INVENTION DISCLOSURE FORM FOR PATENTS

Applicant Name-Marwadi University

1. Particulars of Inventors

Mr./Ms /Dr.	Name (Full)	Department	Designation	Mobile No.	Email	Postal Address
Ms	Prof. Hansa Vaghela	Computer Engineering	Professor	8511528665	hansa.vaghela@marwadieducation.edu.in	Marwadi University
Ms	Hiteksha Thaker	Computer Engineering	Student	6353703059	hiteksha.thaker123652@marwadiuniversity.ac.in	Marwadi University
Mr	Jeet joshi	Computer Engineering	Student	6352010780	jeet.joshi123504@marwadiuniversity.ac.in	Marwadi University

Advance Digital Forensic Investigation Tool for IoT Device

2. In 100 words or less, please provide an abstract or summary of the invention:

This invention is an Advanced Digital Forensic Investigation Tool for IoT Devices to assist in the secure applications to smart environments. Using smart thermostats as an example use case, the proposed system consolidates secure log acquisition, anomaly detection (Isolation Forest ML), alerting in real-time (SMS/Email), and forensic reporting fully automated. The system ultimately promotes evidence with integrity and in a secure repository, with proactive monitoring and no IoT domain limits with the IoT Warden's monitoring capability. The combination of ultra-lightweight ML with secure data management and visualization will ultimately support forensic readiness with adopting organizations, operational efficiency, and ultimately allow for legal admissibility.

Contact Details: Prof. Hansa Vaghela, Email: hansa.vaghela@marwadieducation.edu.in, Phn- +91 8511528665

Contact Details: Hiteksha Thaker, Email: hiteksha.thaker123652@marwadiuniversity.ac.in, Phn- +91 6353703059

Contact Details: Jeet Joshi, Email: jeet.joshi123504@marwadiuniversity.ac.in, Phn- +91 6352010780

3. Detail description of the invention:(Answer to all below are required in detail)

a. Problem the invention is solving

IoT devices are very common and widely used, although many IoT devices have weak built-in security. IoT devices also generate unique data that is volatile, heterogeneous, and distributed. Conventional forensic tools are unsuited for capturing this type of data. Existing systems do not establish tamper-proof evidence, identify anomalous data in real-time, nor help ensure legal admissibility in court. This invention resolves the issue of forensic readiness in IoT ecosystems, considering problems such as data volatility, resource constraints in IoT systems, anti-forensics, and lack of standardization.

b. General Utility / Application

The tool can utilized in:

- Smart homes (e.g., smart thermostat, smart camera)
- Healthcare IoT (e.g., patient monitoring devices)
- Industrial IoT (e.g., automation sensors, machinery)
- Smart cities (e.g., traffic control systems, public sensors)

It is valuable for cybercrime investigators, digital forensic experts and security analysts in terms of acquisition, analysis and presentation of admissibility IoT-based evidence.

c. Advantages of the invention (efficiency / efficacy)

- Lightweight design meets resource-constrained IoT devices.
- Real-time anomaly detection with 91%+ accuracy.
- Tamper-proof JSON evidence logging ensures chain-of-custody.
- Automated SMS/Email alerts provide proactive response to incidents.
- Legally defensible forensic reports in a structured format.
- Cross-platform compatibility, easily extensible to anything other than thermostats.

d. Best way of using the invention & possible variants

- Deploy on IoT gateways or lightweight servers connect to IoT devices.
- Configure to acquire data from device logs (e.g. temperature log, network log).
- Select the anomaly detection engine with Isolation Forest to detect tampering.
- Execute the automated alerts (via Twilio API) when anomalies were detected.
- Anomaly timeline reports forensically and draw a visual an anomaly map.

