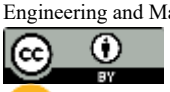
TRADE SECRET PROTECTION IN INDUSTRIAL IOT DATA SHARING RISKS, REGULATORY GAPS, AND A CONCEPTUAL FRAMEWORK FOR PROTECTION

B M Manohara ,Bhavika Bandu, Garvit Choudhary

How to Cite this Article:
Manohara, B. M., Bandu, B. & Choudhary, G. (2026). TRADE SECRET PROTECTION IN INDUSTRIAL IOT DATA SHARING RISKS, REGULATORY GAPS, AND A CONCEPTUAL FRAMEWORK FOR PROTECTION. International Journal of Creative and Open Research in Engineering and Management, 02(6). https://doi.org/10.55041/ijcope.v2i6.061



https://doi.org/ 10.55041/ijcope.v2i6.061

ABSTRACT

By facilitating constant data interchange between sensors, machinery, and industrial platforms, the Indus- trial Internet of Things (IIoT) has completely transformed production. The hazards of IIoT data sharing to trade secrets are examined in this study from three perspectives: the business risk of unapproved data reuse, legal ambiguities about the ownership of machine-generated data, and technical shortcomings in IIoT architecture. It further develops a tiered conceptual framework that makes use of privacy-preserving monitoring techniques to strengthen trade secret protections in IIoT ecosystems, blockchain-based governance to establish transparency and traceability of data access, and trusted execution environments for secure data processing.

Keywords: Industrial Internet of Things, Trade Secrets, Data Sharing, Data Governance, Cybersecurity, Regulatory Gaps

I. INTRODUCTION

The integration of sensors, actuators, and linked devices in industrial infrastructure that allow real-time data collecting in industries including manufacturing, energy, logistics, and supply chain management is known as the Industrial Internet of Things (IIoT). Industries have also transitioned over the last ten years from the automation-focused Industry 4.0 paradigm to Industry 5.0, which emphasizes reliable and human-centric industrial intelligence (Zhao et al., 2026). Data is becoming a key component of efficiency and competitive advantage rather than a consequence of industrial activity, which has accelerated the deployment of interconnected industrial systems.

Data sharing between devices, platforms, and organizations is the value of IIoT. Continuous data interchange between manufacturers, suppliers, and service providers is essential for autonomous quality control, supply chain optimization, and predictive maintenance (Liu et al., 2026). But there's a cost to this. Some of an organization's most private information, such as proprietary algorithms, production specifications, process expertise, and performance benchmarks, is also contained in the same data.

These types of data are covered by the legal definition of trade secrets. Any information that has commercial value derived from its confidentiality, is not widely known to others, and is subject to reasonable measures taken by its owner to maintain confidentiality is considered a trade secret (José, 2026). Trade secrets can safeguard a wider variety of industry knowledge and do not need to be formally registered like patents or copyrights do.

This comprises performance data, sensor calibration parameters, and predictive maintenance models in the context of IIoT, in addition to software code or algorithms.

Trade secret law is built on the principle of control, requiring owners to actively restrict access to protected information (José, 2026; Kwon et al., 2023). IIoT, by contrast, is designed for openness, requiring data to flow continuously across devices, networks, and organizational boundaries to deliver its core value. The conditions that make IIoT valuable are therefore the same conditions that make trade secret protection difficult. Every data sharing agreement, third-party analytics platform, and cross-border data transfer represents a potential point at which confidentiality can erode.

Owners must deliberately limit access to protected knowledge under trade secret legislation, which is based on the control principle (José, 2026; Kwon et al., 2023). In contrast, IIoT is built for transparency; in order to provide its fundamental value, data must constantly move across devices, networks, and organizational boundaries. Therefore, the same factors that make IIoT lucrative also make trade secret protection challenging. Confidentiality may be compromised in any cross-border data transmission, third-party analytics platform, and data sharing agreement.

