International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| Volume 6 Issue 3 PP 103-112, 2025
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V6I3P112

Original Article

A Comprehensive Review of Telemetry Data-Driven AI Cybersecurity Solutions in IoT-Based Insurance Ecosystems

Subhojit Ghosh[1], Srinivas Dadi[2]
[1,2] Independent Researcher.

Received On: 02/07/2025 ***Revised On: 21/07/2025*** ***Accepted On: 23/08/2025*** ***Published On: 04/09/2025***

Abstract - *The Internet of Things (IoT), artificial intelligence (AI), and telematics are all contributing to the digitization of the insurance industry. Because of the Internet of Things' (IoT) explosive growth, insurance systems are now able to collect data in real time from linked devices like wearables, cars, and industrial sensors. While this connectivity enhances risk assessment, claims processing, and operational efficiency, it also introduces significant cybersecurity and privacy challenges. Improving cybersecurity in insurance ecosystems based on the IoT is the focus of this article, which offers a thorough analysis of AI solutions powered by telemetry. Discuss normal and adversarial scenarios in Industrial IoT environments, including scanning, denial-of-service, ransomware, backdoor, and injection attacks, and highlight the role of AI in automated threat detection, anomaly identification, and real-time mitigation. Furthermore, the paper examines AI applications in predictive underwriting, fraud detection, and usage-based insurance, alongside key challenges such as data privacy, legacy system integration, ethical concerns, and regulatory compliance. Finally, future directions, including privacy-preserving AI, Explainable AI, blockchain integration, and edge intelligence, are outlined to foster secure, transparent, and scalable adoption of AI in insurance. The study highlights the crucial role of telemetry-driven AI in developing resilient, equitable, and trustworthy insurance ecosystems.*

Keywords - *Internet of Things (IoT), Telemetry Data, Artificial Intelligence (AI), Cybersecurity, Insurance, Predictive Underwriting, Fraud Detection.*

1. Introduction

The field of cybersecurity has come a long way in the last several decades, as organizations and individuals have faced cybersecurity hazards in contemporary digital contexts that are becoming more complicated and frequent. To find known attack pathways, traditional defenses like firewalls, antivirus programs, and intrusion detection systems mostly relied on signature-based or pattern-matching techniques [1][2]. While these methods provided a foundational layer of security, their inability to detect novel or sophisticated threats rendered them increasingly ineffective over time [3][4]. As cybercriminals adopted advanced techniques, conventional defenses often lagged, leaving critical infrastructures and industries exposed to emerging risks.

The fast-growing Internet of Things (IoT) has also altered the cybersecurity environment, bringing both threats and opportunities. The industrial, healthcare, financial, and insurance sectors have adopted IoT, which has facilitated unmatched connectivity, efficiency, and data-driven decision-making [5][6]. The widespread integration of heterogeneous IoT hardware, most of which possess limited computational power and little in-built security, has, however, introduced new attack surfaces [7][8]. Cyber adversaries have taken advantage of these vulnerabilities, and they leverage the IoT devices as networks of computers that are exploited to carry out massive distributed denial-of-service (DDoS) attacks, disrupt the security of essential systems by enabling data breaches to take place, and conduct such attacks. IOT ecosystems, in turn, need more advanced levels of security paradigms that can be adjusted to the evolving threats [9].

Artificial intelligence (AI) cybersecurity is the most promising among such directions and is based on telemetry. Telemetry data, generated by IoT sensors, devices, and networks, provides real-time insights into system behavior and operational states. Telemetry-driven AI systems make anomaly identification, predictive threat intelligence, and automated incident response possible during the implementation of DL and ML models [10][11]. Unlike signature-based systems, these approaches analyze dynamic patterns, correlations, and contextual signals, thereby identifying both known and zero-day attacks. In insurance ecosystems, the integration of IoT and telemetry data has become particularly valuable [12]. For instance, telematics in vehicles, wearables in health insurance, and smart sensors in property insurance not only enhance risk assessment and underwriting but also require strong cybersecurity systems to safeguard private customer information and maintain confidence. It discusses the evolution of cybersecurity practices, highlights IoT-specific vulnerabilities, explores telemetry-enabled AI models, and evaluates their applications in safeguarding insurance operations.

1.1. Structure of the Paper

The paper is structured to provide a comprehensive review of telemetry-driven AI solutions in IoT-based insurance. Section II presents Cybersecurity in IoT-Based Insurance Systems. Section III discusses the AI-Driven Techniques for Telemetry-based Cybersecurity and Section IV explains the Application of Telemetry-Driven Ai Security

in Insurance Finally, Section V concludes the study and outlines future research directions.

2. Cybersecurity in IoT-Based Insurance Systems

The IoT has grown to become a crucial part of contemporary insurance networks, with devices such as wearables, smart vehicles, and home sensors generating vast amounts of real-time data [13]. This continuous data stream enables insurers to perform more accurate risk assessments, personalize policies, and enhance claims processing efficiency. By leveraging IoT data, insurers can proactively monitor risks and optimize coverage, leading to improved operational effectiveness and customer satisfaction. However, the extensive connectivity and data exchange inherent in IoT systems also introduce significant cybersecurity challenges.