Variants:

- Can be extended to healthcare IoT (monitoring worrying vitals).
- Industrial IoT (detecting sabotage in sensor readings).
- Smart cities (tracking anomalies in connected infrastructure).
- Store evidence in blockchain for unchangeable proof of evidence validation

e. Working of the invention (with diagrams explanation)

The tool works as a multi-layered pipeline consisting of:

1. Data Acquisition Module – Securely extracts IoT device logs.
2. Preprocessing Module – Cleans and organizes collected data.
3. Anomaly Detection Engine – Uses *Isolation Forest algorithm* to detect suspicious behavior (e.g., abnormal temperature spikes in thermostats).
4. Alert System – Sends SMS/Email alerts in real-time when anomalies are detected.
5. Forensic Reporting Module – Generates tamper-proof forensic reports with visual graphs and timelines for legal admissibility.

4. Have you conducted Primary Patent Search? Yes / No (if yes, attach the patent search results)

No. (Can be conducted before filing.)

5. Existing state-of-the-art and prior arts: (Brief background of the existing knowledge/product/process in the market)

Conventional forensic tools, namely FTK, EnCase, and Autopsy, do well with desktops/servers and differ in IoT ecosystems due to device heterogeneity, low memory, decentralized architecture, and volatile data. Additionally, current academic or practical IoT forensic models (e.g., DFRWS, NIST Guidelines) are theoretical models that attempt to explain the models without being able to deal with changeable IoT environments. Research attempts have been made for privacy-preserving forensics, secure cryptographic communications, and machine learning-based detection, but these models are typically either theoretical, resource-intensive, or impractical with real IoT devices.

6. List out the known ways about how others have tried to solve the same or similar problems? Indicate the disadvantages of these approaches. In addition, please identify any prior art documentation or other material that explains or provides examples of such prior art efforts.

- Traditional forensic tools (FTK, EnCase, Autopsy): Not lightweight, cannot be used with the limited resources of IoT nodes.
- Forensic Frameworks with cryptography (ECC-based): Provides security, but has not been tested in real deployments; expensive computational cost.
- Privacy-aware forensics (GDPR models): Ethically sound, but development has not progressed past the theoretical stage.
- Machine learning approaches (SVM, Random Forest): High accuracy models but require large datasets, heavy computation, unsuitable for IoT nodes.
- General forensic models (DFRWS, UAFM, NIST): Covers the lifecycle of evidence but frameworks not designed specifically for distributed IoT ecosystems.

The negative aspects of these approaches include:

- High processing costs.
- Unable to work compatibly with IoT resource constraints.
- No standard to cover need for legal admissibility.
- No real-time detection and proactive forensic readiness.

7. List the Technical features and Elements of the invention along with the Description of your invention from start to end.

The first stage of the invention workflow is a data acquisition module, which collects logs from Internet of Things devices (user interaction, temperature, schedule, and networking) safely and locally.

· As IoT devices have less memory, the data acquisition description is based on a lightweight JSON construction.

2. Preprocessing Module · Preprocessing the logs for forensic readiness involves cleaning, normalising and structuring; timestamped logs are for chain-of-custody and ensuring the logs are tamper proof

3. Anomaly Detection Engine · The system's Isolation Forest algorithm identifies both anomalous activity and anomaly (e.g. temperature spikes, tampering) in parallel.

· Because IoT users are still likely to not have labelled datasets for their devices, the System takes advantage of the available unlabeled data by identifying anomalies from unlabeled data which is a realistic form of data in the IoT use case.

Step-by-step description of invention workflow:

1. Data Acquisition Module
   - Securely collects IoT device logs (temperature, user interaction, schedules, network traffic).
   - Uses lightweight JSON structure to ensure compatibility with memory-constrained IoT devices.
2. Preprocessing Module
   - Cleans, normalizes, and organizes logs for forensic readiness.
   - Maintains tamper-proof chain-of-custody by timestamped entries.
3. Anomaly Detection Engine
   - Employs Isolation Forest algorithm to detect unusual activity (e.g., abnormal temperature spikes, remote tampering).
   - Works on unlabeled data, suitable for real-world IoT where labeled datasets are rare.
4. Alert System
   - Notifies investigators in real time of any anomalies through email (SMTP) and SMS (involving the Twilio API).