In addition to identifying the regulatory gaps that current frameworks fail to fill, this paper looks at the technical, legal, and business risks that IIoT poses to trade secret protection. It also suggests a layered conceptual protection framework that incorporates technical controls, governance mechanisms, and monitoring systems. The current legal and regulatory frameworks are reviewed in Section II. The hazards to trade secrets resulting from IIoT data sharing are examined in Section III. The main regulatory inadequacies are listed in Section IV, and the conceptual protection framework is suggested in Section V.

II. EXISTING LEGAL AND REGULATORY FRAMEWORKS

A. Trade Secret Protection Laws

The European Union Trade Secrets Directive offers civil remedies and a precise definition of trade secrets that must be implemented in every Member State (José, 2026). Prior to this Directive, trade secret protection varied greatly throughout EU member states, making it difficult for enterprises to traverse borders. According to the Directive, information must be confidential, have commercial value, and adhere to the owner's reasonable efforts to maintain confidentiality. It was a step in the direction of coordinated defense.

A federal civil cause of action for trade secret misappropriation was established in the United States by the Defend Trade Secrets Act, allowing businesses to file a lawsuit and pursue relief in federal courts (Kwon et al., 2023). Trade secret protection was only managed by state law prior to this Act, which resulted in varying standards between jurisdictions. All financial, commercial, scientific, and technical information is covered by the Act's wide definition of trade secrets, as long as the owner has taken appropriate precautions to keep it hidden.

There are no specific trade secret laws in Indian territory. Instead, they are legally protected, mostly through contract law, which is predicated on confidentiality clauses and non-disclosure agreements, with courts using the concepts of breach of contract and breach of confidence to resolve disputes (José, 2026). This method means that protection is only as strong as the agreements in place because the contracting parties bear the entire weight of protection. When trade secret issues occur, especially in cross-border situations involving foreign corporations, Indian enterprises confront considerable ambiguity due to the lack of a formal framework.

B. Data Governance Frameworks

Laws governing the gathering, processing, and transfer of personal data are provided by the General Data Protection Regulation (GDPR) (José, 2026). The GDPR's principles of data reduction, purpose limitation, and consent have a big impact on IIoT data sharing policies, even if its main focus is on individual privacy rights.

Companies running IIoT systems in the EU have a dual compliance burden as they must manage both GDPR regulations and trade secret protection.

In order to preserve ethical data policy, interoperability, and cross-border information flow, the Organization for Economic Co-operation and Development (OECD) has formulated data governance guidelines (José, 2026). These guidelines will assist businesses and governments in managing data as a shared resource. The OECD principles are helpful in formulating policy, but they are not legally binding and do not address trade secret protection.

The reference architecture for the safe and independent exchange of data between organizations is provided by the International Data Spaces Association (IDSA) model (José, 2026). The first step is data sovereignty, which allows businesses to choose how their data is used even after it has been shared. This approach is basically a technological and organizational standard rather than a legally binding framework, even though it logically supports trade secret protection objectives.

III. TRADE SECRET EXPOSURE IN IIOT: TECHNICAL, BUSINESS, AND LEGAL RISK DIMENSIONS

A. Technical Risks to Trade Secret Confidentiality

The technological dangers associated with IIoT data sharing are features of a network composed of linked devices rather than software defects (Urquhart & McAuley, 2018; Li et al., 2025). The terminal layer, which consists of the sensors and actuators that carry out sensing and data collection, is the foundation of an IIoT system. The majority of IIoT sensors often have limited memory, processing power, and energy capacity (Urquhart & McAuley, 2018). These restrictions make it impossible to install security features like multi-factor authentication or high-grade encryption directly on the device. In the end, this confidential operational data is gathered at the terminal layer and sent with minimal security, making it vulnerable to interception.

Within intricate, interconnected IIoT networks, the risk is higher (Urquhart & McAuley, 2018; Li et al., 2025). A vulnerability in a networked component could spread throughout the entire infrastructure in conventional industrial settings, where a single machine failure was a confined incident. Even if a company has internal security measures in place, it is still vulnerable to the weaknesses of the partners they exchange data with. It is not necessary to acquire such trade secrets from their proprietor. A weaker node in the shared network may be able to retrieve them.