2.1. Normal and Attack Scenarios

In Industrial IoT (IIoT) environments, systems operate under both normal and adversarial conditions. Understanding these scenarios is crucial to differentiating legitimate activities from malicious behaviors that threaten the security and reliability of connected devices.

- Prior to initiating a real attack, scanning is said to be the initial stage in which the information about the target system, including the ports that are open and the services that are available on the victim's device or sensor, is obtained by an attacker [14].
- Denial of Service (DoS) is a popular flooding attack in which a hacker usually initiates a series of malevolent efforts to prevent a genuine user from accessing resources. To launch this attack, one only has to connect too many IIoT devices at once, causing them to run out of resources, such as memory and CPU.
- Ransomware is an advanced kind of malware that encrypts systems or services to prevent authorized users from accessing them and then tries to sell the decryption key that allows access to the machine again. Similar in nature, an IoT ransomware prevents users from accessing IoT devices. IIoT apps and devices might be targeted by IoT ransomware since they often carry out essential tasks, and denying access to or locking down these apps might have disastrous results, including monetary losses for businesses [15].
- In a backdoor, an adversary can remotely gain unauthorized access to compromised IIoT devices with backdoor software. The enemy becomes a member of the botnets in an attempt to attempt a DDoS attack and uses the backdoor to claim control of the compromised IIoT devices.
- Injection attacks often strive to add harmful information or execute malicious software to the IIoT applications. Also, the injection attack can modify control instructions and telemetry of the IIoT system, disrupting normal processes.

2.2. AI Role in Improving IoT Security

The real-time data processing enables AI to offer automated responses to threats, which means it can identify a harmful action and initiate an automated response procedure without human intervention [16]. It is automation that comes in handy when a fast response is desired, e.g. stopping an attack or preventing damaged devices from being damaged. Systems of automated threat response and increased threat detection become possible due to AI integration. Artificial Intelligence-facilitated behavioral analysis is essential in constructing and maintaining a reference of normal usage of devices. AI systems may eventually pick up on and adapt to the typical activities of IoT devices, creating a profile of the expected interactions between them. and AI is able to identify abnormalities when there are departures from this trend. For instance, this method has worked well for detecting Android malware. The overall security of IoT devices may be improved by applying AI to identify and stop questionable activities by analyzing trends.

2.3. Artificial Intelligence in Insurance: Predictive Underwriting and Fraud Detection

The rise of AI and the expansion of the IoT are bringing to the underwriting and fraud detection processes for health and life insurance [17]. Medical examinations, protracted delays, and mountains of paperwork were once associated with underwriting. AI is already increasing speed, intelligence, and accuracy.

2.3.1. Improved Underwriting Made Possible by Artificial Intelligence

Artificial intelligence-powered underwriting algorithms almost instantly assess risk by utilizing wearable technology, electronic health records, and past medical claims. Using real-time health data and risk variable forecasting, AI allows insurance firms to establish policy pricing rather than using a predetermined strategy [18]. In only a few minutes, a person who has no history of smoking, frequent high activity levels, and regular heart rate patterns might be approved for life insurance at a lower cost. AI systems might assess future risks by analyzing family medical history and lifestyle decisions, making insurance more accurate and equitable.

2.3.2. Using Behavioral Analytics to Identify Fraud

The annual cost of insurance fraud can reach billions of dollars; AI greatly reduces this danger. Machine learning techniques find anomalies in transaction records, historical claims, and behavior patterns that can point to possible fraud. Someone who unexpectedly files many claims for minor injuries in multiple locations makes one wonder. The real-time detection of these variations by AI aids insurance companies in evaluating and preventing fraud prior to making payments.

2.4. Challenges in Implementing AI in Insurance

There are some related challenges to implementing AI in Insurance are as explained below and in Figure 1.

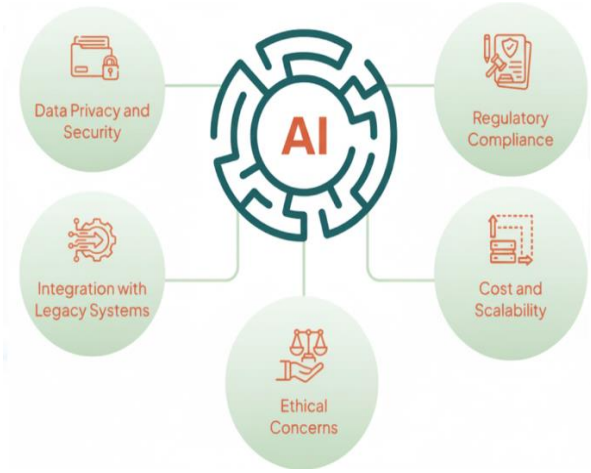

Fig 1: Challenges of AI in Insurance

2.4.1. Data Privacy and Security

AI relies significantly on contextualized and clean data, and dealing with such data places additional burdens on insurers.

- **Handling Sensitive Customer Information:** Insurance companies must protect the data of AI systems and make sure that it is protected from breaches and illegal access [19].
- **Compliance with Data Protection Regulations (e.g., GDPR, HIPAA):** Governments and regulatory agencies have begun imposing strict guidelines on data processing that must always be followed.

2.4.2. Integration with Legacy Systems

It is necessary to upgrade several additional peripheral systems in order to transition to an AI-powered process.

