Things** (IoT) devices, such as smart home products, wearables, and connected cars, has created major challenges for digital forensics.
- These devices consistently generate, store, and send sensitive information.
- This data is crucial evidence in cases of cybercrime, fraud, and data breaches.
- The "**Advanced Digital Forensic Investigation Tool for IoT Devices**" project offers a specific forensic solution that can capture, analyze, and preserve digital evidence from various IoT environments.
- It supports common communication protocols like HTTP, which allows it to collect network traffic, logs, device settings, and interaction histories.
- By connecting traditional forensic methods with new IoT technologies, this system is a vital resource for modern forensic investigations.

PROBLEM STATEMENT

PROBLEM STATEMENT

- We are surrounded by devices that use the Internet of Things (IoT), a reality that has provided even more opportunities for cybercriminals to target us.
- IoT devices have limited storage, limited processing, limited security features, and have been vulnerable to manipulation, remote access, and tampering.
- A lot of digital forensic capabilities currently available to investigators (getting the evidence, storage and processing) cannot cope with the amount of devices in a decentralized, variable, and resource-poor IoT ecosystems.
- The IoT environment has made it difficult for investigators to come up with legally acceptable and secure methods to recover and process digital evidence from the smart devices.

TECHNICAL FEATURES AND ELEMENTS

TECHNICAL FEATURES AND ELEMENTS

- **Lightweight & Modular Form Factor:**

Designed for low-resource IoT devices. Allows for flexible and plug-and-play modules.

- **Real-Time Data Collection:**

Collects both volatile (RAM, processes in the process table), and non-volatile (logs, config, storage) data without impacting the operation of the device.

- **Chain of Custody:**

Digital logs are maintained which are digitally signed with a timestamp to show every step of evidence handling to support and ensure its legal admissibility.

- **Anomaly Detection:**

Incorporates Machine Learning modules built into the tool to identify suspicious, anomalous behavior in the IoT data.

- **Cross-Platform Compatibility:**

Supports several IoT operating systems such as Linux-based IoT OS, Android Things.

WORKING OF FORENSIC TOOLS

WORKING OF FORENSIC TOOLS

APPLICATIONS OF THE FORENSIC TOOL

APPLICATION OF FORENSIC TOOLS

Marwadi University
Marwadi Chandarana Group
NAAC A+

- Cybercrime Investigation
- Digital Evidence Collection
- Incident Response and Analysis
- Fraud Detection
- Data Breach Forensics
- Smart Home & Industrial IoT Monitoring
- Automotive Forensics
- Compliance & Regulatory Audits
- Academic and Research Use
- Connected Healthcare Device Monitoring

