HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Vol. 9, No. 1, (2025)

Digital Forensics and Investigation Framework for Industrial IoT (IIoT) Systems

Buthaina Al-Zadjali [a)], Setyawan Widyarto[*,b)]
*Corresponding author

(a) Sultanate of Oman, b.zadjali111@gmail.com, ORCID iD
(b) Department of Computing, Faculty of Communication, Visual Art and Computing, Universiti Selangor, Selangor, Malaysia, widyarto@unisel.edu.my, 0000-0002-6317-9875

Abstract: The increasing integration of traditional industrial systems with communication technologies in the Industrial Internet of Things (IIoT) has revolutionized industry efficiency. However, this interconnectedness exposes IIoT systems to cyber-based vulnerabilities. There is a lack of a systematic study method for IIoT forensics within existing research. This research investigates current methodologies and challenges in IIoT forensics and aims to propose innovative solutions for effective data collection, analysis, and interpretation within IIoT environments. The primary objective of this research is to propose a framework that can improve the forensic investigation process within the IoT environment. This research employs mixed methods, including a comprehensive literature review of current methods, barriers, and future directions for IoT forensic investigations. It also includes surveying IIoT systems in some organizations and devices to gain insights into their structure, data storage, communication protocols, and possible forensic obstacles. A case study will examine real-life scenarios involving IIoT systems in some organizations in Oman to understand the unique forensic obstacles auditors face. The study is intended to highlight the forensic approach to analysing IIoT systems. It will evaluate IoT forensics tools in terms of time complexity, reliability, ease of usability, and other parameters. The research seeks to contribute to a regulatory framework for Industrial IoT Security, particularly in Oman, and raise awareness about the use of IoT systems. The anticipated outcome is a framework that improves the forensic investigation process within the IoT environment

Keywords: Industrial Internet of Things (IIoT), Digital Forensics, Cybersecurity, Framework, Forensic Investigation

1. Introduction

The Industrial Internet of Things (IIoT) or Industry 4.0 refers to the application of the Internet of Things (IoT) in the industrial sector which is used to monitor, collect, exchange, process, and analyze data gained from industrial devices (Abbas et al., 2021). IIoT is one of the advanced, automated, and intelligent technologies that make use of smart sensors and actuators to enhance manufacturing and industrial processes and empower industries with self-organizing and self-optimizing capabilities via real-time monitoring and control of the production environment.

The IIoT has transformed the modern world and the future of technology-driven Industry 4.0, and these changes have led to a multitude of cybersecurity risks in industrial sectors (Gudlur* et al., 2020). Cybercriminals exploit vulnerabilities in IIoT systems to gain unauthorized access, compromise user privacy, and manipulate data. Due to unreliable machine-to-machine (M2M) communication should be considered the existence of cybersecurity issues threats and data breaches on the IIoT applications. Adopting a new technology will bring new

challenges to cybersecurity and expose vulnerabilities in terms of AI and BI applications and can used with forensic investigation and accuracy of information sharing between smart devices (Gudlur* et al., 2020).

The Industrial IoT (IIoT) has received the attention of researchers and businesses, which play a significant role in the conversion of commercial systems. Implementing IIoT in industrial sectors is intended to increase manufacturing efficiency and reduce device downtime, business productivity, and raise the caliber of the final output. IIoT devices characterized by the decentralization systems, variety of applications and schemes, diversity of data, and networking strain (Sasikumar et al., 2024).

The rapid deployment of IIoT technologies has introduced new challenges in ensuring the privacy and security of connected systems. The interconnected nature of these devices has created a complex cybersecurity landscape. The integration of AI and Blockchain technology has emerged as a potential solution in response to these challenges (Tyagi, 2023).

IIoT technology can be applied in various areas of the industrial sector for example in smart cars, Industrial wearable technology, smart communications, smart grid, smart industry, smart city, robotics, factory /manufacturing, transportation, health, and Agricultural farming. This is best illustrated in Figure 1. The figure presents various Industrial IoT (IIoT) Applications arranged around a central label. Each application is connected to the central term with a dotted line and accompanied by an icon. The applications include:

- Smart Car – Connected vehicles that use IoT for navigation, diagnostics, and automation.
- Industrial – Traditional industries utilizing IoT for automation, monitoring, and optimization.
- Smart Grid – IoT-enabled energy systems for efficient power distribution and management.
- Robotics – Use of interconnected robots in manufacturing and services for automation.
- Smart City – Urban infrastructure utilizing IoT for traffic control, surveillance, waste management, etc.
- Factory / Manufacturing – Smart factories using IoT for predictive maintenance, real-time analytics, and automation.
- Smart Communications – IoT used to enhance connectivity and data exchange in communication systems.
- Smart Utilities / Power – Monitoring and control of electricity, water, and other utilities using IoT.