- **Adapting AI to Work with Outdated Infrastructure:** AI integration might be difficult with rigid legacy systems, requiring expensive improvements.
- **High Costs of System Upgrades and Integration:** The expense of this update might be high, particularly for smaller businesses.

2.4.3. Ethical Concerns

There have been, and may continue to be, some concerns about the impartiality and reliability of AI in making decisions.

- **Bias in AI Algorithms:** AI algorithms that have been biasedly trained produce unfair or skewed outcomes. as exorbitant prices or policy denials.
- **Transparency in Decision-Making Processes:** Insurance companies must be ready to defend AI choices to their clients.
- **Fairness in Premium Calculations:** To provide total fairness in premium computations, AI in insurance must be trained with extreme accurately.

2.4.4. Cost and Scalability

There are substantial expenses and scalability concerns associated with implementing AI.

- **High Initial Investment in AI Technology:** The initial investment required to integrate AI might be prohibitive for small and medium-sized enterprises [20].
- **Scalability Challenges for Small Insurance Firms:** The maintenance of the AI systems requires resources and experience in addition to the initial expenditure.

2.4.5. Regulatory Compliance

The rules that authorities have put in place surrounding AI should make insurers extremely cautious.

- **Navigating Complex Insurance Laws and Regulations:** The implementation of AI solutions is made more challenging by the requirement that they be created in accordance with national and international rules and regulations.
- **Ensuring AI Tools Meet Regulatory Standards:** Insurers must make sure that their systems are current and up to speed because the government may occasionally amend the requirements.

1. Bioenergy refers to electricity and gas that is generated from organic matter,
2. known as biomass. This can be anything from plant and timber to agriculture and food
3. waste and even sewage. Bioenergy includes the production of fuel from organic matter as
4. well. Energy from biomass can be used for electricity, heating, and transportation, and
5. can be replenished anywhere. Around seventy-five percent of the world's renewable
6. energy is composed of biomass energy due to its potential and wide use [7]. Also, it is
7. carbon-neutral, meaning that it adds no net carbon dioxide to the atmosphere. In addition,
8. it reduces the level of trash in the ground by as much as 90 percent by burning solid
9. waste. Biomass fuels, on the other hand, are not completely clean and can also cause
10. deforestation. They are also less efficient than fossil fuels. But proper management and
11. planning of its disadvantages will improve its potential.
12. Bioenergy refers to electricity and gas that is generated from organic matter,
13. known as biomass. This can be anything from plant and timber to agriculture and food
14. waste and even sewage. Bioenergy includes the production of fuel from organic matter as
15. well. Energy from biomass can be used for electricity, heating, and transportation, and
16. can be replenished anywhere. Around seventy-five percent of the world's renewable
17. energy is composed of biomass energy due to its potential and wide use [7]. Also, it is
18. carbon-neutral, meaning that it adds no net carbon dioxide to the atmosphere. In addition,
19. it reduces the level of trash in the ground by as much as 90 percent by burning solid

20. waste. Biomass fuels, on the other hand, are not completely clean and can also cause
21. deforestation. They are also less efficient than fossil fuels. But proper management and
22. planning of its disadvantages will improve its potential.

3. AI-Driven Techniques for Telemetry-Based Cybersecurity

In this era of lightning-fast technological development, the optimization and administration of complex networks is crucial for sectors as diverse as transportation, energy, healthcare, banking, and more. The rapidly growing area of real-time telemetry analytics is pivotal to this change, as it ensures the dependability, efficiency, and safety of networked systems.

3.1. Telemetry Dataset Based on Cybersecurity

This study may have made use of a variety of different datasets, each of which has offers both benefits and drawbacks when compared to the selected datasets. These include:

- The Bot-IoT model dataset was designed to use ML and DL algorithms for network forensics research and analysis. Five IoT scenarios are used: a weather station, a smart refrigerator, lights that turn on when motion is detected, a garage door that can be opened from a distance, and a thermostat that can be adjusted remotely [21][22]. The three types of attacks tested in these simulated environments include information gathering, denial-of-service, and information theft. The former two attacks are commonly used by botnets, while the latter two use protocols like Hypertext Transfer Protocol (HTTP) for both DoS and distributed denial of service (DDoS).
- A camera and a speaker were used to construct the IoT Network Intrusion Dataset (IoTNID) [23]. The dataset includes denial-of-service, man-in-the-middle, reconnaissance, and Mirai assaults. The Nmap tool was used to capture all attack packets except for the Mirai ones, which were produced on a laptop.
- A smart light from Philips, the HUE a Somfy smart door lock, an Amazon Echo, and a Light-Emitting Diode (LED) bulb were the components that made up IoT-23, a dataset [24]. 20 distinct malware scenarios and three benign situations were simulated on these devices. Botnet attacks, such as Mirai, Gafgyt, Torii, etc., were made available to any malware scenario. In order to identify malicious and benign traffic characteristics, this dataset underwent human analysis.
- MedBIoT is an attempt at simulating three physical devices and eighty virtual ones make up a medium-sized network. A fan, a light bulb, a lock, and a switch were the tools that were utilized. The system was vulnerable to three distinct botnet types: Tomori, BASHLITE, and Mirai [25]. The data in this dataset is intended to be used for the purpose of identifying botnet invasions.
- MQTT-IoT is an implementation of messaging Queue Telemetry Transport (MQTT), a publish/subscribe messaging protocol, is part of the middleware/application layer. All twelve IoT sensors were part of a simulated environment that included four hostile and one benign assault scenario [26]. Using ML algorithms for intrusion detection was the original intent of this dataset.
- The ToN_IoT dataset is named after its goal of addressing the characteristics of the IIoT and the IoT by gathering information from operating systems, network data, and telemetric sources.