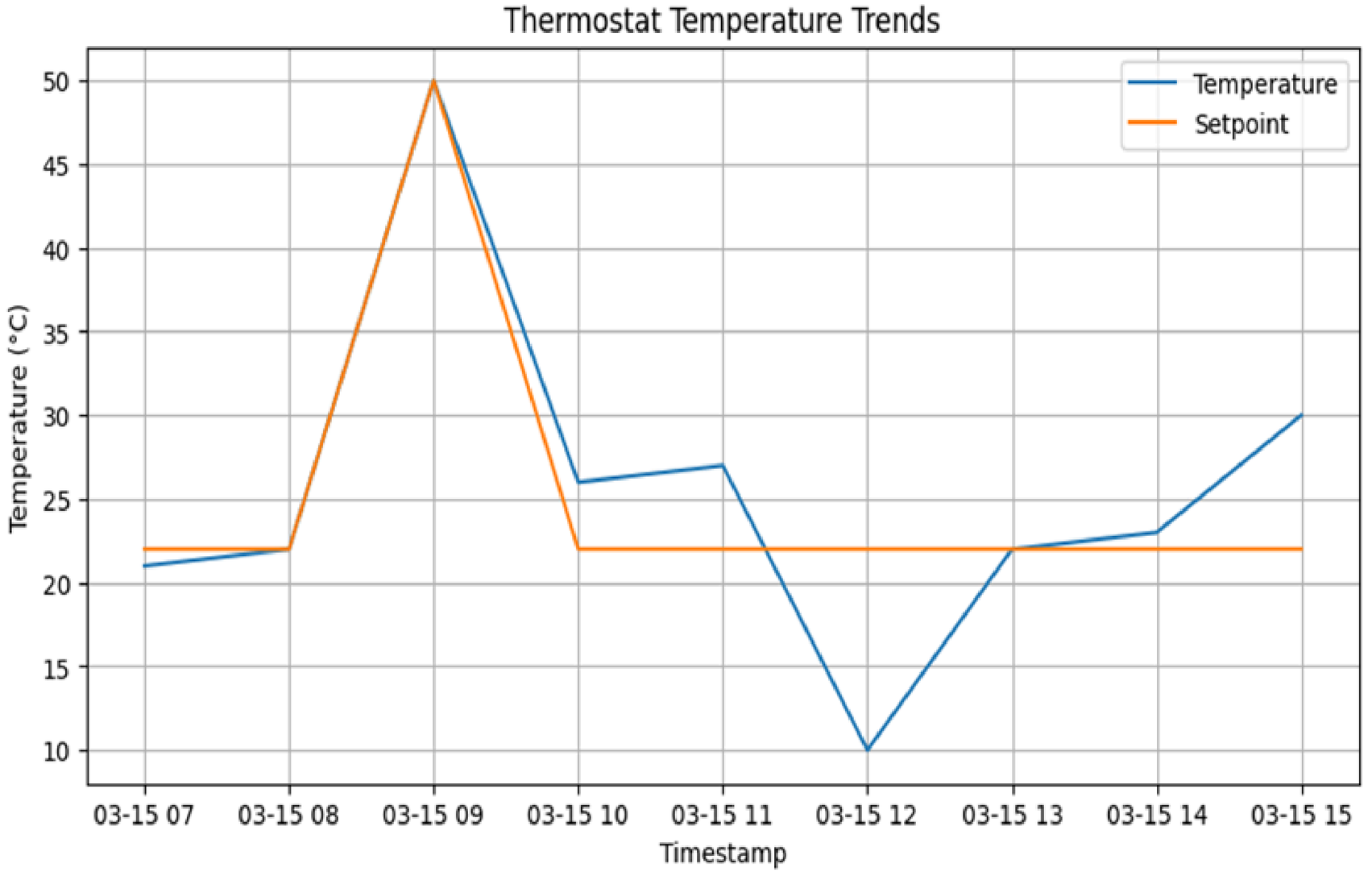
ADVANTAGES OF THE INVENTION

ADVANTAGES OF THE INVENTION

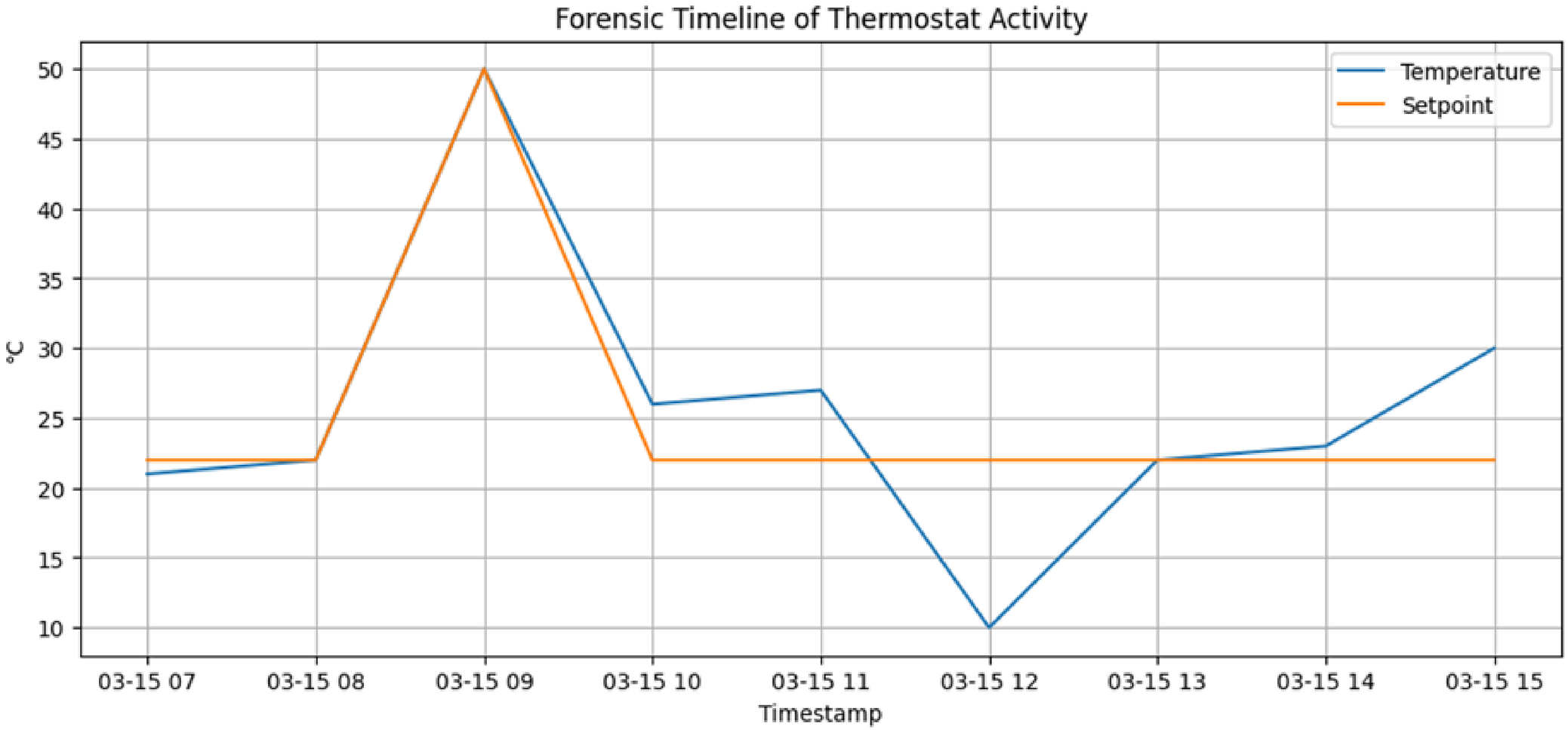
- High precision in evidence collection for transient IoT environments.
- Military encryptions strong enough to protect confidentiality, especially in dispute situations.
- Platform-independent, ready for future IoT technologies.
- Automates investigator workflows thanks to AI-based intelligence.
- Provides solid forensic readiness rather than waiting for a breach to passively react.

