

Applying Dempster Shafer Theory and Causal Inference in Investigating Internet of Things Digital Forensic Challenge

Mohamed El-Dosuky^{1,2}, Sherif K. Ratib^{2,3} and Mostafa M. El-Gayar^{2,4}

¹Department of Computer Science, Faculty of Computers and Information, Mansoura University, Egypt

²Department of Computer Science, Arab East Colleges, Saudi Arabia

³Department of Communications and Computer Engineering, October University for Modern Sciences and Arts, Egypt

⁴Department of Information Technology, Faculty of Computers and Information, Mansoura University, Egypt

Article history

Received: 08-05-2026

Revised: 09-07-2026

Accepted: 16-07-2026

Corresponding Author:

Mohamed El-Dosuky
Department of Computer
Science, Faculty of Computers
and Information, Mansoura
University, Egypt
Email:
maldosuky@arabeast.edu.sa

Abstract: The rapid growth of IoT ecosystems has transformed digital forensics, creating challenges in analyzing distributed, heterogeneous, and uncertain evidence. Conventional forensic methods often struggle to handle ambiguous and conflicting IoT data, highlighting the need for robust frameworks that effectively manage uncertainty across multiple evidence sources. This research presents a hybrid forensic framework that integrates Dempster Shafer Theory (DST) for probabilistic uncertainty modeling with causal inference for deterministic reconstruction of event relationships. Together, these methods provide a comprehensive approach to evidence fusion and event attribution in complex IoT investigations. Using the DFRWS 2017 IoT Digital Forensic Challenge as a case study, the framework systematically processes and correlates diverse evidence sources, including Google Hangouts messages, Alexa voice logs, IoT sensor traffic, and wearable activity data. Results show that DST-based evidence fusion reduces the DST-based epistemic uncertainty (i.e., the proportion of uncommitted belief/ignorance) from 18% before evidence fusion to 0.2% after integrating all available evidence, while achieving a belief value of 97.4% for suspect identification. Complementary causal inference analysis reconstructs temporal and behavioral dependencies, improving the interpretability of probabilistic outcomes. The combined model enhances reliability, transparency, and reproducibility, offering a scientifically grounded methodology suited to modern, data-rich IoT forensic environments where traditional techniques fall short.

Keywords: Digital Forensic, Dempster Shafer Theory, Causal Inference, Internet of Things, Temporal Logic

Introduction

The explosive growth of smart devices and the Internet of Things has fundamentally transformed our world into a vast network of interconnected systems that have become essential to how we live and work. These devices, from fitness trackers and smartwatches to voice assistants powered by cloud computing and sophisticated sensor networks, have undeniably improved our quality of life by offering unprecedented convenience and functionality. However, this technological revolution comes with a significant drawback: These devices continuously collect and

transmit enormous volumes of diverse data types, creating new vulnerabilities that criminals can exploit for cyberattacks, privacy breaches, and other malicious purposes (Ahmed et al., 2024; 2025; Kim et al., 2023).

This digital transformation has placed the field of digital forensics at a critical juncture. Investigators now face extraordinarily complex challenges when attempting to gather, analyze, and interpret evidence from these intricate ecosystems. The traditional methods of digital investigation are often inadequate when dealing with the interconnected nature of IoT devices and the challenge of correlating evidence across multiple platforms and data formats. As a result,

developing innovative, robust, and scalable forensic methodologies specifically designed for IoT investigations has become not just a priority, but an urgent necessity that is driving significant research efforts across academic institutions worldwide (Montasari and Hill, 2019; Zikria et al., 2021; Alshabibi et al., 2024).

Traditional digital investigation methods fall short when dealing with IoT environments, where evidence is inherently scattered and constantly evolving. Information can be spread across numerous smart devices, cloud platforms, and various communication networks, creating significant challenges in connecting events and understanding the relationships between different data sources. Moreover, evidence often appears incomplete, questionable in its accuracy, or even contradictory, which complicates the task of identifying those responsible for criminal activities. These challenges highlight the urgent need to develop advanced analytical systems capable of unifying evidence gathered from diverse sources, handling ambiguity and uncertainty, and drawing reliable conclusions within complex investigative frameworks (Kim et al., 2020; Spiekermann and Keller, 2023; Yaacoub et al., 2022). The distributed nature of IoT ecosystems means that a single incident might leave traces across dozens of interconnected devices and services, each with its own data formats, storage methods, and access protocols. This fragmentation makes it extremely difficult for investigators to piece together a complete picture of what actually happened. When evidence exists in multiple formats across different platforms, establishing a clear timeline or determining causality becomes a complex puzzle that traditional forensic tools simply weren't designed to solve. The need for sophisticated correlation techniques and unified analysis platforms has never been more critical in ensuring that digital investigations can keep pace with our increasingly connected world (Friedl and Pernul, 2024; Saleh et al., 2023).

The DFRWS 2017 IoT Digital Forensics Challenge stands as one of the most important and widely recognized benchmarks in this specialized field. The challenge presents a realistic crime scenario that unfolds within a smart home environment, where multiple users interact with various connected devices including Amazon Alexa assistants, smartphones, and different IoT sensors. Forensic experts are expected to reconstruct the sequence of events, trace how devices communicated with each other, and link suspicious activities to specific individuals. This practical example highlights the fundamental challenges facing IoT digital forensics, which include the diversity of evidence sources, the presence of multiple users, the emergence of ambiguous or contradictory data, and the difficulty of establishing a reliable logical chain of events (Janarthanan et al., 2021; Nieto et al., 2018).

Addressing these complexities requires advanced methodologies that go beyond traditional evidence correlation approaches. Instead, investigators must rely on sophisticated mathematical models designed to handle uncertainty and causal relationships. The challenge demonstrates how modern forensic investigations can no longer depend solely on straightforward data analysis, but must incorporate probabilistic reasoning and advanced analytical frameworks to make sense of the interconnected web of digital evidence that IoT environments produce. This shift represents a fundamental evolution in how digital forensics adapts to keep pace with an increasingly connected world.

In this paper, we present a comprehensive methodology for digital forensic investigation that leverages Dempster-Shafer theory and causal reasoning to analyze data from the DFRWS 2017 IoT challenge. Our research contributions encompass three key aspects: First, we demonstrate how Dempster-Shafer theory can efficiently integrate diverse evidence sources, including text conversations, Alexa voice recordings, IoT sensor activities, and wearable device data, while systematically reducing uncertainty levels. Second, we employ causal reasoning mechanisms to explore the interconnections between events and temporal relationships, providing a logical explanation for observed behaviors. Third, we present a comprehensive experimental evaluation of our proposed approach, demonstrating its capability to achieve high confidence levels in suspect identification.