3.2. Machine learning and Its Types

The area of study known as machine learning (ML) assists computers with comprehending and resolving issues without the need for direct programming. It analyses historical data to predict future results [27]. In this section, an attempt is made to provide a synopsis of ML architectures, classifications, and paradigms. This method of learning encompasses a wide variety of ML algorithms and organizes them into classes based on the task they perform or the complexity of their operations; these algorithms vary significantly from one another. Figure 2 shows the classification of ML algorithms into four groups: supervised, unsupervised, semi-supervised, and RL.

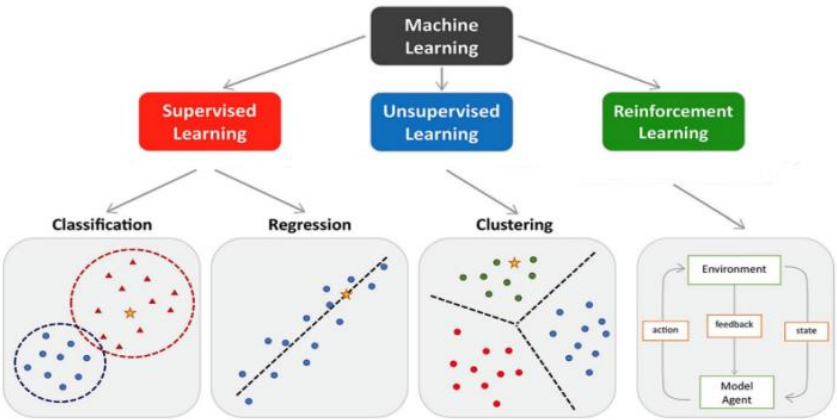

Fig 2: Main types of ML

- **Supervised learning:** The model is trained using a collection of labelled input-output pairs in supervised learning. As part of the process, data analysis is done to make an operation that maps inputs (x) to outputs (y). Common uses include regression and categorization.
- **Unsupervised learning:** In this technique, labeled data are not used in training, and it tries to find the patterns or structures existing in the data according to its intrinsic characteristics [28]. It lacks built-in labels or outputs, but rather it is concentrated on such activities as learning association rules, clustering, and dimension reduction. Attacks typically target language models employed in unsupervised learning.
- **Reinforcement learning:** Reinforcement learning (RL), which is based on trial-and-error learning, involves contact with the environment. Using past events, it makes predictions about what is likely to occur in the future. In this learning paradigm in particular, no privacy threats have been documented.
- **Semi-supervised learning:** This method, which combines elements of supervised and unsupervised learning, trains models with both labelled and unlabelled data. The labelled component is used to refine tasks, while the unlabelled data is used to improve interpretation. It is frequently used to solve problems with regression and classification [29].
- **Active learning:** Active learning techniques optimize the time and expense needed to collect labelled training data by carefully choosing training data to reduce the demand for large labelled datasets.
- **Ensemble learning:** In ensemble learning, many weak classifiers are combined to produce a powerful classifier that bases its judgements on the total of each model's predictions. Techniques that demonstrate ensemble learning processes include boosting and bagging.

3.3. Challenges in Implementing Security Telemetry

Although there are many benefits to security telemetry, there are also challenges in implementing it. A few typical obstacles include:

- **Unencrypted cybersecurity telemetry data:** A significant obstacle in security telemetry is the transfer of data without encryption. Telemetry data is vulnerable to interception or manipulation by hackers when transmitted across networks without encryption, the potential for man-in-the-middle attacks.
- **Data exposure and leakage:** Critical information regarding an organization's IT infrastructure is frequently included in security telemetry data [30]. This data is vulnerable to unscrupulous actors who might use it to gain unauthorized access to the IT environment or, worse, keep it captive for ransom if it is not encrypted.
- **Privacy concerns:** Significant privacy problems may arise from the collection of telemetry data, especially when tracking user activity. Implementing security telemetry in a company's network requires finding a balance between privacy and security.
- **Managing diverse data sources:** Organizations can gather a wide range of data sources for their security telemetry. A major difficulty is determining which sources to use, how to interpret this data, and where to keep it. It is crucial to preserve security and accessibility across various data sources and processing techniques.
- **Handling data in high volumes:** A significant amount of organized and unstructured data is produced by security telemetry. To manage this data thoroughly, efficient methods and procedures are required. At the same time, for cybersecurity data to be properly secured, processed, and stored around the clock, constant monitoring is essential.
- **Data governance and quality assurance:** It is essential to set up checks and balances to confirm the accuracy and integrity of data. It can be difficult to manage data uniformly across processes in complicated IT systems [31]. It is difficult to draw valuable conclusions from the data to improve security posture in the absence of strong data governance mechanisms.