The IIoT applications illustrate how IoT is integrated across various sectors to enhance efficiency, safety, automation, and data-driven decision-making in industrial environments.

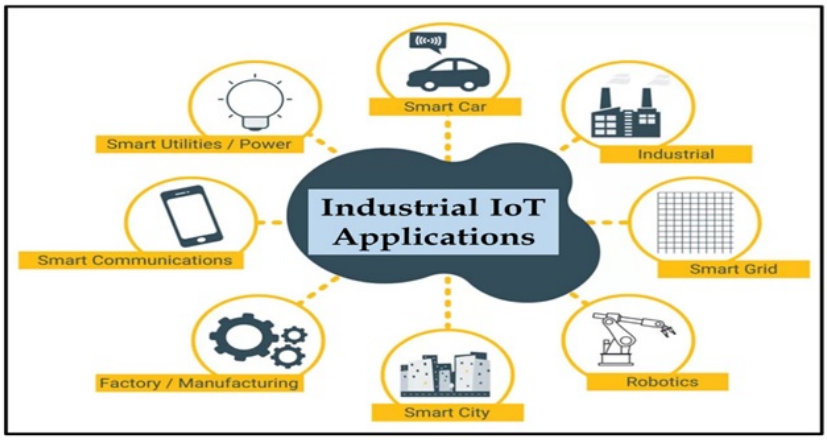

Figure 1. IoT application in the industrial sector

This research focuses on enhancing the investigation of digital forensics using IoT techniques in the industrial sectors of Oman to find solutions for detecting IoT systems by adopting specific rules and addressing any gaps that may affect the flow of systems in those areas.

1.1. Background

As mentioned earlier, individuals or groups hide behind IoT systems to perform malicious activities. Forensic examinations or investigations must be conducted to arrest and prosecute such individuals. The criminal justice system is designed to identify, monitor, deter, and prosecute crimes and criminals. In the digital world, the digital criminal justice system is no different from the traditional criminal justice system which includes law enforcement, courts, and corrections that operate at the same depth, providing greater accountability, engagement, and public trust in a virtual environment.

The developments in the digital age have led to the emergence of new types of criminal activity, which require the presence of skilled specialists to deal with these crimes, which also requires the justice system to adapt by developing policies and collecting digital evidence amidst complex challenges related to data storage and accessibility on various Internet of Things devices.

The Internet of Things (IoT) forensics can be described as a separate branch of digital forensics at the device, network, and cloud levels. The local memory of IoT devices can be examined for evidence, network log files can provide a scope of user activities if an IoT device's connection is compromised through a network, and the cloud becomes an important repository of IoT device data and can serve as potential evidence. IoT forensics can be particularly challenging due to issues of non-standardization, lack of historical data, and the fact that IoT devices are always connected (Lutta, 2024).

1.2. Problem Statement

The increasing integration of IoT technologies in industrial sectors in Oman has enhanced operational efficiency but has also introduced significant cybersecurity challenges. Industrial IoT systems, including smart sensors, automated machinery, and interconnected monitoring devices, generate huge amounts of sensitive data, making them prime targets for cyber threats. Unauthorized access, data manipulation, and system breaches pose substantial risks to business continuity, national security, and industrial safety.

Despite the growing reliance on IoT systems, the field of IoT forensics remains underdeveloped in Oman, with limited standardized frameworks and methodologies for investigating cyber incidents involving IoT devices. Traditional digital forensic techniques often fail to address the complexities of IoT environments, such as data volatility, device heterogeneity, and decentralized architectures. This gap in forensic capabilities hinders law enforcement and cybersecurity experts from effectively identifying attack vectors, tracing malicious actors, and mitigating cyber threats.

This research aims to enhance digital forensic investigations in IoT-driven industrial sectors in Oman by developing a specialized forensic framework tailored to IoT systems. The study will identify existing gaps in IoT forensic investigations, explore advanced methodologies for evidence collection and analysis, and propose solutions to strengthen security measures. By addressing these challenges, the research seeks to improve the effectiveness of forensic investigations, ensuring better detection, analysis, and response to cyber incidents in industrial IoT environments.