Results show that DST-based evidence fusion reduces the DST-based epistemic uncertainty (i.e., the proportion of uncommitted belief/ignorance) from 18% before evidence fusion to 0.2% after integrating all available evidence, while achieving a belief value of 97.4% for suspect identification. Complementary causal inference analysis reconstructs temporal and behavioral dependencies, improving the interpretability of probabilistic outcomes.

Related Work

Research into digital evidence in Internet-of-Things (IoT) environments has led scientists to create sophisticated reasoning systems that handle uncertain data and combine different information sources to find explanations for complicated forensic cases. The following section evaluates existing research through three essential areas that form the basis of our investigation: Dempster Shafer Theory and its applications to causal inference and digital forensic analysis of IoT systems.

The mathematical framework of Dempster Shafer Theory (DST) proves effective for managing uncertain data while uniting information from multiple conflicting sources. The initial research showed DST's effectiveness in multimedia forensics through data fusion methods, which restricted anti-forensic techniques by uniting

evidence traces from different tools (Fontani et al., 2014). The application of DST in data classification tasks produces high accuracy through attribute-based evidence combination while handling uncertain decision-making processes (Chen et al., 2014). The cybersecurity field uses DST extensively for network intrusion forensics because it enables automatic evidence combination from distributed sensors to enhance real-time crime detection capabilities (Tian et al., 2014). Recent research has applied DST to IoT systems because these environments face two major challenges: Data diversity and sensor system instability. Research on adaptive evidence fusion models and enhanced conflict management systems demonstrates how DST enables dependable decision-making in unpredictable IoT systems with noisy data (Yang et al., 2019; Hamda et al., 2023). The integration of DST with complex event processing systems proves its ability to handle real-time event stream analysis in IoT-based systems that include fire detection and anomaly monitoring (Bezerra et al., 2021). The research demonstrates DST's ability to handle uncertain data, which makes it an ideal choice for forensic investigations that require analysis of multiple digital evidence sources.

The method of causal inference provides an alternative approach to DST by establishing the directional connections between events. The application of causal inference methods has gained popularity throughout recommendation systems (Wei et al., 2023), finance (Xing et al., 2024), and manufacturing (Xiao et al., 2025) because they enhance both decision model interpretability and robustness. Digital forensics researchers have adopted causal reasoning to improve investigation methods by revealing cause-and-effect relationships between events instead of relying on basic correlations (Qian et al., 2025).

Research studies demonstrate that causal inference methods show promising results when applied to IoT systems and security applications. The research by Gad developed an IoT network anomaly detection framework using causal analysis, which delivered enhanced detection precision and clearer results (Gad, 2024). Wang et al. used causal inference to identify IoT devices at a detailed level through their analysis of communication features that drive causality (Wang et al., 2023). The research indicates that causal reasoning systems create connections between

raw events and logical explanations of user activities, which proves essential for forensic investigations that need to establish user responsibility.

Several studies have investigated IoT digital forensic methodologies using open-source tools (Al-Sadi et al., 2018). The investigation of digital evidence in IoT systems faces multiple obstacles because of different device types, restricted resources, distributed storage systems, and evidence that changes frequently. For instance, DST-based investigation has been proposed (Jayakrishnan and Vasanthi, 2020). The collection and preprocessing of IoT evidence face major challenges according to recent surveys because of the complex nature of cloud-based services and multi-user systems (Ahmed et al., 2024). The DFRWS community has made substantial progress in forensic science through case-based challenges, including the DFRWS 2017 IoT Challenge, which serves as a benchmark for smart home forensic analysis (Breitinger et al., 2024). The field of network and IoT forensics employs artificial intelligence, machine learning, and ensemble methods to enhance evidence analysis and detect abnormal activities (Rizvi et al., 2022). The current state of evidence analysis in investigations faces an essential challenge because investigators need to handle uncertain evidence that conflicts with each other while establishing event relationships that need to be understood. The research gap between DST evidence fusion and causal inference models drives the development of a new framework that combines these approaches for IoT digital forensic analysis.

Table 1 summarizes the existing methodologies, their applications, and their respective strengths and limitations. The comparison indicates that Dempster-Shafer Theory (DST) is particularly effective in managing uncertainty and fusing heterogeneous evidence from multiple sources, whereas causal inference excels at identifying cause-and-effect relationships and providing interpretable explanations of forensic events. Integrating these complementary methodologies enables investigators to leverage the strengths of both approaches. DST offers a mathematically rigorous framework for evidence fusion and decision-making under uncertainty, while causal inference reconstructs event dependencies to explain how forensic outcomes arise.

Table 1: Summary of Related Work

Methodology	Application	Advantage	Disadvantage
Dempster-Shafer Theory	Multimedia forensics, IoT event fusion, network intrusion forensics	Handles uncertainty; fuses conflicting evidence; robust decision-making	High complexity with many sources; conflict resolution can be difficult
Causal Inference	Recommendations, finance, IoT anomaly detection, device identification, forensic explainability	Provides interpretability; uncovers cause-effect relations; improves attribution	Sensitive to confounders; requires accurate causal models
Digital Forensics in IoT	Smart home forensics, IoT/cloud evidence analysis, anomaly detection	Context-specific insights; benchmark challenges like DFRWS; supports real-world incident analysis	Device heterogeneity; limited resources; difficulty in evidence collection/preprocessing

Consequently, the proposed hybrid framework enhances both the reliability and interpretability of IoT forensic investigations by overcoming the limitations associated with using either methodology in isolation.

Methods

Fig. 1 illustrates the data analysis and decision-making pipeline that integrates uncertainty and certainty reasoning methods. Each stage of the proposed methodology is discussed in detail in the following sub-sections.

Case Study Input Data

In the initial stage, raw data is collected from a real-world case study. The input data includes logs, JSON files, timestamps, and network capture files (PCAPs) obtained from IoT sensors and smart devices. This raw data serves as the foundation for the analysis process and may come from multiple heterogeneous sources, each containing valuable but unprocessed information.