Additionally, the industrial assets are at risk. Legacy systems, which have lifespans of decades and outlive the software and firmware support cycles, are used in many IIoT implementations (Urquhart & McAuley, 2018). These systems offer basic security protections and were never intended to be networked. They provide a vulnerability when incorporated into contemporary data-sharing systems, giving hackers access to the confidential business information they hold.

Risk Factor	**Mechanism**	**Vulnerability**
Resource Constraints	Limited processing power, memory, and energy in edge devices	Weak or no encryption and authentication mechanisms
Layer Integration Complexity	Interaction between device, network, and cloud layers	Higher risk of insecure interfaces and data exchange points
Legacy Systems	Use of outdated industrial systems not designed for connectivity	Security flaws that cannot be patched easily

Communication Limitations	Low-bandwidth and unstable industrial communication environments	Increased chances of data loss and interception
Device Density	Large number of interconnected sensing devices	Higher risk of data leakage and sensitive information exposure

TABLE I: Technical Risk Factors and Vulnerabilities in IIoT Systems

IIoT connections lead to attacks targeting confidential industrial data in addition to those architectural flaws. By taking advantage of inadequate device authentication, distributed denial of service attacks interfere with operations (Urquhart & McAuley, 2018). Man-in-the-Middle attacks reveal private operational information to unapproved parties by intercepting data packets while they are being transmitted across networks (Li et al., 2025). The most concerning is data integrity manipulation, in which an attacker manipulates sensor data to trick systems and cause operational errors that seem unintentional while concealing process knowledge theft (Liu et al., 2026; Li et al., 2025).

B. ***Business Risks to Competitive Advantage***

The economic ramifications of trade secret leakage are critical for industrial firms in IIoT contexts. Loss of competitive advantage is the main danger (Li et al., 2025; Dao et al., 2026). Businesses take advantage of weaknesses in common industrial networks to steal performance data, research standards, and procedures. In the IIoT, this theft is extremely covert. Instead of obtaining a blueprint directly, an attacker gathers manufacturing line performance data and uses it to reverse engineer the aspects that contribute to a competitor's efficiency (Dao et al., 2026).

Insider threat also matters a lot. With the permission that IIoT systems require during maintenance, employees or contractors who have real access may download and transfer sensitive data sets to competitors (Li et al., 2025). Because IIoT environments involve interconnectivity among multiple actors, the trust boundary is wide. Internal actors are allowed access to data that should have been kept restricted. The growth of large language models and machine learning tools has now introduced a new layer of danger. The sharing of sensor data within organizations is a matter of competition because when data is shared with a third- party platform, they can enter the domain and develop new models which could in turn be used to serve their own competitor's needs (Liu et al., 2026; Dao et al., 2026). Previous studies have shown that machine learning algorithms can learn and remember private training data and a competitor might employ an extraction attack to extract the private data from the shared model (Liu et al., 2026). When industrial data such as this type of data is passed onto any competitor the creator is no longer masters of spreading and reproducing it.

When data sharing does not align with company goals, risk also arises. To save money, a company may give operational data to a vendor without realizing that the data could be sold illegally (Dao et al., 2026). In the end, a company's reputation in the market may eventually suffer as a result of this misalignment of data sharing with commercial objectives.

C. ***The Legal Ownership Paradox***

Because machine-generated data is not considered property under the law, IIoT data sharing indicates a deeper problem. In this intellectual property paradigm, businesses expect the data generated by their machines to be their own, yet this is not the case. Under existing legislation, most nations only allow material that falls into one of five traditional categories: trade secrets, industrial designs, patents, trade- marks, or copyrights (Dao et al., 2026). Data is frequently seen as free-flowing information if it does not fit into one of these categories. The problem with IIoT data is that human authorship is required by copyright law. The United States Copyright Office confirmed in 2022 that automated systems that create content fully by themselves cannot be copyrighted

as copyright protection requires a meaningful connection between human creativity and the final output (Dao et al., 2026).

Control is achieved through rights of access because data cannot be owned in the conventional legal sense. Frameworks such as GDPR regulate personal data as an individual's right rather than the company's private asset. Contracts such as terms of service give control over non-personal industrial data (Dao et al., 2026). However, only parties who have signed a contract are bound by it. The original owner cannot make a direct legal claim against any third party that obtains the data.