1.3. IIoT-Layered Architecture

Internet of Things (IoT) is a network device that includes sensors and software that connects to and exchanges data over the Internet. IoT Applications are used in various sectors, such as smart cities, healthcare, and agriculture. The Industrial Internet of Things (IIoT) is a subset of IoT focused on industrial sectors such as manufacturing, supply chain, and logistics, enhancing operational efficiency and safety. The IIoT-layered architecture is a framework used to describe the different components and functions of an IIoT system. The IIoT architecture consists of seven layers: application layer, device layer, data layer, decision layer, management layer, analytics layer, and communication layer.

In IIoT architecture, each layer is important for ensuring the security and functionality of the IIoT system. Understanding the IIoT-layered architecture is important for understanding the components and functions of the IIoT system, which helps to develop effective security strategies for these systems.

In IIoT system layers the device layer consist of physical IoT devices that generate and collects data, the data layer stores and manages the information, communication layer facilitates data exchange, application layer processes it for users, the analytics layer extracts insights, the decision layer makes informed choices based on those insights, and the management layer oversees the entire system.

When focusing on IoT Forensics, the exploration of IoT-layered architecture is important, which helps to understand the different components and how they interact with each other. This information is important to identifying the origin of a security breach or any other issue in the IIoT system. Security experts can better understand the possible attack vectors and ways to defend against them by understanding the different layers. In addition, the architecture provides a framework for understanding the flow of events and data in the system. It also provides a reference for developing and implementing appropriate forensics techniques and methods.

IIoT is crucial in industrial settings and supports the convergence of IT and operational technology (OT), as OT oversees communication with integrated machines. This makes IIoT forensics essential for leveraging incident-related data from its architecture.

Figure 2 shows the Industrial Internet of Things (IIoT) architecture divided into four main layers, with specific components and functions described at each layer. The relationship between IoT and IIoT and processes in Industry 4.0 are in a four-layer architecture. The perception layer is regarded as vulnerable; the network layer faces threats from CIA-based attacks, and the control layer manages industrial processes through programmable logic controllers (PLCs), human-machine interfaces (HMIs), and distributed systems. The application layer oversees these processes while being prone to encryption vulnerabilities in the cloud environment. Here's a textual breakdown:

1. Application Layer (Top Layer). This layer represents IIoT applications in various domains:

- Robotics
- Energy Efficiency
- Mining
- Transportation
- Remote Power Grid
- Heavy Machinery

It utilizes:

- Middleware

- Databases
- Processing/Analytics
- Device/Network Management
- Cloud Services

2. Control Layer. This layer is responsible for decision-making, coordination, and control. It includes:

- Control Algorithm – Executes control logic.
- Equipment Management – Manages devices and assets.
- Supervisory Control System – Supervises operations.
- Human Machine Interface (HMI) – Facilitates user interaction.
- Actions Management – Executes system responses.

3. Network Layer. This layer handles data transmission and communication across systems:

- Network Infrastructure
- Cloud Infrastructure
- Network Protection Methods – Includes encryption, authentication, and protocols like LoRaWAN, MQTT, CoAP.
- Security Protocols – Focused on secure access, encryption, and user verification.
- Edge Gateway – Enables local data processing and connectivity to cloud services.

4. Perception Layer (Bottom Layer). This foundational layer includes sensing and data collection technologies:

- Sensors
- Actuators
- Processors
- Transceivers
- Data Acquisition Devices

This layered architecture provides a clear view of how IIoT systems are structured—from physical devices and sensors to applications that drive automation and decision-making in industrial environments. Let me know if you'd like this turned into a written report or slide!

An IIoT architecture features three layers—perception, network, and application—that align with the seven-layer OSI (open systems interconnection) model, allowing for comprehensive forensics by integrating all layers and addressing IoT-specific challenges through techniques like log analysis, data recovery, and network traffic analysis, while ensuring proper protocols and standards to maintain data integrity for investigations.