The DFRWS 2017 IoT Digital Forensic Challenge presented a virtual smart home crime scene, which evaluated investigators' skills in uniting different IoT data platforms to rebuild actual incidents. The system linked multiple devices through a network that included Amazon Echo (Alexa) smart speakers, motion detectors, door sensors, and smartphones and computers that operated through network connections across different rooms. The digital evidence showed that Betty, Simon, and John were involved in a personal conflict that developed into a physical encounter. The forensic team received various evidence sources, which included Google Hangouts databases (babel1.db), Alexa JSON and audio logs, and SmartHome PCAP network captures.

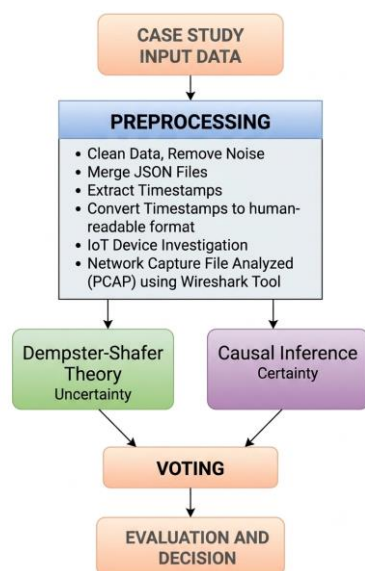


Fig. 1: Proposed Methodology

The investigators used combined evidence to prove John used Alexa before he entered the living room to face Betty and then departed the scene through matching timestamps, voice recordings, and IoT sensor trigger records. The smart home layout and forensic environment appear in Fig. 2, which demonstrates how digital and physical components interacted through the smart home system. The living room area where Betty and Amazon Echo resided included door and motion sensors which monitored the space in real-time. The bedroom computer operated by Simon generated network data that served as additional contextual information. The evidence sources in the diagram use different colors to represent their significance: Structural elements appear in gray, while participants are shown in blue, and sensors and digital devices are represented by orange and red, respectively. The setup design focuses on the main goal of connecting human actions to IoT digital output for forensic evidence collection in actual crime scene investigations.

Preprocessing

In the preprocessing stage, the input data undergoes cleaning, integration, and transformation to prepare it for analysis. Noise and irrelevant data are removed, multiple JSON files are merged into a unified dataset, and timestamps are extracted and converted into human-readable formats. Additionally, IoT device activity is investigated, and network captures are analyzed using tools like Wireshark. The main goal of preprocessing is to structure and refine the data so it can be effectively analyzed in the next stages.

Fig. 3 shows the timeline of events in the DFRWS 2017 IoT digital forensic challenge. The digital evidence timeline reveals a sequence of events spanning personal and smart home interactions. Early in the morning, at 4:39:08 AM, John initiated a chat with Betty through Google Hangouts on her phone.