4. Application of Telemetry-Driven AI Security in Insurance

The integration of telemetry data with AI-driven security mechanisms is transforming the insurance sector by enabling real-time monitoring, proactive risk assessment, and intelligent decision-making. Telemetry-driven security solutions leverage data collected from IoT devices, connected vehicles, wearable sensors, and smart infrastructure to enhance both operational resilience and customer trust.

4.1. Application of AI in insurance sectors

The application of AI in the automotive insurance industry. In order to improve claims processing, insurance pricing, risk assessment, and operational performance, they looked at a variety of strategies [32]. The key contributions are based on the following categorizations.

- **Insurance pricing and risk assessment:** The significance of risk exposure and driving behaviour components in insurance pricing models is emphasised in the article. Insurers may gain a better understanding of a driver's risk profile by integrating telematics data, such as "mileage driven," "speed limits exceeded," and "types of roads frequented."
- **Telematics and Usage-based Insurance (UBI):** The consequences of using telematics devices to collect proprietary data on customer Behavior, market competitiveness, and road safety. The study also focuses on creating a thorough framework for determining rates for Usage-based Insurance (UBI) products [33]. To improve risk categorization and forecast claim frequency, the framework skilfully blends several predictive models with data binning approaches (discrete binning).

- **Ethical considerations of AI in insurance:** The effects of big data analytics, machine learning, and AI on the insurance industry at several levels, such as product-market dynamics, Insurtech operations, and AI systems that act like people, and more [34]. In order to effectively handle ethical challenges, the study emphasises how important explainability, openness, and governance are for AI systems, underscoring the necessity of comprehending the complex relationships between technological and social systems.
- **Comparison of AI-based and Traditional Methods:** Provides insightful information for insurance sector decision-making, challenging the widely held belief that fraud detection methods based on AI are inherently more cost-effective. Their study's surprising finding was that, when tested on actual databases, the existing AI-based techniques for detecting vehicle insurance fraud were less economical than more conventional statistical-econometric approaches.

4.2. Key considerations for AI adaptation in insurance

The digital insurance industry might undergo an advancement in fraud detection, risk assessment, and customer service made possible by artificial intelligence [35]. The following crucial factors need to be taken into account to guarantee the effective and ethical application of AI in the insurance industry:

- **Data quality and governance:** An AI model cannot be successfully trained without high-quality data. Data governance can also be used to ensure the correctness, consistency, and security of an AI model by providing it with the information it needs to operate. The insurance market is not an exception.
- **Ethical considerations:** In order to prevent prejudice and discrimination, insurers should ensure that ethical considerations, such as equity, openness, and accountability of AI algorithms, are considered prior to the adoption of AI in the insurance processes.
- **Regulatory compliance:** The insurance industry must comply with security and privacy regulations when applying AI in its operations. Use of AI solutions by insurers requires the use of intricate law and regulation demands and data protection regulations in different jurisdictions.
- **Interpretability and explainability:** There is an immediate requirement to introduce AI models in a transparent and simple manner [36] so as to gain the confidence of the stakeholders and end users, explainable AI (XAI) methods can reveal the decision-making procedure of AI in the future, elevating the insurance practice to a higher moral and trusted level.
- **Innovation, continuous learning, and adaptation:** There has been a change in the insurance industry that has been characterized by innovation in all aspects such as product development as well as risk evaluation. As the risk environment is constantly evolving, insurers need to ensure that AI models are retrained on a regular basis as risk variables and fraud trends change to remain correct and current over time [37].
- **Cultural/societal acceptance:** The influence of digitalization in the insurance sector could be questioned by social and cultural apprehensions. The trust issue can be there since people can distrust the algorithm of decisions to prices of policies or allegations. It nice to have the human touch in such sensitive issues.

4.3. Benefits of AI in Pricing

The adoption of AI in auto insurance pricing models have a number of advantages:

- **Accuracy:** AI improves the accuracy of prices and considers more factors, including driving behaviour on the fly and environmental conditions [38]. This allows the insurers to offer more personalized rates that benefit the actual risk of a driver.
- **Fairness:** Insurers can ensure that the price setting model is fairer and more transparent through AI and its greater capability to analyze data, which will help build confidence with their policyholders.
- **Flexibility:** The AI can be applied to offer dynamic pricing, where premiums may be altered on-the-fly based on individual driving behaviour or changing external conditions, e.g. weather trends or the state of traffic [39].
- **Efficiency:** The AI-based pricing systems can replace manual data entry and analysis and enhance the underwriting process, besides reducing the administrative cost of insurers.
- **Customer Satisfaction:** The concept of individualized and precise pricing presumably results in increased rates of customer satisfaction since the policyholders feel that they are charged appropriately depending on their individual driving patterns and risk systems.

5. Literature Review

This literature reviews a full overview of telemetry-based AI-based cybersecurity solutions in IoT-supported insurance settings and what it can be applied to, what advantages and obstacles it brings to research, and what research should be done in the future. Paragioudakis, Smyrlis and Spanoudakis (2025) attacks become more sophisticated and frequent and holistic cyber insurance is necessary to account for remaining risks and ensure organizations are not at risk of facing devastating financial and reputational losses in case of such an attack. Nonetheless, insurers usually have difficulties with the effective measurement of cyber risk because of non-standardized data and dynamic threat vectors. Consequently, policies may be obsolete or provide a small scope of inconsistent coverage. This highlights the necessity to have more transparent and data-driven and flexible insurance that can be easily adapted to the demands of contemporary cybersecurity [40].