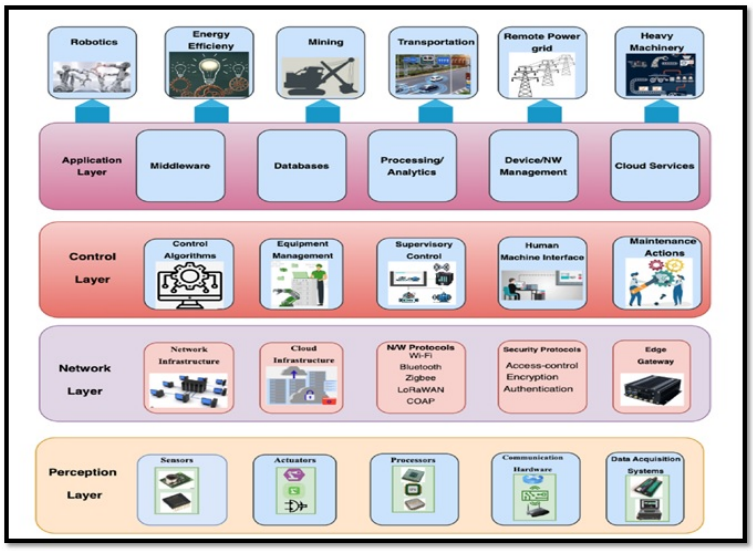

Figure 2. Figure 2: Layered IIoT architecture

1.4. IIoT-Forensic Processes

IIoT forensics is a subfield of digital forensics. The term "IIoT forensics" refers to the gathering, examination, and preservation of digital evidence from IIoT systems for use in administrative, legal, or security investigations. IIoT forensics aims to provide a comprehensive and accurate assessment of incidents and determine the cause and the steps taken to mitigate the risks. In IIoT forensics, the process involves several steps, identification of relevant digital evidence, evidence preservation, data collecting, data analysis, and findings presentation.

To the success of any IIoT forensics investigation, the proper handling of digital evidence is critical. The analysis of IIoT forensics data includes several techniques (log analysis, malware analysis, network forensics, and packet analysis). The investigation findings are used to support decision-making and to inform the development of security strategies and countermeasures.

When focusing on forensic investigations in the Industrial Internet of Things (IIoT), exploring forensic processes in the Industrial Internet of Things (IIoT) is crucial, as it provides a deeper understanding of the various stages and techniques used in investigating incidents occurring in the IIoT environment. The layered structure of the IIoT platform requires distinct forensic methods that go beyond traditional digital forensics platforms. Separating and reconnecting each layer in the Industrial IoT platform represents a critical transition that can lead to the mishandling and distortion of potential digital evidence

Researchers and practitioners can identify the challenges and limitations in current practices and develop more efficient and effective solutions for investigating incidents in the IIoT environment by understanding the IIoT forensics processes. Additionally, it helps to identify the requirements for standardization in IIoT forensics field to ensure the reliability, integrity, and consistency of the investigation results(Kebande & Ikuesan, 2025).

It is important to develop digital forensic models and systems that can support future investigative technologies. This is because during incident response, an attack, a potential security incident, and a disaster, have to be attributed to a potential perpetrator. The concept of digital forensics in IIoT suffers from a lack of accepted

policies, standards methodologies, and procedures that can define what a digital environment constitutes and how potential incidents can be handled in the wake of an attack.

2. Related Work

In this section, review existing literature and the related work on IIoT Forensics are reviewed and discussed. The review of existing literature helps to understand the current state of IIoT forensics research. This study provides the key challenges of IIoT forensics and proposes a framework to address them.

2.1. Standardization and Framework Development in IIoT Forensics

The lack of standardized forensic processes in the Industrial Internet of Things (IIoT) is a recurring concern in recent literature. Kebande and Ikuesan (2024) emphasize this gap in "Standardizing Industrial Internet of Things (IIoT) Forensic Processes", where they propose a taxonomy to guide forensic procedures and call for aligning IIoT forensics with existing standards in digital forensics and cybersecurity. Similarly, Kebande (2022) refers to IIoT forensics as a "forgotten concept" in the push for Industry 4.0, advocating for the development of a generic, standards-compliant forensic framework.

Molinaro and Wagner (2023) address forensic readiness in their guidelines for IIoT environments, focusing on practical aspects like data logging, verification, and reporting. They propose expanding the scope of these guidelines to encompass cloud forensics and suggest further validation by a wider range of experts.