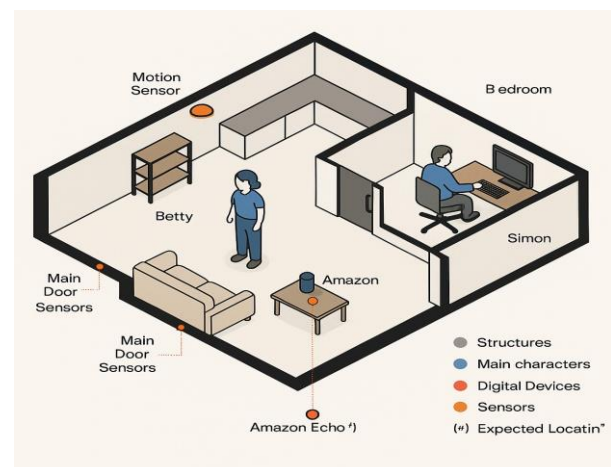


Fig. 2: The settings of DFRWS 2017 IoT Digital Forensic Challenge

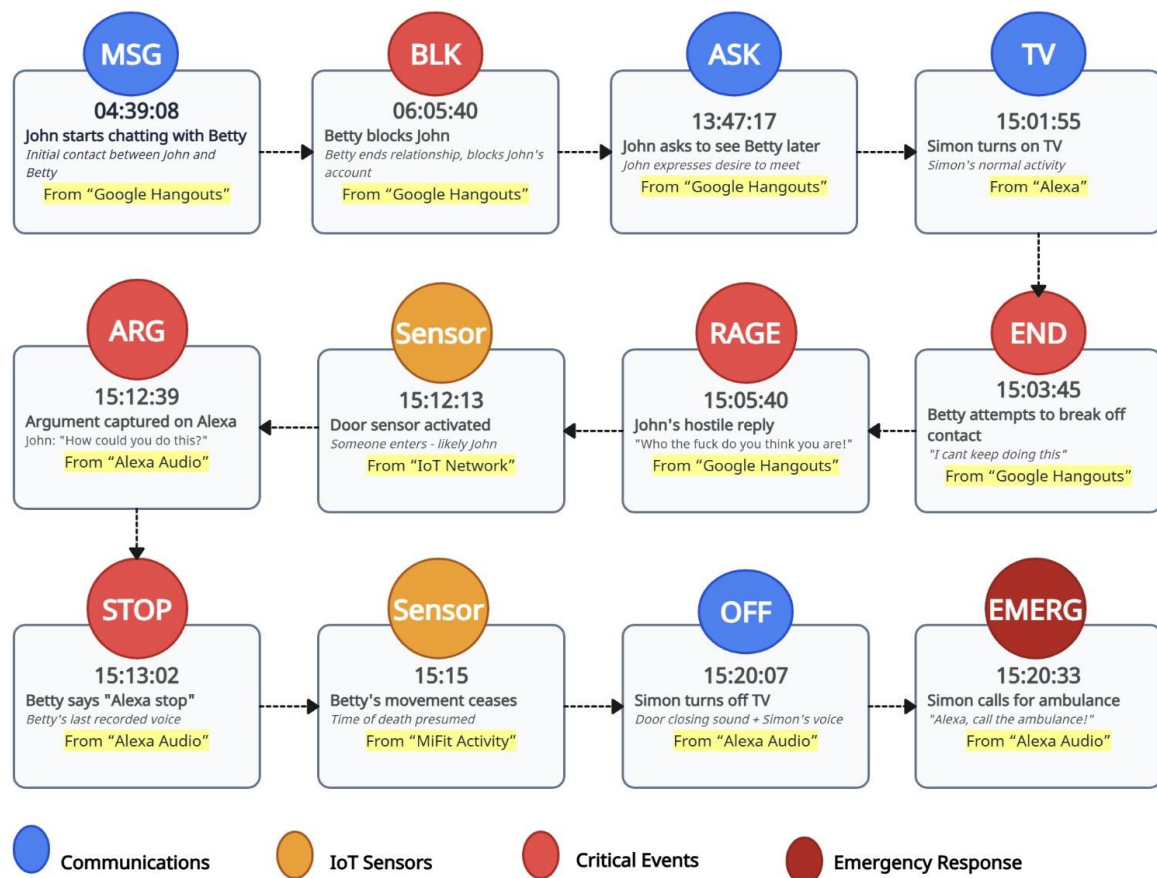


Fig. 3: The Timeline of events in the DFRWS 2017 IoT Digital Forensic Challenge

Less than two hours later, at 6:05:40 AM, Betty blocked John, indicating a conflict or emotional fallout. Later that afternoon, at 3:01 PM, Simon used Alexa to turn on the TV, as recorded in the Alexa Web Portal data. About ten minutes later, at 3:12:39 PM, Alexa captured John shouting, "How could you do this," suggesting a tense emotional outburst. Shortly afterward, at 3:13:17 PM, IoT network logs recorded a command sent to the management server to turn off a device, consistent with the following Alexa command at 3:20 PM when Simon asked Alexa to turn off the TV. However, the IoT logs show that at 3:20:26 PM, a new request with the same device ID and a parameter indicating activation was sent, meaning the device or sensor was turned on again. Together, these records illustrate a tightly linked series of human and device interactions, beginning with a personal dispute and extending into the smart home environment, where both Alexa and IoT network traffic corroborate each other's timestamps and actions.

Following data acquisition, all evidence sources underwent a preprocessing stage to transform heterogeneous forensic artifacts into a unified event representation. Google Hangouts messages stored in the SQLite database were parsed to extract message

identifiers, sender and receiver information, timestamps, message content, and attachment metadata. Network traffic captured in PCAP format was processed using Wireshark to identify IoT devices, extract HTTP request and response fields, determine source and destination IP addresses, communication endpoints, request methods (GET and PUT), response codes, and packet timestamps. Alexa voice interaction logs were parsed to obtain invocation times, executed commands, device identifiers, and response events, while wearable activity records were processed to extract timestamps, motion events, and user activity indicators.

Since the evidence originated from multiple devices with different data formats and timestamp representations, all timestamps were converted to a common UTC-based format and chronologically synchronized. Duplicate records generated by repeated packet captures or redundant log entries were removed, and incomplete or malformed records that lacked essential forensic attributes were excluded from further analysis. Finally, each artifact was transformed into a standardized event structure consisting of {Timestamp, Device ID, Event Type, Source, Destination, Evidence Source, and Confidence}. This unified representation enabled

efficient temporal correlation, Dempster–Shafer evidence fusion, and causal inference across heterogeneous IoT evidence sources.

Fig. 4 shows the Blocked_People table extracted using Sqliteman. The message investigation focused on analyzing communication data extracted from the database file 002-BettyNote2Black_SHV-E250L_Physical_20170717_SHV E250L_Physical_20170717_USERDATA.mdf/data/com.google.android.talk/databases/babel1.db, which corresponds to Google Hangouts data stored on Betty's device. Using the tool SQLiteManager, investigators

accessed and queried the stored chat messages. The process involved launching SQLiteManager, navigating to the Databases section, and selecting the Build Query option. From the available tables, the Messages table was chosen to display the relevant communication records.

Fig. 5 depicts the analysis of IoT network traffic using Wireshark. The IoT Device Investigation focused on analyzing network activity captured in the file \IoT_Net_Traffic\IP-filtered-SmartHome-Traffic.pcap. This file contained recorded network traffic from a smart home environment and was examined using Wireshark, a network analysis tool.