Sunna et al. (2025) Examine the history of cyberattacks, coverage plan issues, risk assessment of cyberthreats, and the assaults' dynamic character. It discusses how important AI is for figuring out cyber danger and protecting digital assets. The article explores the growth of cyber insurance in addition to outlining the many coverage possibilities, including first-party coverage for direct spending, third-party policies, and "silent cyber" coverage provided by standard policies. A thorough analysis of earlier studies emphasizes the potential benefits of AI for cybersecurity, the challenges encountered by insurers and policyholders, and the increase in advanced cyber threats in the years after the pandemic [41].

Jawhar et al. (2024). AI has been shown to be useful in a number of areas to improve cybersecurity, such as cyber threat assessments, cybersecurity awareness, and compliance. AI also offers tools for creating strategies, rules, processes, and cybersecurity training. However, managing and measuring cybersecurity risk assessment and cyber insurance is extremely difficult. Professionals in cybersecurity must be well-versed in cybersecurity risk factors and assessment methods. AI may therefore be a useful instrument for generating a more exhaustive and in-depth examination [42].

Patil and Patil (2024) implements design and deployment of a Vehicle Monitoring and Theft Prevention System (I-VMTPS) based on the IoT. The system is divided into two parts: part A is Monitoring and part B is theft prevention system. The reported system integrates existing technology such as GPS and GSM to monitor the vehicle. GPS is used in tracking systems and for SMS based communication GSM is used. GPS and GSM technology working together provide efficient, real-time vehicle location and log of owner information. Part B is a mechanism that makes vehicle theft almost impossible. Two security features are offered by the described system: a remote ignition cut-off mechanism and vehicle password protection [43].

Yang, Liang and Qi (2023) This study proposed A useful, non-intrusive technique for evaluating the risk of cyber security vulnerabilities because cybersecurity insurance companies are not allowed to evaluate policyholders' cybersecurity vulnerabilities before they sign an insurance without getting their permission or legal authority. Additionally, cybersecurity insurance providers seek policyholders' risk profiles for network security vulnerabilities in a convenient, quick, and affordable manner prior to policy signing. In model employs an ensemble ML approach to evaluate an organization's cyber vulnerability risk using only publicly available network information data and open-source intelligence. Comparing its accuracy rate to a rating derived from comprehensive data from cybersecurity specialists, it comes out at 75.6% [44].

Y et al. (2023) propose an automated method for managing the insurance industry's fraud detection procedure for auto insurance claims. To incorporate the benefits of each technique, the proposed study combines Particle Swarm Optimization (PSO), Genetic Algorithm (GA), and Federated Learning (FL). For the best feature subset extraction, the proposed model takes advantage of GA. Then, the optimized feature subset is loaded into a federated learning model that employs particle swarm optimization (FPSO). The findings show that the recommended hybrid model is 94.47% accurate. It might be made even better by using additional nature-inspired algorithms that are designed just for fraud detection [45].

Min, Zhao and Lu (2022) provide a framework and procedure for applying switching equipment's In-band Network Telemetry (INT) technology in intricate public packet networks to handle use cases including defect location, recovery, and network status monitoring. Implementing network telemetry in a cross-domain network is challenging, though. As a result, this study suggests a way to implement network telemetry in the tunnelling technique to handle use cases such as issue localization in cross-domain networks (complicated public packet networks), recovery, and keeping an eye on the state of the network [46].

6. Conclusion and Future Work

The rapid proliferation of the IoT is leading to insurance systems becoming increasingly data-driven and interconnected. The fusion of real-time telemetry with AI has emerged as a crucial enabler for improving risk management, fraud detection, and operational efficiency. At the same time, these advancements introduce new security, privacy, and ethical challenges that demand robust and adaptive solutions. In the paper, the author provides an overview of how telemetry-driven AI can be used to improve the cybersecurity of insurances based on the IoT by allowing proactive response to threats, the detection of anomalies, and automated response capabilities. Moreover, AI-based approaches are expected to improve predictive underwriting, automate claims and decrease fraud which, in the end, will make the process fairer, more transparent, and more reliable to the customers. However, challenges like interaction with existing systems and data privacy, algorithmic bias, and regulatory compliance still prove to be serious obstacles to major implementation.

Future research efforts should focus on privacy-sensitive AI interventions, such as homomorphic encryption and federated learning, to safeguard sensitive insurance and telemetry information. Transparency in underwriting and fraud detection can be guaranteed with the help of explainable AI (XAI). Blockchains combined with AI can increase the auditability and integrity of insurance transactions. The telemetry data at high velocity needs lightweight AI models that will be optimized to execute in the edge computing platform. Lastly, AI systems that operate within regulatory and ethical guidelines should be established to help the society accept and integrate sustainably in insurances ecosystems.

Table I categorizes prior research based on the approach, key findings, major challenges and highlights future research directions, such as integrating federated learning for privacy-preserving analytics, developing adaptive AI frameworks for evolving cyber threats.