2.2. Security Vulnerabilities and Blockchain Integration

Security in IIoT remains a significant concern, with several studies advocating for blockchain-based approaches. Awad and Kebande (2024) present a comprehensive analysis of IIoT ecosystems and underline the need for secure blockchain integration, particularly for smart contract execution and malicious node detection.

In line with this, Rathee et al. (2022) propose a trust-enhancing mechanism using blockchain to evaluate and exclude malicious devices from IIoT networks. Their model, validated via MATLAB simulations, demonstrates strong defense capabilities against various attack vectors.

Juma, Alattar, and Touqan (2023) extend blockchain applications to big data integrity in smart manufacturing. Their Trusted Consortium Blockchain (TCB) framework uses consensus protocols to validate and safeguard evidence in real time, enhancing fault tolerance in IIoT environments.

2.3. Forensic Toolkits and Evidence Collection Strategies

Justice et al. (2024), in a systematic review, assess forensic evidence collection in IoT environments. By employing tools such as IoTScent, Cellebrite, and Magnet AXIOM, they identify strategic gaps and propose the development of AI-driven frameworks to improve data integrity and investigative reliability. Their approach underscores the importance of accommodating device heterogeneity in forensic toolkits.

Shin et al. (2024) tackle the challenges of heterogeneous IoT environments, especially in smart homes, by using tools like NMAP, Binwalk, and PuTTy to address encrypted packet analysis and hardware access limitations. Their work calls for deeper focus on hardware-level forensics and adaptation of existing tools to non-uniform device infrastructures.

2.4. Performance, Scalability, and System Feasibility

Fitzpatrick and Thorpe (2024) examine the performance of Distributed Digital Ledger (DDL) technology in forensic contexts. Their quantitative study highlights the considerable processing overhead involved in encrypted IIoT transactions, pointing to scalability challenges as device volumes increase. Despite these constraints, they provide a replicable methodology for benchmarking DDL in digital forensics.

2.5. Intrusion Detection Systems and AI in IIoT Security

AI and machine learning are increasingly being explored for proactive forensic and intrusion detection applications. Sharma et al. (2024) introduce a transformer-based Intrusion Detection and Prevention System (IDPS) that achieves near-perfect anomaly detection accuracy. Tested on the UNSW-2018-IoT-Botnet dataset, the model demonstrates robustness across various traffic classifications, including subtle forms of DoS and DDoS attacks.

In a complementary effort, Shtayat et al. (2023) propose an ensemble deep learning model combining Convolutional Neural Networks (CNNs) and Extreme Learning Machines (ELMs). They further enhance interpretability using SHAP and LIME, thus addressing one of the critical limitations of traditional deep learning models—lack of transparency.

2.6. Opportunities and Challenges in Industry 4.0 and 5.0 Forensics

Nelufule, Masango, and Singano (2024) provide a macro-level overview of digital forensics in the context of Industry 4.0 and 5.0. Their mixed-method research highlights both opportunities and challenges arising from emerging technologies such as edge computing. They emphasize the development of adaptive frameworks and raise awareness about digital forensics among industry stakeholders.

Rathee et al. (2024) further this discourse with TrustNextGen, a proposed security mechanism aimed at enhancing trust and performance in next-gen IIoT environments. Through comparative simulations, their framework demonstrates higher accuracy and responsiveness, suggesting a promising direction for future developments in trust-aware IIoT systems.Kebande & Ikuesan, emphasize the critical need for standardized forensic processes in IIoT. The lack of such standards creates significant obstacles to effective investigations, especially as IIoT devices become increasingly prevalent in essential infrastructure. The authors propose a taxonomy of forensic processes specifically designed for the IIoT landscape. This taxonomy aims to categorize and clarify the various forensic processes that are necessary for effective investigations in IIoT environments and discusses the challenges and impacts of the current lack of standardization, as well as the roles that both industry and government can play in achieving these standards. This collaborative effort is essential for enhancing the overall effectiveness of IIoT forensics. The key findings of this research is the current IIoT suffers from relatively weak security protocols and a lack of unified accepted standards (Kebande & Ikuesan, 2025).

Kebande & Awad, in this research, present an in-depth analysis of the state-of-the-art in the IIoT ecosystem from security and digital forensics perspectives. The dimensions of this study are twofold: first, present an overview of the cutting-edge security of IIoT ecosystems, and second, survey the literature on digital forensics. The state-of-the-art survey has provided a comprehensive analysis of existing research, from which it is evident that the current IIoT suffers from relatively weak security protocols and a lack of unified accepted standards.