Complicating matters further is the processing of derived data. Legal disputes arise from the fresh insights that are produced when a vendor processes a customer's raw data. Customers protest that ownership should belong to the original data source, but vendors frequently claim ownership of derived data because their proprietary algorithms produced it (Dao et al., 2026). However, this means that many of the most valuable, possibly proprietary deliverables a firm creates can legally go to someone else, even if the company claims to have secured its data by contractual agreements.

IV. ANALYTICAL ASSESSMENT OF REGULATORY GAPS

A. The Problem of Proving Misappropriation

Applying trade secret law to IIoT applications presents certain difficulties when it does exist. Many indus- trial datasets are semi-public compilations, indicating that while individual data may have no significance, the combination of these data may have private value (Dao et al., 2026). Consider a smart factory that collects thousands of sensor readings every hour. The total dataset offers exclusive information regarding manufacturing efficiency, even though each reading can be useless. Whether or not such aggregations qualify for trade secret protection has not been decided by the courts.

Distinguishing misappropriation from various routes of data exposure becomes challenging. Determining whether data was intentionally stolen or unintentionally disclosed due to a technological vulnerability is challenging in an IIoT community with numerous suppliers and automated processes (Li et al., 2025; Dao et al., 2026). In the system logs, a rival obtaining a manufacturer's process data through an incorrect API endpoint seems to be standard data access. It is nearly tough to prove improper means as required under trade secret legislation.

Owners of trade secrets are required to take prompt action when they suspect theft (Dao et al., 2026). However, a business may not realize that its trade secrets have been compromised for years in a setting where IIoT data flows are nearly automated and never stop. By the time it is found, the statute of limitations might have elapsed.

B. The Continuous Sharing Conflict

The foundation of trade secret legislation is the idea that confidential information is only disclosed under strict guidelines. That notion is totally disproved by IIoT. In the context of smart manufacturing, sensors quickly send operational data to different systems that rely on automated procedures without human intervention (Urquhart & McAuley, 2018; Dao et al., 2026). Trade secret law cannot be applied to a specific moment of dissemination. Only the bare minimum of data must be gathered for a particular purpose, according to frameworks like the GDPR (José, 2026). However, because value arises from patterns across huge datasets, IIoT systems are specifically built to gather as much data as possible.

Informed consent is a prerequisite for sharing or processing data under traditional data governance frameworks (José, 2026). Consent cannot be controlled transaction by transaction in an IIoT. Decisions about sharing are made by automated algorithms in milliseconds, which is faster than any consent mechanism could function. Ultimately, data exchange in IIoT systems nearly invariably surpasses all relevant regulatory frameworks.

C. Cross-Border Enforcement Breakdown

IIoT data flows are worldwide. Sensors providing data to cloud platforms in one nation, vendors processing it in another, and partners analyzing it in a third might all be part of a single manufacturing operation. Data enters conflicting regulations that no single framework can resolve as soon as it crosses an international boundary, leaving its original jurisdiction's legal protection (Li et al., 2025; Dao et al., 2026). A business that operates in both the US and the EU may be subject to GDPR regulations that restrict cross-border data transfers and US regulations that mandate data disclosure (José, 2026). One framework may be violated by adhering to another.

Another level of complexity is introduced by data localization rules. Certain types of data must only be kept on domestic servers in nations like China and Russia (Dao et al., 2026). This entails duplicating infrastructure across several locations, which raises operating expenses for multinational manufacturers. In contrast to a cohesive environment, each of these interfaces offers a chance for trade secret exposure.

Governments can override privacy and data protection guarantees on the basis of national security ac- cording to exemptions included in national frameworks (José, 2026). The extent of these exclusions has grown dramatically as governments view industrial data as a matter of national strategic interest. This implies that government action may stop the legal safeguards that industrial firms rely on to preserve trade secrets at any time.