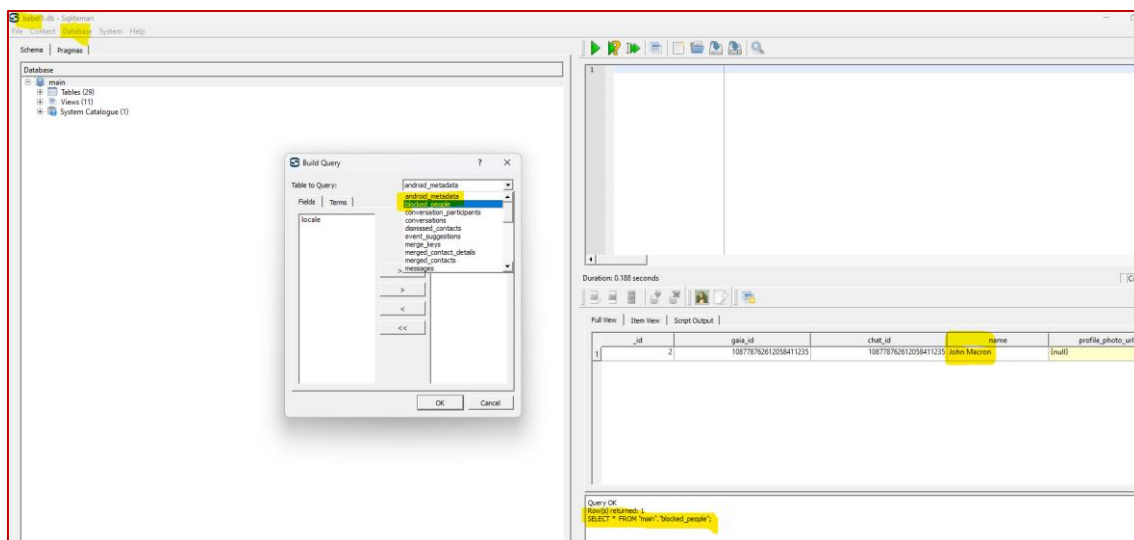


Fig. 4: The Blocked_People table extracted using SQLite Manager

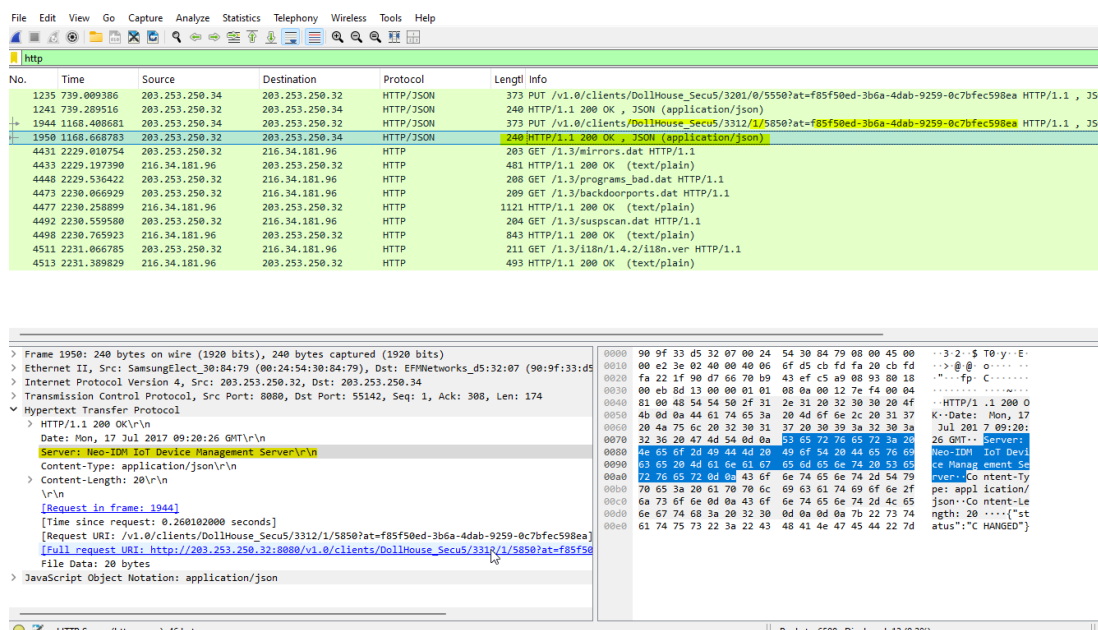


Fig. 5: Analysis of IoT network traffic using Wireshark

After launching Wireshark, the PCAP file was imported for detailed inspection. Investigators concentrated on HTTP traffic, as this protocol can reveal valuable clear-text information. By filtering the data in the Protocol column to display only HTTP packets, the analysis revealed communication involving an IoT device identified as “Dollhouse.” This device appeared to use both PUT and GET requests, indicating active interaction with its sensors and remote control features. According to the metadata and traffic context, the Dollhouse device integrates multiple smart features commonly associated with IoT-enabled toys and smart environments. The HTTP responses showed that the device was communicating with the Neo-IDM IoT Device Management Server, a platform responsible for managing and authenticating IoT devices and sensors. This finding confirmed the Dollhouse's registration and activity within a managed IoT network, providing critical evidence of its operational status and external communications.

Dempster Shafer Theory

Dempster-Shafer Theory focuses on handling uncertain or incomplete data, which allows reasoning with degrees of belief rather than binary true/false logic. It quantifies uncertainty by assigning probabilities to various hypotheses based on available evidence. This helps account for situations where data might be ambiguous or insufficient for clear conclusions, ensuring that uncertainty is explicitly represented in the decision-making process. DST provides a mathematical framework for modeling uncertainty and combining evidence from multiple sources without requiring prior probabilities. The frame of discernment is denoted by: $\Theta = \{John, Simon, Unknown, Accident\}$.

Θ represents the set of all possible hypotheses related to the forensic case. Each hypothesis $\theta_i \in \Theta$ is mutually exclusive and collectively exhaustive such that $U_i \theta_i = \Theta$ and $\theta_i \cap \theta_j = \phi$ for $i \neq j$. The power set of Θ , denoted 2^Θ , includes all subsets of Θ , representing every possible evidence combination. Each source of evidence (e.g., chat logs, Alexa recordings, IoT sensors, and MiFit data) provides a Basic Probability Assignment (BPA) $m(A)$, which quantifies the confidence that a subset $A \subseteq \Theta$ is true. The belief and plausibility functions are computed as:

$$Bel(A) = \sum_{B \subseteq A, B \neq \emptyset} m(B) \quad (1)$$

$$Pl(A) = 1 - Bel(\neg A) = \sum_{B \cap A \neq \emptyset} m(B) \quad (2)$$

Where $Bel(A)$ represents the minimum support (degree of certainty) for hypothesis A, and $Pl(A)$ denotes the maximum possible support (degree of plausibility). To combine evidence from multiple independent sources, Dempster's rule of combination is applied:

$$m_{1,2}(C) = \frac{\sum_{A \cap B = C} m_1(A)m_2(B)}{1 - K} \quad (3)$$

$$K = \sum_{A \cap B \neq \emptyset} m_1(A)m_2(B) \quad (4)$$

Where K measures the conflict between evidence sources. The normalization term $1 - K$ ensures that conflicting mass is redistributed among consistent hypotheses.

Causal Inference

In contrast to the uncertainty-based approach, the causal inference stage focuses on establishing causal relationships within the data using statistical or logical reasoning methods. Causal inference identifies how certain variables influence others, helping to determine cause-and-effect patterns. This stage operates with greater confidence and is typically supported by consistent, high-quality data that allows deterministic conclusions.

The timeline chart in Fig. 6 illustrates the sequence of events and the presence of Simon and John in the moments leading up to a death incident. Simon's activity, shown in green, begins around 15:05 when he turns on the TV and remains continuous until after 15:20, indicating his ongoing presence in the scene. John, represented in blue, appears later when he enters the location (DoorIn event) and is immediately involved in an argument, as captured in the data. The critical event, marked by a red “X,” occurs around 15:14, signifying the time of death, which falls within the highlighted red zone representing the window immediately preceding the incident. Following the death, the records show that the TV was turned off and an ambulance was called, both actions associated with Simon. The chart therefore suggests that Simon was continuously present throughout the event, while John arrived shortly before the argument and the death occurred, making their overlapping presence in this narrow timeframe a key focus for further forensic interpretation.

The causal relationship diagram in Fig. 7 illustrates the sequence of connected events that may have contributed to the death incident. The graph identifies three primary actors or event sources and maps the flow of actions leading to the central outcome, represented by the red node labelled Death.