Together, these weaknesses make IIoT integration vulnerable to a variety of security attacks (Kebande & Awad, 2024).

Rathee et al., developed a mathematical model to identify malicious IoT devices by computing the trust factor (TF) based on probabilistic hypotheses. This model allows for the assessment of device legitimacy within IIoT networks, which had not been adequately addressed in previous literature. The proposed framework was rigorously validated through simulations conducted in a controlled environment using MATLAB. The proposed model identifies the legitimacy of each IoT device by computing its Trust Factor (TF) through an elected Coordinator IoT Device (CID). To prevent changes in the information of the local database, a data model based on blockchain is maintained at the back-end to keep track of all the transactions within the industry. The approach is validated extensively for different network sizes and evaluation criteria. Simulation results suggest that our proposed framework achieves 91% success rate against the network without a blockchain (Rathee et al., 2022).

After reviewing the above-mentioned works, it was noted that all research focused on developing forensic frameworks tailored to traditional IoT environments. These environments offer insights into data collection, analysis techniques, and evidence preservation.

This research aims to standardize forensic processes for IIoT environments by providing a comprehensive taxonomy that addresses the unique challenges posed by integrating IIoT devices into critical infrastructure, thus enhancing the effectiveness of investigations.

2.7. Research Gap

In recent years, the rise of IIoT systems has led to more connected devices in industries, increasing cyber threats and highlighting the urgent need for standardized IIoT forensics processes.

The IIoT offers numerous advantages for enhancing efficiency and productivity, and there are also growing concerns about security and potential cyber-attacks that underscore the need for effective forensic measures to investigate breaches, yet the lack of standardization in IIoT forensics hampers the ability to conduct thorough investigations and draw significant conclusions.

Various standards have been developed for digital forensics to ensure the preservation, analysis, report, and acquisition of digital evidence in criminal investigations. These standards do not fully address the challenges posed by the large-scale, distributed, and complex nature of IIoT systems.

Standardizing IoT forensics processes is challenging due to the diverse range of IIoT devices, which differ greatly in technology, architecture, and protocols. Despite advancements, the lack of standardization in IIoT forensics hampers effective investigations and underscores the necessity for consistent, reliable processes to foster trust and facilitate ongoing research and progress in the field. A taxonomy of interconnected processes is proposed to enhance digital forensic investigations in IIoT environments, encompassing stages from data acquisition and preservation to analysis and reporting, as shown in Figure 3. The figure presents a flowchart of the Industrial IoT (IIoT) Digital Forensics Process, outlining a systematic sequence of steps involved in managing and investigating security incidents within IIoT environments. The process begins with Anomaly Detection, where unusual or suspicious behavior is identified. This triggers Alert Generation, prompting the start of the forensic investigation. Next, Data Collection & Preservation ensures that relevant digital evidence is securely gathered and maintained without alteration. The collected data then undergoes Forensic Evidence Analysis, where investigators examine the evidence to understand the nature and scope of the incident. Following this, the Incident Response &

Containment step focuses on mitigating the impact of the incident and preventing further damage. The process continues with Legal Documentation & Reporting, which involves compiling findings for legal and organizational purposes. Finally, the process concludes with System Recovery & Future Preservation, aimed at restoring systems to normal operation and implementing measures to prevent similar incidents in the future. This structured flow ensures both a technical and legal framework for effective digital forensics in IIoT systems.