V. A LAYERED CONCEPTUAL FRAMEWORK FOR TRADE SECRET PROTECTION IN IIOT

A. Overview of the Framework

Data sharing between sensors, edge devices, and industrial systems is made possible by the Industrial Internet of Things (IIoT) technology, which raises concerns about protecting the sensitive data. Industrial data protection necessitates a mix of many security methods, as numerous studies show. In addition to allowing data to be shared throughout industrial systems, these procedures can help firms manage sensitive information. Three primary types of protection methods are typically discussed in the literature: decentralized data governance models, trusted infrastructure systems, and privacy-preserving monitoring techniques (Imran, 2026; Sengupta et al., 2023; Goutam et al., 2026).

Trusted infrastructure technologies contribute to the creation of secure environments by facilitating the safe processing of sensitive data and computations. Implementing Trusted Execution Environments (TEEs), which allow crucial activities to operate inside secured hardware areas, is a popular method (Imran, 2026). Another method has focused more on blockchain governance, where data transactions are documented on distributed ledgers and smart contracts are used to decide how to share the data to improve accountability and transparency among the organizations (Sengupta et al., 2023). Additionally, companies may detect unwanted access and hold IIoT systems responsible for their activities by using privacy-preserving monitoring techniques to securely record device operation and data access events (Goutam et al., 2026).

These processes work together to create the multi-level protection that includes monitoring systems, governance procedures, and secure infrastructures. When it comes to IIoT industrial data sharing in IIoT contexts, integrated models could improve security and accountability.

B. Trusted Infrastructure Mechanisms for Secure Industrial Data Processing

A crucial component of safeguarding sensitive data in industrial IoT systems is trusted infrastructure. In these settings, a lot of gadgets collect and utilize operating data. However, disclosing these data or algorithms could result in the loss of important information. Therefore, secure environments that allow critical procedures to be carried out safely are desperately needed. One method has been proposed by research using Trusted Execution

Environments (TEEs). A TEE is a protected section of a processor that allows specific tasks to be performed safely and independently from the remainder. This suggests that even if other parts of the device or operating system are compromised, proprietary algorithms and sensitive data can be handled within this restricted area (Imran, 2026).

A more straightforward illustration would be a smart factory that uses machine data to forecast which parts would break. A company's algorithm may be used by the data to create such a forecast. By using this algorithm in a trusted execution environment, the business will be able to give the model and sensor data a safe environment while still allowing the system to evaluate machine performance. This allows enterprises to benefit from IIoT data analysis while maintaining their delicate industrial processes.

C. ***Blockchain-Based Data Governance for Industrial Data Sharing***

Manufacturers, suppliers, and service providers work together to create industrial IoT systems. Since such data is frequently shared under a single umbrella across business boundaries, it becomes crucial for everyone to understand how data can and cannot be accessed and used. Studying blockchain as a governance system for industrial data exchange is a suitable strategy to solve the issue.

Blockchain is built on a distributed ledger, which implies that rather than a single database, transactions are stored by multiple network participants. It is extremely difficult to amend or remove data once it has been entered into the ledger (Sengupta et al., 2023). Smart contracts are an additional functionality. These are automated programs that impose restrictions on the usage and access of data. For instance, a business may permit partner businesses to sort through specific machine data, but restrict the reuse of that data. These requirements might be automatically enforced by smart contracts, which would also record each access event on the ledger (Sengupta et al., 2023).

A practical example can be seen in industrial supply chains where machine performance data is shared with maintenance providers. Using a blockchain-based system, each data request and transaction can be logged transparently. This allows all participating parties to verify how the data was used, increasing trust between organizations.

D. ***Privacy-Preserving Monitoring and Logging Mechanisms***

In industrial IoT sites, ongoing monitoring is crucial in addition to data access control and infrastructure security. IIoT systems consist of a collection of linked devices that communicate often, therefore it's critical to monitor how data moves through the system and how those devices interact with one another.

Because of this, researchers have created privacy-preserving logging frameworks that actively monitor devices and safeguard sensitive data. To ensure that only authorized users can access logs, these systems store them on a secure medium. Once the logs are put up, the integrity guarantee and privacy management techniques ensure that they cannot be tampered with or altered. Secure device logs, which document important system information such as device authentication, data requests, and communication between system components, are the foundation of the framework described in (Goutam et al., 2026). The logs show anomalous behavior and provide organizations with information about how devices function within the IIoT network.