RESULT

RESULT OF THERMOSTAT TEMPRATURE TRENDS

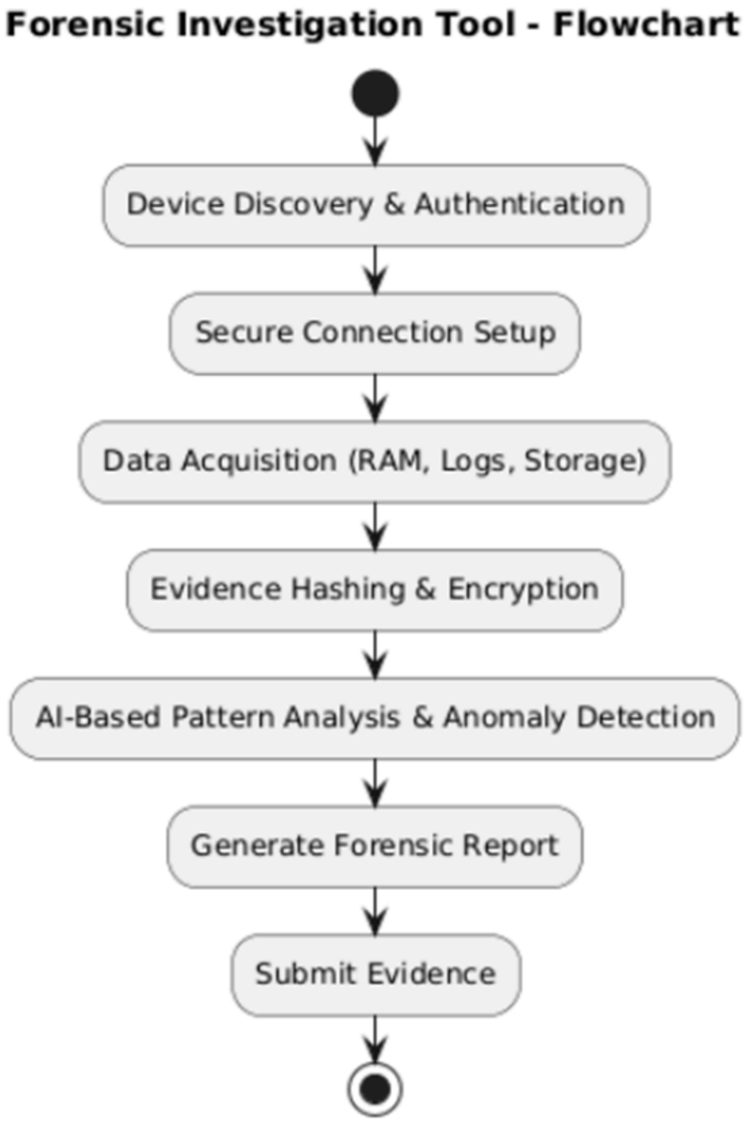


RESULT OF FORENSIC TIMELINE OF THERMOSTAT ACTIVITY



FLOWCHART

FLOWCHART OF THE INVESTIGATIONS TOOL



RESEARCH PAPER

REFERING RESEARCH PAPERS

Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations

LITERATURE REVIEW

Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations

Field	Details
Authors	Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Ali Chehab
Key Contributions	- Identifies and classifies digital forensics and anti-forensics techniques relevant to IoT. - Proposes Counter Anti-Forensics (CAF) using cryptographic and machine learning solutions. - Highlights the Internet of Forensics Things (IoFT) and Internet of Digital Forensics Things (IoDFT) as emerging frameworks for forensic readiness.
Advantages	- Comprehensive taxonomy of IoT digital forensics domains (cloud, mobile, network, computer). - Detailed evaluation of both anti- and anti-anti-forensics strategies. - Emphasizes privacy and evidence preservation.
Disadvantages	- Theoretical in nature; lacks real-world implementations or validation. - Challenges remain in applying anti-anti-forensics to resource-constrained IoT devices.
Proposed Tools	IoFT, IoDFT frameworks; Cryptographic methods (AES, HMAC); Machine learning-based detection (CNN, SVM); Conventional forensic tools (FTK, EnCase, Autopsy, Volatility, Wireshark).
Remarks	- Strong foundational review helpful for researchers and practitioners. - Recommends better investigator training, forensic education programs, and privacy-preserving protocols to address emerging IoT forensics needs

SUMMARY OF RESEARCH PAPER

Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations

Field	Details
Title	Advanced Digital Forensics and Anti-Digital Forensics for IoT Systems: Techniques, Limitations and Recommendations
Authors	Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Ali Chehab
Year	2022
Publication	*Internet of Things*, Elsevier
Methodology	Literature review of IoT forensics sub-domains (computer, network, cloud, mobile), analysis of anti-forensics and counter anti-forensics strategies; proposes IoFT/IoDFT frameworks
Advantages	Provides a comprehensive taxonomy of IoT forensics tools and challenges; introduces counter anti-forensics concepts; integrates multi-domain forensics approaches
Disadvantages	Theoretical; lacks experimental validation or real-world deployment; complexity in applying counter anti-forensics solutions on resource-constrained IoT devices
Remark	Serves as a strong foundational study for researchers and practitioners exploring IoT forensics; highlights the need for standardized forensic protocols and adaptive investigation techniques

REFERING RESEARCH PAPERS

Digital Forensics Analysis of IoT Nodes using Machine Learning

M Zeeshan Arshad1 , Hameedur Rahman2 , Junaid Tariq3 , Adnan Riaz4 , Azhar Imran4 , Amanullah Yasin4 and Imran Ihsan4

LITERATURE REVIEW

DIGITAL FORENSICS ANALYSIS OF IOT NODES USING MACHINE LEARNING

M ZEESHAN ARSHAD1 , HAMEEDUR RAHMAN2 , JUNAID TARIQ3 , ADNAN RIAZ4 , AZHAR IMRAN4 , AMANULLAH YASIN4 AND IMRAN IHSAN4

Author	Key Contributions	Advantages	Disadvantages	Proposed	Tools	Remarks
Hameed, S.	Reviewed IoT privacy and routing issues	Broad overview of threats	No forensic model provided	Security challenges analysis	Conceptual	Sets foundation for IoT vulnerabilities
Arıs, A.	Explored DDoS and IDS in IoT networks	Focused on MAC and attacks	Detection limitations	IDS approach	IDS concepts	Highlights attack surfaces in IoT
Kasinathan, P.	Developed Suricata-based IDS with Linux	Efficient for low-resource devices	Signature update issues	Lightweight IDS	Suricata	Suitable for constrained IoT setups
Fagbola, F. I.	Proposed forensic readiness model for IoT	Step-by-step, ISO-based	Basic and generic	Forensic structure	PSO-DL, ML	Useful for initial forensic readiness
Koroniotis, N.	Designed deep learning framework for forensics	High accuracy (98%)	Setup complexity	Particle Deep Framework	Tcpdump, Wireshark, PSO, DNN	Strong ML integration
Scheidt, N.	Introduced IoT device DNA identification	Easy attack tracing	Needs pre-registration	Device DNA model	Hybrid Forensic Server	Novel approach to device tracking
Patil, A.	Mapped forensic tools for modern systems	Covers various tech environments	Integration gaps	Tool discovery roadmap	General forensic tools	Pushes for tool advancement
Aslan, Ö. A.	Reviewed malware detection techniques	Covers ML and heuristics	Heuristics fail on complex threats	Detection models	Signature, Heuristic, ML	Informs attack classification methods