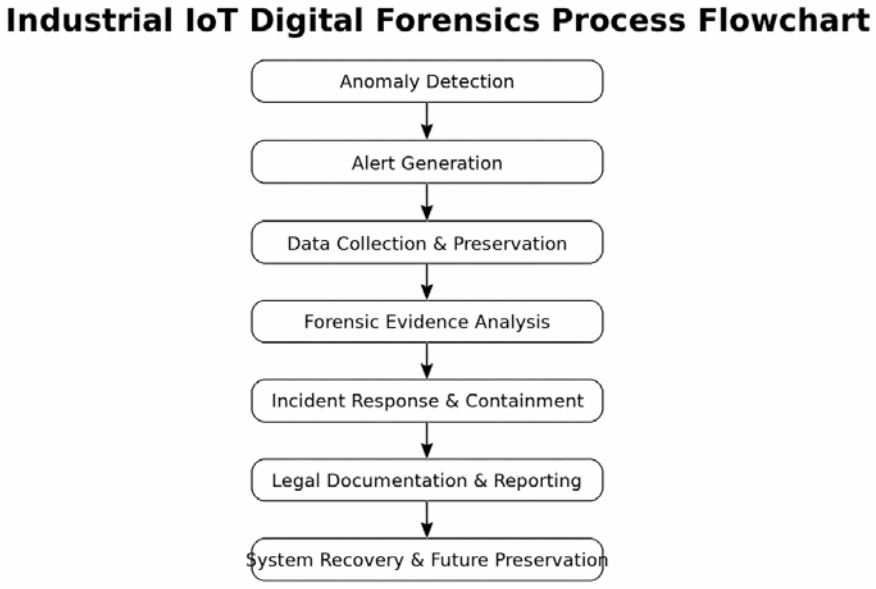

Figure 3. Forensic processes in industrial Internet IoT (IIoT) environments.

3. DISCUSSIONS

The study of Industrial Internet of Things (IIoT) forensics has revealed several key challenges and opportunities that must be addressed to realize the full potential of this technology. The main contribution of this paper is to provide a comprehensive review of current developments in IIoT forensics, including its key applications, techniques, and concepts. Based on the concepts defined in Section 1, the term IIoT forensics refers to the collection, analysis, preservation, and presentation of digital evidence. This is an important aspect of ensuring the security and integrity of industrial systems, facilitating the investigation of cyberattacks, accidents, and system failures.

Additionally, IIoT forensics relies on a variety of tools and techniques, including data acquisition, data analysis, and data visualization. These tools and techniques are utilized to extract and analyze digital evidence from a wide array of industrial devices and systems, including sensors, controllers, and other connected devices.

Lastly, IIoT forensics applications are used in a wide range of industrial sectors, which include manufacturing, transportation, healthcare, and energy. IIoT forensics in industrial sectors is used to investigate system failures, cyber-attacks, and incidents. In addition is used to improve system security and integrity.

Additionally, this study identified the challenges that need to be fully leveraged for IIoT forensics. These challenges include technical, legal, and organizational challenges. Technical challenges like standardization and system complexity. In Legal challenges, need for clear and consistent regulations. In organizational challenges need for better communication and collaboration between different stakeholders and to development.

Consequently, it cannot be understated that exploring case studies in the field of IIoT forensics. Researchers and practitioners can gain a deeper understanding of the practical aspects by examining real-world scenarios, applications, and limitations of IIoT forensics. Case studies provide valuable insights into the challenges and opportunities that arise during the actual deployment of IIoT forensics.

These case studies illustrate the practical applications of IIoT forensics in various real-world contexts, emphasizing its importance in investigating and resolving security incidents, as well as the challenges that must be tackled to effectively utilize IIoT forensics in the industrial sector.

One key takeaway from case studies is the importance of collaboration among diverse stakeholders for the successful implementation of IIoT forensics. The manufacturing company should work closely with the cybersecurity firm to identify and address security incidents. This highlights the necessity for organizations to clearly understand the different roles and responsibilities involved in IIoT forensics, along with the need for effective communication and coordination among various stakeholders.

Case studies emphasize that organizations must have a robust incident response plan that includes clearly defined procedures for investigation, evidence preservation, and stakeholder communication.

4. FUTURE RESEARCH DIRECTIONS

The following points display the future research direction for the IIoT forensics study:

a. Developing new techniques and methodologies for collecting and analyzing data in IIoT forensics that can help to address the technical challenges identified in the study.
b. Exploring solutions for the legal challenges identified in the study, such as the establishment of clear legal frameworks for IIoT forensics and addressing privacy and security concerns for data.
c. Examining the potential for using machine learning and AI in IIoT forensics to improve the efficiency of investigations and automate data analysis.
d. Conducting more Real-Life Case Studies in Industrial IoT Forensics to further understand its capabilities and limitations
e. Exploring ways to ensure that the benefits of IIoT forensics are distributed and accessible to all organizations.

5. CONCLUSION AND FUTURE WORK

This study highlights the latest developments in the field of Industrial Internet of Things (IIoT) forensics, including key applications, concepts, and technologies. It also identifies the key challenges that must be addressed for the implementation of IIoT forensics. These challenges include legal, regulatory, and technical issues that must be addressed to ensure the reliability and integrity of systems. This study also identifies future directions for research. Future IIoT forensics research should focus on addressing the challenges identified in this study. This may include developing new data collection and analysis techniques, establishing new legal frameworks, and developing new forensic methods.