Table 1: Summary of a Study on AI cybersecurity approaches within IoT-based insurance

Author	Study On	Approach	Key Findings	Challenges	Future Directions
Paragioudakis, Smyrlis & Spanoudakis (2025)	Cyber insurance and residual risk coverage	Analysis of challenges in cyber insurance policies	Highlighted that policies often outdated, inconsistent, and lack standardized data	Difficulty in quantifying cyber risk due to evolving threat vectors	Development of transparent, data-driven, and adaptable insurance solutions
Sunna et al. (2025)	Cyber insurance evolution and AI in cyber risk assessment	Literature analysis on coverage options and AI role	AI crucial for cyber risk assessment; explained coverage types (third-party, first-party, silent cyber)	Dynamic nature of cyberattacks, insurer/insured challenges	Leverage AI for adaptive insurance models and stronger digital asset protection
Jawhar et al. (2024)	The application of AI to insurance and cyber risk assessment	Application of AI in cybersecurity training, policies, and risk analysis	AI can enhance cyber threat assessments and compliance frameworks	Complexity in managing and measuring cyber risk for insurance	Use AI for comprehensive risk analysis frameworks
Patil & Patil (2024)	Vehicle monitoring and theft prevention system based on the IoT (I-VMTPS)	GPS + GSM integration with remote ignition cut-off and password protection	Real-time vehicle location tracking; improved theft prevention	Dependence on connectivity and hardware integration	Extend system with AI-driven anomaly detection and broader IoT integration
Yang, Liang & Qi (2023)	Non-invasive evaluation of cyber vulnerabilities for insurance	Ensemble machine learning using open-source intelligence	Achieved 75.6% precision in assessing cyber vulnerability without intrusive methods	Legal and authorization constraints in assessing policyholders	Enhancing precision and automation using additional data sources and ML models
Y et al. (2023)	Fraud detection in auto insurance	Hybrid model combining FL, GA, and PSO (FPSO model)	Improved fraud detection accuracy with optimized feature selection	Privacy preservation of insured data	Expand federated learning frameworks for large-scale fraud detection
Min, Zhao & Lu (2022)	INT (In-band Network Telemetry) in networks across domains	Application of INT with tunneling for fault detection & recovery	Effective in public packet networks for failure detection, recovery, and network state measuring	Hard to implement telemetry across domains	Advance cross-domain telemetry using tunneling and AI-driven network monitoring

References

[1] N. U. Prince *et al.*, "AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction," 2024. doi: 10.13140/RG.2.2.22975.52644.

[2] V. Verma, "Security Compliance and Risk Management in AI-Driven Financial Transactions," *Int. J. Eng. Sci. Math.*, vol. 12, no. 7, pp. 107–121, 2023.

[3] D. Patel, "Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 576–583, Dec. 2023, doi: 10.14741/ijcet/v.13.6.10.

[4] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.

[5] P. Radanliev, D. De Roure, C. Maple, J. R. C. Nurse, R. Nicolescu, and U. Ani, "AI security and cyber risk in IoT

systems," *Front. Big Data*, vol. 7, Oct. 2024, doi: 10.3389/fdata.2024.1402745.

[6] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[7] D. D. Rao, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," *J. Intell. Syst. Internet Things*, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.

[8] R. Patel, "Artificial Intelligence-Powered Optimization of Industrial IoT Networks Using Python-Based Machine Learning," *J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 138–148, 2023, doi: 10.56472/25832646/JETA-V3I8P116.

[9] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[10] K. Sutariya and K. K. Pramanik, "Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning," in *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, IEEE, Jan. 2023, pp. 1323–1328. doi: 10.1109/AISC56616.2023.10085343.

[11] R. Q. Majumder, "Machine Learning for Predictive Analytics: Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3557–3564, May 2025, doi: 10.38124/ijisrt/25apr1899.

[12] V. Shah, "Analyzing Traffic Behavior in IoT-Cloud Systems: A Review of Analytical Frameworks," *Int. J. Sci. Res. Comput. Sci. Eng. InfoShah, V. 'Analyzing Traffic Behav. IoT-Cloud Syst. A Rev. Anal. Fram. Int. J. Sci. Res. Comput. Sci. E*, vol. 9, no. 3, pp. 877–885, 2023, doi: 10.32628/IJSRCSEIT.

[13] A. Adewuyi *et al.*, "The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems," *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 379–394, Jul. 2024, doi: 10.30574/wjarr.2024.23.1.1993.

[14] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[15] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *Dep. Oper. Bus. Anal. Inf. Syst. (OBAIS*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

[16] R. Abreu, E. Simão, C. Serôdio, F. Branco, and A. Valente, "Enhancing IoT Security in Vehicles: A Comprehensive Review of AI-Driven Solutions for Cyber-Threat Detection," *AI*, vol. 5, no. 4, pp. 2279–2299, Nov. 2024, doi: 10.3390/ai5040112.

[17] V. K. Tarra, "Telematics & IoT-Driven Insurance with AI in Salesforce," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 5, no. 3, pp. 72–80, 2024, doi: 10.63282/3050-9416.IJAIBDCMS-V5I3P108.

[18] G. Mantha, "Transforming the Insurance Industry with Salesforce: Enhancing Customer Engagement and Operational Efficiency," *North Am. J. Eng. Res.*, vol. 5, no. 3, 2024.

[19] B. V. Swamy, P. P. Barmola, S. Thangavel, S. Kaliappan, H. Patel, and G. Abhyankar, "Cognitive Twins for Predictive Maintenance and Security in IoT Software Systems," in *2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, IEEE, Dec. 2024, pp. 1–8. doi: 10.1109/ICMNWC63764.2024.10872082.