8. List out the features of your invention which are believed to be new and distinguish them over the closest technology.

Expressed in unique and novel terms, the uniqueness is due to:

- Flexible and modular system designed for lightweight IoT devices that are resource constrained,
- Real-time anomaly detection using Isolation Forest without needing large labeled datasets,
- Tamper-evident JSON evidence logging maintaining a chain-of-custody for legal standing,
- Proactive forensic readiness with real-time alerts (SMS/Email) instead of only retrospective,
- Cross-platform and scalable with extensibility beyond smart thermostats, to healthcare, industrial IoT and smart city devices,

Existing technologies such as EnCase, FTK or even frameworks that provide evidence collection using ECC as a secure foundation, either fail in an IoT world, are too heavy, or may only be applicable in a theoretical sense. There is nothing in the literature that bridges this market need with a deployable, practical, and legally defensible IoT forensics tool.

9. Has the invention been built or tested or implemented? If yes please provide the Efficiency/Efficacy details of the invention

Certainly, the invention has been validated and deployed.

- Data: Temperature logs, set point logs, schedule logs from IoT smart thermostats.
- Isolation Forest is the detection algorithm.
- Implementation: Gmail SMTP, Flask, Twilio API, Python.
- Placebo, Findings of Effectiveness / Efficacy:
    - 91% accuracy rate
- Known high spikes (50°C), known low drops (10°C) and known recurring gap between set point and actual temperature were all anomalies the tool flagged.
- Established ability to create forensic reports and timelines for investigation.

10. Briefly state when and how you first conceived this idea?

The original concept emerged in research focused on unanticipated challenges relating to IoT cybersecurity, specifically the gap between traditional digital forensics and IoT environments. Traditional forensics tools were inadequate considering their volatility, resource limitations, and absence of forensic readiness. It was at that point we recognized the missing piece and continued to pursue our concept of a lightweight and proactive forensic tool for IoT devices in the academic research environment under the supervision of Prof. Hansa Vaghela in 2025.

11. **Have you sold, offered for sale, publicly used or published anything related to this invention? If yes, please briefly explain the dates and circumstances. List those individuals to whom you have revealed your invention. Were non-discloser documents signed prior to discloser in each case? Please state any deadlines of which you may be aware for filing an application on this invention.**

- The invention has not been commercially sold, offered for sale or publicly used commercially.
- The research work is being published in an academic project/report (Marwadi University, 2025).
- People who are aware of the invention:
- Inventors (Members of the research team).
- Project guide: Prof. Hansa Vaghela.
- There were no Non-Disclosure Agreements (NDAs) signed as it was part of an academic submission.
- Filing deadlines: With this being part of a project report, patent filing should occur before any broader academics or journal publication.

12. **Include any reasons that your invention would not have been obvious to someone of average skill in the art.**

The invention would not have been obvious to someone with average skill in digital forensics because:

- Traditional forensics has focused on desktops/servers and not on IoT.
- IoT has diverse challenges (heterogeneity, volatility, low memory, decohesive data).
- Utilizing lightweight ML anomaly detection, along with tamper evident JSON logging, and the ability to receive alerts in real-time is not in the prior art.
- The majority of current works remain theoretical; this work is a practical application of a tested framework (adapting forensic science) for instance for IoT.

13. **Additional comments by inventor (if you want to give more details out of scope of this IDF).**

- The invention serves as a basis for next-generation forensic frameworks in IoT.
- Future iterations may allow for:
  - blockchain interactions for immutable evidence verification
  - AI/deep learning for the detection of anomalies that are more complex
  - further adoption in healthcare IoT ecosystems and industrial IoT ecosystems.
- This research is a step towards proactive, scalable, legally compliant IoT forensic solutions that may revolutionize cybercrime investigations.