As IIoT technologies continue to expand, ensuring their security is crucial. This research aims to enhance IIoT forensic investigations in Oman by developing a robust and innovative framework. By aligning with Oman Vision 2040, the study contributes to advancing cybersecurity efforts, protecting digital assets, and ensuring secure digital transformation in the country.

REFERENCES

Abbas, N., Nasser, Y., Shehab, M., & Sharafeddine, S. (2021). Attack-specific feature selection for anomaly detection in software-defined networks. In 2021 3rd IEEE Middle East and North Africa Communications Conference (MENACOMM) (pp. 142–146). IEEE. https://doi.org/10.1109/MENACOMM50775.2021.9678396

Awad, A. I., & Kebande, V. R. (2024). Industrial Internet of Things Ecosystems Security and Digital Forensics. ACM Computing Surveys, 56(5). https://doi.org/10.1145/3635030

Fitzpatrick, P., & Thorpe, C. (2024). Distributed Digital Ledger Technology for Digital Forensics for IIoT. https://tinyurl.com/4d2tsnmt

Gudlur, V. V. R., Shanmugan, V. A., Perumal, S., & Mohammed, R. M. S. R. (2020). Industrial Internet of Things (IIoT) of forensic and vulnerabilities. International Journal of Recent Technology and Engineering, 8(5), 1234–1240.

Gudlur, V. V. R., Shanmugan, V. A., Perumal, S., & Mohammed, R. M. S. R. (2020). Industrial Internet of Things (IIoT) of forensic and vulnerabilities. International Journal of Recent Technology and Engineering, 8(5), 2277–3878.

Juma, M., Alattar, F., & Touqan, B. (2023). Securing Big Data Integrity for IIoT. Internet of Things, 4(1), 27–55. https://doi.org/10.3390/iot4010002

Justice, J., Alade, O. M., Amusan, E. A., Ojo, O. J., Alade, T. R., & Fenwa, O. D. (2024). Forensic Evidence Collection in IoT Environments. Asian Journal of Research in Computer Science, 17(9), 70–91. https://doi.org/10.9734/ajrcos/2024/v17i9500

Kebande, V. R. (2022). Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. Forensic Science International: Reports, 5. https://doi.org/10.1016/j.fsir.2022.100257

Kebande, V. R., & Ikuesan, R. (2024). Standardizing Industrial Internet of Things (IIoT) Forensic Processes. https://doi.org/10.22541/au.171669128.84117392/v1

Molinaro, P., & Wagner, R. (2023). Guidelines for IIoT Forensics Readiness.

Nelufule, N., Masango, M., & Singano, T. (2024). Digital Forensics in Industry 4.0 and 5.0.

Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2022). A Secure and Trusted Mechanism for Industrial IoT Network using Blockchain. http://arxiv.org/abs/2206.03419Structure

Rathee, G., Iqbal, R., Kerrache, C. A., & Song, H. (2024). TrustNextGen: Security Aspects of Trustworthy Next-Generation Industrial Internet of Things. IEEE Internet of Things Journal, 11(15), 25568–25576. https://doi.org/10.1109/JIOT.2024.3361801

Sasikumar, P., Arulmurugan, R., & Manogaran, G. (2024). A comprehensive survey on security and privacy challenges in Industrial Internet of Things. Journal of Ambient Intelligence and Humanized Computing, 15(1), 123–145.

Sharma, S., Kumar, A., Rathore, N. S., & Sharma, S. (2024). Intrusion Detection in IIoT. https://doi.org/10.1007/s12046-024-02567-zS

Shin, D. H., Han, S. J., Kim, Y. B., & Euom, I. C. (2024). Digital Forensics of Heterogeneous IoT. Applied Sciences, 14(3). https://doi.org/10.3390/app14031128

Shtayat, M. M., Hasan, M. K., Sulaiman, R., Islam, S., & Khan, A. U. R. (2023). An Explainable Ensemble Deep Learning Approach for Intrusion Detection in IIoT. IEEE Access, 11, 115047–115061. https://doi.org/10.1109/ACCESS.2023.3323573

Tyagi, S. (2023). Cybersecurity challenges in Industrial IoT: A survey. International Journal of Computer Applications, 182(1), 25–30.