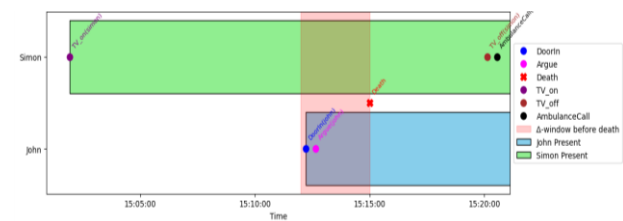


Fig. 6: The Temporal Diagram for the case study

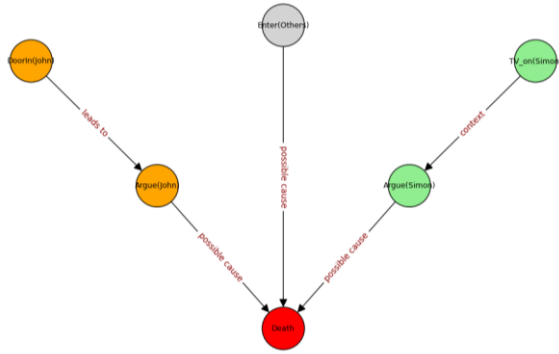


Fig. 7: Causal Reasoning Graph for the case study

On the left side, John's entry (DoorIn) is shown leading directly to an argument, suggesting that his arrival triggered a confrontation. This argument is then linked to the death as a possible cause, indicating that the conflict involving John may have played a significant role in the fatal outcome. On the right side, Simon's actions begin with turning on the TV, establishing the situational context for his involvement, followed by his participation in an argument, which is also identified as a possible contributing factor to the death. Additionally, a neutral event labelled Enter (Others) connects to the death as another possible cause, implying that other individuals may have been present or influenced the situation.

Voting

The voting stage acts as a fusion mechanism that integrates results from both the Dempster-Shafer (uncertain) and causal inference (certain) analyses. By combining the outcomes, the system balances probabilistic reasoning with evidence-based conclusions. The simplest and most interpretable fusion is a weighted linear combination:

$$V_i = \alpha B_i + (1 - \alpha)C_i \quad (5)$$

Where:

- V_i is the final voting score
- $\alpha \in [0,1]$ controls the influence of DST
- $1 - \alpha$ controls the influence of causal inference

Typical choices are:

- $\alpha = 0.5$: equal importance
- $\alpha = 0.6$: slightly favor uncertain evidence
- $\alpha = 0.4$: slightly favor causal reasoning

The selected hypothesis is:

$$H^* = \arg \max_i V_i \quad (6)$$

To illustrate the proposed voting mechanism, Table 2 presents an example in which the DST belief values and causal inference scores for three suspects are combined to obtain the corresponding final scores.

Table 2: Example Results

Suspect	DST Belief B_i	Causal Score C_i	Final Score ($\alpha = 0.5$)
A	0.974	0.96	0.967
B	0.021	0.18	0.101
C	0.005	0.09	0.048

Suppose three suspects produce the following results: Since: $V_A = 0.967$ is the largest score.

$H^* = A$. This ensures that decisions are not solely based on either uncertain beliefs or deterministic causality but on a well-rounded consensus derived from both approaches.

Evaluation and Decision

The final stage involves assessing the integrated outputs and making a data-driven decision. Here, the system evaluates the combined results from the voting stage, interpreting them to produce actionable insights or final judgments. This evaluation ensures that both uncertainty and certainty have been adequately considered, leading to robust, transparent, and justified decision-making outcomes.

Results and Discussion

The forensic investigation incorporated four distinct IoT evidence sources: Google Hangouts messages, Alexa voice recordings, IoT door sensor data, and MiFit activity records, each contributing Basic Probability Assignments (BPAs) with varying confidence levels and inherent uncertainties. Initial BPAs ranged from moderate confidence in communication-based evidence (Hangouts: 0.750, Alexa: 0.700 for John) to higher uncertainty in sensor-based behavioral data (MiFit: 0.220 uncertainty). Sequential application of Dempster's combination rule demonstrated remarkable evidential convergence, with John's belief mass increasing progressively from individual source values of 0.450-0.750 to a final combined assessment of 0.974, while uncertainty diminished dramatically from 0.180 to 0.002. The fusion process yielded final belief and plausibility intervals of $\text{Bel}(\text{John}) = 0.974$ and $\text{Pl}(\text{John}) = 0.976$, representing a narrow confidence interval [97.4%-97.6%] with minimal epistemic uncertainty, while alternative hypotheses (Simon, Unknown) maintained consistently low probability masses below 0.02 throughout all combination stages. Although cumulative conflict reached 0.339 (33.9%) due to natural disagreements between heterogeneous evidence types,

this level remained within acceptable forensic limits and reflected the inherent tension between direct communication evidence and ambiguous behavioral sensor data.

The DST-based evidence fusion successfully addressed three critical challenges in IoT digital forensics: Handling incomplete evidence, quantifying investigator confidence, and resolving conflicts between heterogeneous data sources while maintaining mathematical rigor and transparency.

The systematic convergence of four independent data streams on the same hypothesis, despite their heterogeneous nature and individual uncertainties, validates the robustness of multi-modal IoT evidence integration and demonstrates that diverse behavioral indicators communication patterns, voice interactions, environmental access, and biometric activity collectively create a comprehensive attribution fingerprint significantly more reliable than any individual source. As shown in Table 3, the quantified confidence level (97.4%) with explicit uncertainty bounds ($\pm 0.2\%$) provides a scientifically rigorous foundation for legal proceedings, offering clear metrics for courtroom presentation and appeals processes while enhancing the credibility of digital forensic conclusions through systematic evidence assessment rather

than subjective interpretation. This investigation confirms that DST provides an effective framework for quantitative evidence fusion in complex digital forensic scenarios, successfully transforming uncertain and potentially conflicting IoT data streams into coherent, mathematically grounded conclusions suitable for high-stakes legal decision-making, thereby establishing a new standard for evidence-based attribution in the expanding landscape of IoT-enabled criminal investigations.

Table 4 presents the results of the Ordinary Least Squares (OLS) regression analysis, indicating that the model is statistically significant overall ($F(2,997) = 127.4$, $p < 0.001$) and explains approximately 20.4% of the variance in the dependent variable Death ($R^2 = 0.204$, Adjusted $R^2 = 0.202$). Among the predictors, Argue John shows a strong and highly significant positive relationship with Death ($\beta = 0.418$, $t = 12.95$, $p < 0.001$), suggesting that increases in this variable are associated with higher values of Death. In contrast, DoorIn_John has no significant effect ($\beta = 0.019$, $t = 0.56$, $p = 0.577$). The Durbin-Watson statistic (2.02) indicates no serious autocorrelation, though the Omnibus and Jarque Bera tests ($p < 0.001$) suggest that residuals deviate somewhat from normality. The model fits moderately well and identifies Argue John as the key predictor influencing Death.