[20] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, pp. 2102–2106, Nov. 2022, doi: 10.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[21] S. Haque, F. El-Moussa, N. Komninos, and R. Muttukrishnan, "A Systematic Review of Data-Driven Attack Detection Trends in IoT," 2023. doi: 10.3390/s23167191.

[22] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, IEEE, Feb. 2025, pp. 431–436. doi: 10.1109/ESIC64052.2025.10962752.

[23] A. R. Bilipelli, "Forecasting the Evolution of Cyber Attacks in FinTech Using Transformer-Based Time Series Models," *Int. J. Res. Anal. Rev.*, vol. 10, no. 3, pp. 383–389, 2023.

[24] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[25] V. Shah, "Traffic Intelligence in IoT and Cloud Networks: Tools for Monitoring, Security, and Optimization," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024.

[26] S. Thangavel, "AI Enhanced Image Processing System For Cyber Security Threat Analysis," 2024

[27] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *J. Big Data*, vol. 11, no. 1, p. 105, Aug. 2024, doi: 10.1186/s40537-024-00957-y.

[28] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[29] S. Pandya, "A Machine and Deep Learning Framework for Robust Health Insurance Fraud Detection and Prevention," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1332–1342, Jul. 2023, doi: 10.48175/IJARSCT-14000U.

[30] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[31] H. Kali, "Optimizing Credit Card Fraud Transactions identification and classification in banking industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 85–96, 2024.

[32] S. Bhattacharya, G. Castignani, L. Masello, and B. Sheehan, "AI revolution in insurance: bridging research and reality," *Front. Artif. Intell.*, vol. 8, Apr. 2025, doi: 10.3389/frai.2025.1568266.

[33] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions : A Case Study Using Real-Time Data Streams," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[34] H. Kapadia and K. C. Chittoor, "Quantum Computing Threats to Web Encryption in Banking," *Int. J. Nov. Trends Innov.*, vol. 2, no. 12, pp. a197–a204, 2024.

[35] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data Inf. Manag.*, vol. 8, no. 2, p. 100063, Jun. 2023, doi: 10.1016/j.dim.2023.100063.

[36] H. Kali and G. Modalavalasa, "Artificial Intelligence (AI)-Driven Business Intelligence for Enhancing Retail Performance with Customer Insights," *Asian J. Comput. Sci. Eng.*, vol. 9, no. 4, pp. 1–9, 2024, doi: 10.22377/ajcse.v10i2.210.

[37] N. Malali, "Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in Finance," in *2025 International Conference on Advanced Computing Technologies (ICoACT)*, IEEE, Mar. 2025, pp. 1–6. doi: 10.1109/ICoACT63339.2025.11005357.

[38] J. Paul, "AI-Powered Data Analytics: Shaping the Future of Auto Insurance Pricing and Claims Processing," 2024.

[39] H. P. Kapadia and K. B. Thakkar, "Generative AI for Real-Time Customer Support Content Creation," *J. Emerg. Technol. Innov. Res.*, vol. 10, no. 12, pp. i36–i43, 2023.

[40] A. Paragioudakis, M. Smyrlis, and G. Spanoudakis, "ERMIS: A Cybersecurity Market for Assurance and Insurance-as-a-Service," in *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, Aug. 2025, pp. 765–770. doi: 10.1109/CSR64739.2025.11130152.

[41] A. A. Sunna, T. Sultana, N. Kshetri, and M. M. Uddin, "AssessCICA: Assessing and Mitigating Financial Losses from Cyber Attacks with Role of Cyber Insurance in Post-Pandemic Era," in *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*, 2025, pp. 1–6. doi: 10.1109/ISDFS65363.2025.11012092.

[42] S. Jawhar, C. E. Kimble, J. R. Miller, and Z. Bitar, "Enhancing Cyber Resilience with AI-Powered Cyber Insurance Risk Assessment," in *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2024, pp. 0435–0438. doi: 10.1109/CCWC60891.2024.10427965.

[43] A. Patil and S. Patil, "IoT Enabled Vehicle Monitoring and Theft Prevention System (I-VMTPS)," in *2024 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC)*, IEEE, Nov. 2024, pp. 1–7. doi: 10.1109/AKGEC62572.2024.10869260.

[44] J. Yang, L. Liang, and J. Qi, "A Practical Non-Intrusive Cyber Security Vulnerability Assessment Method for Cyber-Insurance," in *2023 8th International Conference on Data Science in Cyberspace (DSC)*, IEEE, Aug. 2023, pp. 261–269. doi: 10.1109/DSC59305.2023.00045.

[45] S. Y, N. Victor, G. Srivastava, and T. R. Gadekallu, "A Hybrid Federated Learning Model for Insurance Fraud Detection," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, May 2023, pp. 1516–1522. doi: 10.1109/ICCWorkshops57953.2023.10283682.

[46] C. Min, D. Zhao, and H. Lu, "The Processing Method of the Message Based on the In-band Network Telemetry Technology," in *2022 International Conference on Service Science (ICSS)*, IEEE, May 2022, pp. 21–24. doi: 10.1109/ICSS55994.2022.00013.