For instance, numerous sensors continuously transmit data to monitoring systems in a smart manufacturing setting. The logging system can record the activities and notify system administrators if an unidentified device attempts to request or utilize this data. The logs can also be used to investigate the occurrence in the future because they are safely stored.

E. Integrated Protection Framework for Industrial Data in IIoT

The various security needs in industrial IoT contexts are addressed by the techniques covered in the preceding sections. Combining these mechanisms creates a comprehensive set of safeguards that protects sensitive industrial data, even if each one provides a certain degree of protection.

Security is implemented as a layered structure in this integrated paradigm. Industrial data processing within platforms and devices is protected by the infrastructure layer. Above this, the governance layer regulates how various organizations and stakeholders share data. Last but not least, by documenting device interactions and data access events, the monitoring layer offers insight into system activities.

In order to provide risk-oriented protection, these layers work in concert. Monitoring systems assist in identifying anomalous activity and upholding responsibility, governance defines the methods by which information flow is controlled between partners, and secure infrastructure guarantees that basic calculations occur in safe surroundings. When these components are combined, firms can increase collective sharing and gain greater control over proprietary industrial information.

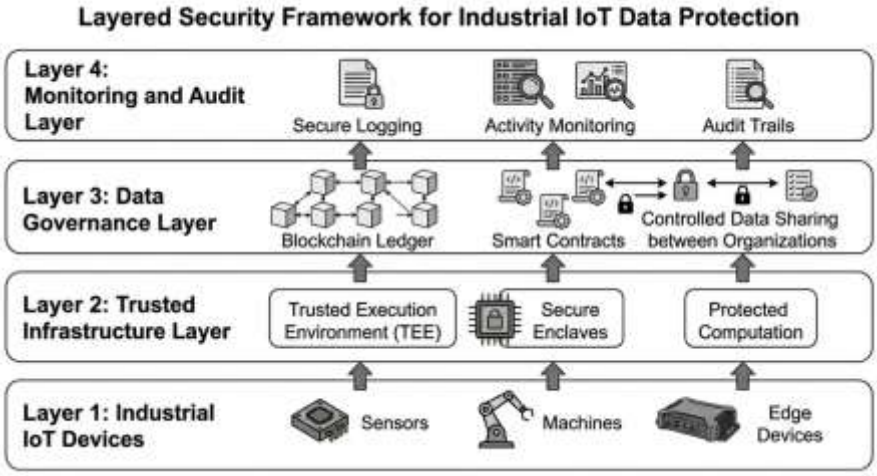


Fig. 1: Proposed layered architecture integrating trusted infrastructure, blockchain governance, and monitoring mechanisms.

F. Illustrative Case Study: Secure Data Sharing in a Smart Manufacturing Environment

We may use Smart Manufacturing, where sensors continuously gather data from manufacturing units, to learn how these mechanisms can work together in real-world scenarios. This information is utilized to predict potential equipment failure as well as track machine performance.

In this case, machine data analysis can be performed within Trusted Execution Environments, guaranteeing that data and models are safe even in the event that other components are compromised (Imran, 2026). Blockchain-enabled governance systems can manage data sharing if the manufacturer is obliged to provide specific information to an outside maintenance provider. A smart contract will automatically record the instance as an access event on a distributed ledger and can specify the conditions under which the maintenance provider should be permitted to utilize the data (Sengupta et al., 2023).

To record device activity and data access across the network, secure monitoring and logging are in place. The system will record and notify the administrators whenever an unauthorized device attempts to get private information. When assessing security occurrences, these records provide reliable proof (Goutam et al., 2026). This tiered approach allows for the release of operational data while retaining control over industry knowledge and proprietary models.