SUMMARY OF RESEARCH PAPER

DIGITAL FORENSICS ANALYSIS OF IOT NODES USING MACHINE LEARNING

M ZEESHAN ARSHAD1 , HAMEEDUR RAHMAN2 , JUNAID TARIQ3 , ADNAN RIAZ4 , AZHAR IMRAN4 , AMANULLAH YASIN4 AND IMRAN IHSAN4

Marwadi University
Marwadi Chandarana Group

NAAC A+

Field	Details
Title	Digital Forensics Analysis of IoT Nodes using Machine Learning
Authors	M. Zeeshan Arshad, Hameedur Rahman, Junaid Tariq, Adnan Riaz, Azhar Imran, Amanullah Yasin, Imran Ihsan
Year	2022
Publication	*Journal of Computing & Biomedical Informatics*, Volume 04, Issue 01
Methodology	A forensic analysis framework was proposed and implemented on IoT nodes (e.g., Raspberry Pi) under attack. The architecture involved a node-to-node (N2N) communication setup with redirected traffic to a logging server using IP tables and Snort rules. Logs were converted to datasets using CICFlowMeter and analyzed via machine learning algorithms (e.g., Decision Tree, Random Forest, Naïve Bayes). Accuracy was validated using standard ML metrics (Accuracy, Precision, Recall, F1-score).
Advantages	- Effective attack detection without overloading IoT devices- Logs are securely stored and used for ML-based detection- Decision Tree model achieved high accuracy (97.29%)- Real-time traffic analysis and alert generation
Disadvantages	- Limited to specific attack types and test scenarios- Accuracy drops with added hardware (e.g., Pi camera)- Dataset scope restricted to common IoT attacks
Remarks	The framework provides an efficient method for IoT forensic analysis, combining ML and forensic tools. It addresses memory and processing limitations of IoT devices and offers scalable potential. Future work could expand dataset variety and device support for better generalization.

COMPARISON

COMPARISON

Research Paper Comparison							
Criteria	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**
Focus	Forensics vs anti-forensics	IoT + secure communication	Comparison of forensic models	Digital trace capture in IoT	Privacy during IoT forensics	Existing digital forensic tools	Machine Learning-based forensic automation
Approach Type	Theoretical + Recommendation	Encryption with forensics	Model framework comparison	Technical trace analysis	Legal + ethical analysis	Comparative tool study	Predictive, data-driven forensic automation
Tools/Tech Used	Comparative analysis methods, file system forensic tools (wiping, timestamp)	Elliptic Curve Cryptography (ECC), secure key exchange, encryption protocols for forensic data transfer.	Frameworks: DFRWS model, NIST model, UAFM (Unified Analytical Forensic Model).	Techniques for trace capture, event logging, timeline analysis, lightweight monitoring tools.	GDPR, Privacy-by-Design, compliance-based frameworks, anonymization tools, ethical analysis methods.	FTK, Encase, Autopsy	Machine Learning algorithms: SVM (Support Vector Machine), KNN (K-Nearest Neighbor), Random Forests for anomaly detection and forensic automation.
Strengths	Covers both forensic & anti-forensic	Secure communication layer	Good overview of standards	Strong trace mapping	Privacy integration	Real tool usability	Adaptive & scalable forensic logic
Limitations	No tools, very broad	Less focus on tools	No implementation, just model	No tool proposals	Abstract + no tech stack	Not IoT-specific	Needs training data + compute
Suitability	Too generic	Security-focused, not forensic-heavy	Too model-oriented	Good context, but not actionable	Privacy first, not investigative	Good for baseline comparison	Best fit for intelligent forensic tool

REFERENCE

REFERENCE

Number	Research Paper
[1]	Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations
[2]	Advanced Digital Forensic IoT Based Secure Communication
[3]	IoT Forensic models analysis
[4]	IoT forensic challenges and opportunities for digital traces
[5]	IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations
[6]	Digital Forensics Tools Used in Cybercrime Investigation – Comparative Analysis
[7]	Digital Forensics Analysis of IoT Nodes using Machine Learning

CONCLUSION

CONCLUSION

The forensic tool being recommended can help significantly alleviate the shortfalls of traditional digital forensics in IoT situations. It provides safe, quick, low weighing evidence collection to enable data integrity and legal acceptability. This forensic tool is making use of encryptions, machine learning and malleable platforms to help provide higher accuracy and acceptability in investigations on smart devices for cyber crimes. This suggestion provides a framework for more scalable, smart and privacy-aware IoT forensics in today's digital world.

THANK YOU