Table 3: DST Results

Evidence Source	John	Simon	Unknown	Uncertainty
Hangouts Messages	0.750	0.050	0.020	0.180
Alexa Voice Logs	0.700	0.080	0.050	0.170
Door Sensor Data	0.550	0.200	0.120	0.130
MiFit Activity Data	0.450	0.150	0.180	0.220
Hangouts + Alexa	0.917	0.032	0.016	0.036
Hangouts + Alexa + Door Sensor Data	0.956	0.026	0.012	0.007
Hangouts + Alexa + Door Sensor Data + MiFit Data	0.974	0.016	0.009	0.002

Table 4: Ordinary Least Squares (OLS) Regression Results

Dep. Variable:	Death	R-squared:	0.204			
Model:	OLS	Adj. R-squared:	0.202			
Method:	Least Squares	F-statistic:	127.4			
Date:	Fri, 12 Sep 2025	Prob (F-statistic):	5.30e-50			
Time:	19:25:47	Log-Likelihood:	-544.23			
No. Observations:	1000	AIC:	1094.			
Df Residuals:	997	BIC:	1109.			
Df Model:	2					
Covariance Type:	nonrobust					
=====						
	coef	std err	t			
			P> t			
			[0.025			
			0.975]			
const	0.1368	0.024	5.740	0.000	0.090	0.184
DoorIn_John	0.0192	0.034	0.558	0.577	-0.048	0.087
Argue_John	0.4182	0.032	12.950	0.000	0.355	0.482
=====						
Omnibus:	69.795	Durbin-Watson:	2.016			
Prob(Omnibus):	0.000	Jarque-Bera (JB):	58.165			
Skew:	0.510	Prob(JB):	2.34e-13			
Kurtosis:	2.403	Cond. No.	4.41			

Note that forensic investigations primarily rely on evidence-based reasoning and logical reconstruction rather than statistical correlation alone. The paper's intention is not to use OLS regression as a decision-

making or evidence attribution tool. Instead, OLS was employed as an exploratory analytical technique to quantify relationships among selected forensic variables and to identify trends that may support the interpretation of the collected evidence.

Direct quantitative comparison is challenging because existing IoT forensic frameworks are generally evaluated using different datasets, forensic scenarios, evidence sources, and performance metrics, making a fair head-to-head comparison difficult. Table 5 demonstrates the incremental benefit of integrating causal inference with DST, even if no prior work has evaluated the same dataset using the same methodology.

Table 5: Comparing Components

Method	Uncertainty Handling	Causal Analysis	Belief	Remaining Uncertainty
Traditional forensic analysis	✗	Expert reasoning	--	--
DST only	✓	✗	97.4%	0.2%
Causal inference only	✗	✓	--	--
Proposed DST + Causal	✓	✓	97.4%	0.2% + causal explanation

Conclusion and Future Work

This investigation successfully developed and validated a unified forensic analysis framework that synergistically integrates Dempster–Shafer Theory with causal inference methodologies to comprehensively address the dual challenges of uncertainty quantification and causality reconstruction in contemporary IoT digital investigations. Through rigorous application to the DFRWS 2017 IoT challenge dataset, the research empirically demonstrated how systematic evidence preprocessing, probabilistic fusion algorithms, and deterministic causal reasoning can effectively reconstruct complex incident timelines while significantly enhancing attribution accuracy in multi-device smart environments. The DST component validated its capacity to integrate heterogeneous digital evidence sources while systematically reducing epistemic uncertainty from 18% to 0.2%, thereby transforming ambiguous multi-source evidence into quantifiable forensic conclusions with 97.4% confidence.

Complementarily, the causal inference analysis successfully revealed underlying cause-effect relationships among temporal events, providing logical reasoning pathways that enhance the interpretability and legal admissibility of probabilistic findings. The innovative fusion of these paradigms through a structured voting mechanism delivered balanced, evidence-based conclusions that maintain both statistical rigor and logical transparency, addressing critical gaps in existing forensic methodologies. The comprehensive findings validate that integrating uncertain probabilistic reasoning with deterministic causal analysis produces a more robust, transparent, and comprehensive forensic model capable of managing the inherent complexity, scale, and heterogeneity of modern IoT ecosystems.

This research significantly contributes to the advancement of intelligent forensic reasoning frameworks by enabling investigators to achieve higher confidence levels in their investigative decisions while maintaining complete traceability and explainability throughout the analytical process, critical requirements for legal proceedings and appeal processes.

Future research will focus on expanding the proposed framework in several directions. First, the framework will be evaluated on larger and more diverse real-world IoT forensic datasets to assess its scalability and generalizability across different smart environments. Second, automated evidence extraction and preprocessing techniques will be integrated to support a wider range of IoT devices, communication protocols, and proprietary data formats. Third, adaptive evidence incorporation methods that dynamically adjust belief mappings based on source reliability and evidence quality will be investigated to further improve decision accuracy.

Additionally, future work will explore integrating machine learning techniques for automated event classification and anomaly detection while preserving the interpretability provided by causal inference. Another promising direction is the integration of temporal causal and probabilistic graphical models to improve the detection of complex event sequences and sophisticated attack scenarios. Finally, the framework will be validated through benchmarking against the latest IoT forensics methodologies using standardized datasets and performance metrics to demonstrate its effectiveness, robustness, and practicality in modern digital forensics investigations.

Abbreviations

DST	Dempster-Shafer Theory
IoT	Internet-of-Things
OLS	Ordinary Least Squares
PCAP	Packet capture

Acknowledgment

The authors would like to express their sincere appreciation to everyone who contributed to the completion of this research.

Funding Information

This research did not receive any funding.

Author’s Contributions

Mohamed El-Dosuky: Software implementation and edited.

Sherif K. Kamel: Conceptualization, identification of the research problem and supervision.

Mostafa M. El-Gayar: Writing the initial draft and edited.

Ethics

This piece of writing is unique and includes unreleased content. All co-authors have read and approved the article, and the corresponding author attests that there are no ethical concerns.