VI. CONCLUSION

Industries now create and trade value more quickly than the legal frameworks meant to protect it because of the Industrial Internet of Things. This study has demonstrated that trade secret risks for IIoT environments are not limited to technical flaws but also encompass business operations and the structural shortcomings of current legal frameworks, creating a multifaceted exposure that cannot be mitigated by a single protective mechanism.

The US Defend Trade Secrets Act, the EU Trade Secrets Directive, and India's contract-based approach are examples of legislative frameworks that were created for a world of intentional, discrete information transactions. Fundamentally, they struggle with the ongoing, automated, international nature of IIoT data flows. When data is continuously transferred between linked systems, it becomes more difficult to prove misappropriation. When data moves between jurisdictions with competing regulatory frameworks, protection enforcement is almost difficult. Furthermore, it is challenging to demonstrate the reasonable safeguards required by trade secret law when the volume and speed of IIoT data exchange greatly exceeds the capabilities of conventional security procedures.

This paper's tiered conceptual framework offers an organized approach to addressing these issues. Organizations can simultaneously address trade secret protection at the technical, legal, and organizational levels by combining trusted execution environments that offer secure computation, blockchain governance to create transparent and enforceable data sharing, and privacy preservation with ongoing oversight around monitoring. It is crucial to remember that the levels of administration and monitoring contribute to more than just enhancing security. They immediately connect actual activities to legal enforceability by producing the measurable proof required under trade secret law.

There are restrictions on this paper. The suggested paradigm has not been empirically verified in actual IIoT deployments; it is merely conceptual. Given that trade secret legislation is still evolving and differs significantly between jurisdictions, the legal analysis is obviously broad. In the future, research into the development of trade secret protection in IIoT environments by integrating newer technologies like federated learning may be necessary, as well as empirical evaluation of the suggested system and the creation of jurisdiction-specific implementation guidelines that serve as a foundation for future implementation guidelines.

IIoT trade secret protection is more than just a technological or legal concern. At the nexus of both, there is a governance dilemma. To properly address it, governments, trade associations, and corporations themselves must work together to create frameworks that accurately capture the realities of how industrial data truly flows in a connected world.

DECLARATIONS

Conflicts of Interest The authors declare that they have no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors. Ethical approval was not required for this conceptual framework study.

REFERENCES

Dao, T., Nguyen, M., Do, S., & Tran, H. (2026). Cybersecurity threats and defense mechanisms in IoT networks. *arXiv*. https://arxiv.org/abs/2601.00556

Goutam, S., Kippen, H., Grace, M., & Rahmati, A. (2026). Proteus: A practical framework for privacy-preserving device logs. *arXiv*. https://arxiv.org/abs/2603.06540

Imran, M. (2026). Architecting trust: A framework for secure IoT systems through trusted execution and semantic middleware. *arXiv*. https://arxiv.org/abs/2602.10762

José, M. (2026). Privacy-preserving protocols in smart cities and industrial IoT: Challenges, trends, and future directions. *Electronics*, *15*(2), 399. https://doi.org/10.3390/electronics15020399

Kwon, Y., Corren, E., Garrido, G. M., Hoofnagle, C., & Song, D. (2023). SoK: The gap between data rights ideals and reality. *arXiv*. https://arxiv.org/abs/2312.01511

Li, K., Wang, C., Xu, M., Zhang, Y., & Cheng, X. (2025). Dataset ownership in the era of large language models. *arXiv*. https://arxiv.org/abs/2509.05921

Liu, L., Machacy, R., & Kuniyilh, S. (2026). Contrastive learning for privacy enhancements in the industrial internet of things. *arXiv*. https://arxiv.org/abs/2602.00515

Sengupta, J., Ruj, S., & Bit, S. D. (2023). FairShare: Blockchain enabled fair, accountable and secure data sharing for industrial IoT. *IEEE Transactions on Network and Service Management*, 1–1. https://doi.org/10.1109/tnsm.2023.3239832

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law & Security Review*, *34*(3), 450–466. https://doi.org/10.1016/j.clsr.2017.12.004

Zhao, H., et al. (2026). Industrial data-service-knowledge governance: Toward integrated and trusted intelligence for industry 5.0. *arXiv*. https://arxiv.org/abs/2601.04569