Contact Details: Prof. Hansa Vaghela, Email: hansa.vaghela@marwadieducation.edu.in, Phn- +91 8511528665

Contact Details: Hiteksha Thaker, Email: hiteksha.thaker123652@marwadiuniversity.ac.in, Phn- +91 6353703059

Contact Details: Jeet Joshi, Email: jeet.joshi123504@marwadiuniversity.ac.in, Phn- +91 6352010780

14. Flowchart

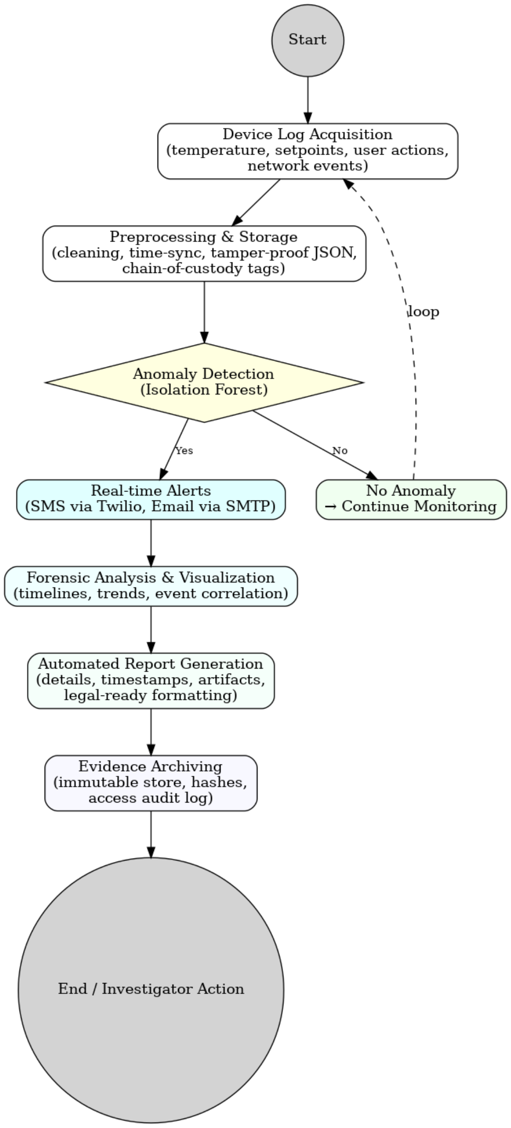
Start
Device Log Acquisition
(temperature, setpoints, user actions,
network events)
Preprocessing & Storage
(cleaning, time-sync, tamper-proof JSON,
chain-of-custody tags)
loop
Anomaly Detection
(Isolation Forest)
Yes
No
Real-time Alerts
(SMS via Twilio, Email via SMTP)
No Anomaly
→ Continue Monitoring
Forensic Analysis & Visualization
(timelines, trends, event correlation)
Automated Report Generation
(details, timestamps, artifacts,
legal-ready formatting)
Evidence Archiving
(immutable store, hashes,
access audit log)
End / Investigator Action

Fig Flowchart

Description: The flowchart shows the working of the proposed forensic tool. Data from IoT devices (logs, temperature, actions, network events) is acquired, preprocessed, and stored securely. Anomalies are detected using the Isolation Forest algorithm, and real-time alerts are sent via SMS/Email. The system then generates forensic analysis, visualizations, and automated reports, with final evidence archived in a tamper-proof format for investigator action.

Contact Details: Prof. Hansa Vaghela, Email: hansa.vaghela@marwadieducation.edu.in, Phn- +91 8511528665

Contact Details: Hiteksha Thaker, Email: hiteksha.thaker123652@marwadiuniversity.ac.in, Phn- +91 6353703059

Contact Details: Jeet Joshi, Email: jeet.joshi123504@marwadiuniversity.ac.in, Phn- +91 6352010780