References

- Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A., & Abdulrahman, A. G. (2024). IoT Forensics: Current Perspectives and Future Directions. *Sensors*, 24(16), 5210. <https://doi.org/10.3390/s24165210>
- Ahmed, S. F., Shawon, S. S., Bhuyian, A., Afrin, S., Mehjabin, A., Kuldeep, S. A., Alam, Md. S. B., & Gandomi, A. H. (2025). Forensics and security issues in the Internet of Things. *Wireless Networks*, 31(4), 3431–3466. <https://doi.org/10.1007/s11276-025-03942-2>

- Al-Sadi, M. B., Chen, L., & Haddad, R. J. (2018). Internet of Things Digital Forensic Investigation Using Open Source Gears. *SoutheastCon 2018*, 1–5. <https://doi.org/10.1109/secon.2018.8479042>
- Alshabibi, M. M., Bu dookhi, A. K., & Rahman, M. M. H. (2024). Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. *Computers*, 13(8), 213. <https://doi.org/10.3390/computers13080213>
- Bezerra, E. D. C., Teles, A. S., Coutinho, L. R., & da Silva e Silva, F. J. (2021). Dempster–Shafer Theory for Modeling and Treating Uncertainty in IoT Applications Based on Complex Event Processing. *Sensors*, 21(5), 1863. <https://doi.org/10.3390/s21051863>
- Breitinger, F., Hilgert, J.-N., Hargreaves, C., Sheppard, J., Overdorf, R., & Scanlon, M. (2024). DFRWS EU 10-year review and future directions in Digital Forensic Research. *Forensic Science International: Digital Investigation*, 48, 301685. <https://doi.org/10.1016/j.fsidi.2023.301685>
- Chen, Q., Whitbrook, A., Aickelin, U., & Roadknight, C. (2014). Data classification using the Dempster–Shafer method. *Journal of Experimental & Theoretical Artificial Intelligence*, 26(4), 493–517. <https://doi.org/10.1080/0952813x.2014.886301>
- Fontani, M., Bonchi, A., Piva, A., & Barni, M. (2014). Countering anti-forensics by means of data fusion. *SPIE Proceedings*, 9569. <https://doi.org/10.1117/12.2039569>
- Friedl, S., & Pernul, G. (2024). IoT Forensics Readiness - influencing factors. *Forensic Science International: Digital Investigation*, 49, 301768. <https://doi.org/10.1016/j.fsidi.2024.301768>
- Gad, I. (2025). TOCA-IoT: Threshold Optimization and Causal Analysis for IoT Network Anomaly Detection Based on Explainable Random Forest. *Algorithms*, 18(2), 117. <https://doi.org/10.3390/a18020117>
- Hamda, N. E. I., Hadjali, A., & Lagha, M. (2023). Multisensor Data Fusion in IoT Environments in Dempster–Shafer Theory Setting: An Improved Evidence Distance-Based Approach. *Sensors*, 23(11), 5141. <https://doi.org/10.3390/s23115141>
- Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT Forensics: An Overview of the Current Issues and Challenges. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 223–254. https://doi.org/10.1007/978-3-030-60425-7_10
- Jayakrishnan, A. R., & Vasanthi, V. (2020). Internet of Things Forensics HoneyNetCloud Investigation Model. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 660–666. <https://doi.org/10.1109/icesc48915.2020.9155775>
- Kim, J., Park, J., & Lee, S. (2023). An improved IoT forensic model to identify interconnectivity between things. *Forensic Science International: Digital Investigation*, 44, 301499. <https://doi.org/10.1016/j.fsidi.2022.301499>
- Kim, S., Park, M., Lee, S., & Kim, J. (2020). Smart Home Forensics Data Analysis of IoT Devices. *Electronics*, 9(8), 1215. <https://doi.org/10.3390/electronics9081215>
- Montasari, R., & Hill, R. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 205–212. <https://doi.org/10.1109/icgs3.2019.8688020>
- Nieto, A., Rios, R., & Lopez, J. (2018). IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations. *Sensors*, 18(2), 492. <https://doi.org/10.3390/s18020492>
- Qian, H., Xia, L., Ge, R., Fan, Y., Wang, Q., & Jing, Z. (2025). From Black Boxes to Glass Boxes: Explainable AI for Trustworthy Deepfake Forensics. *Cryptography*, 9(4), 61. <https://doi.org/10.3390/cryptography9040061>
- Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2022). Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions. *IEEE Access*, 10, 110362–110384. <https://doi.org/10.1109/access.2022.3214506>
- Saleh, M., Othman, S. H., Driss, M., Al-dhaqm, A., Ali, A., Yafooz, W. M. S., & Emara, A.-H. M. (2023). A Metamodeling Approach for IoT Forensic Investigation. *Electronics*, 12(3), 524. <https://doi.org/10.3390/electronics12030524>
- Spiekermann, D., & Keller, J. (2023). Challenges of Network Forensic Investigation in Fog and Edge Computing. *Future Internet*, 15(10), 342. <https://doi.org/10.3390/fi15100342>
- Tian, Z., Jiang, W., Li, Y., & Dong, L. (2014). A digital evidence fusion method in network forensics systems with Dempster shafer theory. *China Communications*, 11(5), 91–97. <https://doi.org/10.1109/cc.2014.6880464>
- Wang, X., Wu, Y., Yu, D., Yang, Y., Ma, Y., & Chen, Y. (2023). IoT Device Identification Method Based on Causal Inference. *Electronics*, 12(12), 2727. <https://doi.org/10.3390/electronics12122727>
- Wei, Y., Wang, X., Nie, L., Li, S., Wang, D., & Chua, T.-S. (2023). Causal Inference for Knowledge Graph Based Recommendation. *IEEE Transactions on Knowledge and Data Engineering*, 35(11), 11153–11164. <https://doi.org/10.1109/tkde.2022.3231352>
- Xiao, X., Alharbi, K., Zhang, P., Qin, H., & Yue, X. (2025). Bayesian federated causal inference in manufacturing. *Journal of Intelligent Manufacturing*, 37(7), 2807–2831.

- Xing, W., Chen, C., & Xue, L. (2024). Deep learning-based causal inference architecture for stock prediction. *Electronics*, 13(11), 2056.
- Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced Digital Forensics and Anti-Digital Forensics for IoT Systems: Techniques, Limitations and Recommendations. In *Internet of Thing* (Vol. 19, p. 100544). <https://doi.org/10.1016/j.iot.2022.100544>
- Yang, J., Wen, J., Jiang, B., Song, H., Kong, F., & Zhen, Z. (2019). Multi-Sensor Information Fusion in Ocean of Things Based on Improved Adaptive Dempster-Shafer Evidence Theory. *2019 IEEE International Conference on Industrial Internet (ICII)*, 399–404. <https://doi.org/10.1109/ici.2019.00074>
- Zikria, Y. B., Ali, R., Afzal, M. K., & Kim, S. W. (2021). Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions. *Sensors*, 21(4), 1174. <https://doi.org/10.3390/s21041174>