INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 5 [2025] | Page 627 – 647

PATENTING OF INTERNET OF THINGS

- Janani G[1]

ABSTRACT

The acceleration in the growth of Internet of Things (IoT) has raised an important question whether it can be patented under patent law or not. Internet of things links physical devices ranging from household items to industrial machines through embedded sensors and software, enabling seamless data exchange and automation with minimal human intervention. With IoT'S impact spanning industries such as healthcare, manufacturing and urban infrastructure, patents play a vital role in shaping competitions and enduring safe, secure device environment. As the reach of IoT expands, securing intellectual property helps innovators protect novel connectivity methods, data analytics and hardware designs. This research explores the challenges of deciding what makes IoT inventions patentable, especially when courts and patenting offices face difficulties in distinguishing genuine technical contributions from abstract ideas. It also examines how different interpretations of abstract ideas affect the approval of IoT patenting.

Keywords: Internet of Things, patenting, intellectual property, technical contributions, connectivity, abstract ideas

INTRODUCTION

The Internet of Things, often called IoT, is a new technology that is changing the way the world works around us. Simply to say, IoT in a nutshell is connecting everyday physical objects to the internet so they can operate by our command through internet even if we are not at the place. This means devices like fan, television, air conditioner, refrigerator, cars, watches, and even industrial machines can 'talk' to each other and to us through the internet. These smart devices use sensors and software to gather information about the environment in which they exist, share it with other devices, and sometimes act automatically without the need for human help.

[1] Student, The Tamil Nadu Dr. Ambedkar Law University, Chennai

IoT is made up of three main parts: the devices themselves (like AC or wearable watches), the internet connection that links these devices, and the software that processes the data and lets user control or monitor the devices. For example, a smart air conditioner can learn your cooling preferences, adjust the temperature automatically when no one is home to save energy, and send alerts to your phone if there's a maintenance issue or a problem with the system. All of this happens because the air conditioner is connected to the internet and can communicate with other devices or apps.

Nowadays IoT is everywhere. In homes, smart devices make life easier and more comfortable. Lights that turn on with your voice or when it feels your presence, refrigerators that remind you when milk is running low, or security cameras you can watch on your phone. In cities, IoT helps manage traffic lights to reduce jams and reduce the accidents caused due to these jamming of lights. Factories use IoT to keep machines running smoothly, remind when the fuel is running low and prevent breakdowns before they happen. In healthcare, IoT devices can track a patient's vital signs and send alerts to doctors in real time, improving care and saving lives on time.

Without technological advancement the growth of IoT wouldn't have been possible. With the increase in the price of power of computers and data storage, the price of sensors and internet connectivity has dropped. This means more devices can be connected, data can be processed faster, and new, smart applications can be created without any barriers. The expansion of high-speed internet, like 5G, also makes it easier for IoT devices to stay connected and work together efficiently.

Like a coin which has two sides, IoT also brings challenges. Security and privacy are the major issues because these connected devices collect lots of personal and sensitive data. It is important to protect this data from hackers to ensure that they are not misused. Another challenge is making sure these devices from different companies can coordinate and work smoothly together. Standards and regulations are still developing to address these issues, aiming to create a safer and more reliable IoT environment.

Therefore, the Internet of Things is about connecting physical things to the internet so they can share data and interact with each other and people. This technology makes life convenient and

efficient and also, they require careful attention to security and cooperation among devices. The gradual growth of IoT, will create the future in new exciting ways that will affect how everyone lives and works. This simple, connected world is just beginning to unfold, offering endless opportunities for innovation and improvement.

RESEARCH QUESTIONS

The following research questions have been formulated to address key challenges, explore important considerations, and guide the analysis of patentability within the Internet of Things domain:

1. What are the key challenges in determining patent eligibility of Internet of Things innovations?
2. How do courts and patent office interpret the concept of "abstract ideas" in the context of Internet of Things patent claims?
3. What strategies can Internet of things patent holders employ to mitigate the risk of patent infringement?
4. How do standard essential patents (SEP's) impact innovation and competition in the Internet of Things industry and what are the implications for patent holders and implementers?

RESEARCH OBJECTIVE

The objective of this research is to provide a wide range of assessment of the patenting of Internet of Things (IoT), a technology that connects devices across sectors and is rapidly shifting day to day life. The study seeks to deliver extensive knowledge in the patent eligibility, legal interpretations, strategic risk mitigation, and industry-wide effects associated with IoT innovation. By exploring these dimensions, the research aims to empower inventors, companies, and policymakers with the knowledge needed to navigate an increasingly complex intellectual property environment.

First, the core objective is to investigate the key challenges in determining patent eligibility for IoT inventions. This research will examine issues of novelty, inventive step, and subject matter,

enquiring how these requirements of patenting interact with the unique features of IoT technologies such as inter-device connectivity, real-time data exchange, and machine autonomy. Since IoT inventions often combine hardware, software, and communication protocols, its difficult to make sure whether they comply with the patent rules. The goal is to identify practical strategies that inventors and companies can use to clearly define their inventions and secure strong patents that withstand legal scrutiny.

Second, the study aims to analyze the interpretations of "abstract ideas" by courts and patent offices in the context of IoT patent claims. In simple terms, abstract ideas are concepts or mental steps that are not related to any physical or concrete invention. The goal is to explore how legal bodies decide on what counts as an abstract idea versus what can be patented as a real invention in the IoT world. Since IoT inventions often involve software, data processing, and connected devices, it can be challenging to determine if they are just abstract ideas or they can qualify for patents. This study aims to look at real examples from court cases and patent office decisions to see how these interpretations are made. Understanding this will help inventors and companies know what kind of IoT inventions are likely to get patent protection and what might face rejection. It will also highlight any challenges or uncertainties in this process, offering clearer insight into the legal landscape surrounding IoT patents. This objective is about making complex legal ideas easier to understand for anyone involved with IoT innovation.

The third objective centers on identifying and recommending strategies for IoT patent holders to mitigate infringement risks. With IoT growing rapidly across various sectors, protecting inventions from being copied or misused by others is becoming increasingly important. The objective is to identify practical ways to help patent owners safeguard their inventions by looking at how they can prepare early through thorough patent searches and legal checks. By reviewing industry trends, licensing patterns, and emerging best practices, the research aims to guide innovators on how to protect their inventions in a situation where many intellectual property rights overlap and ownership is divided among different parties. Strategies such as modular patent filings, participation in standard-setting bodies, active monitoring of competitors, and defensive licensing will be analyzed for their effectiveness. Additionally, it will cover how patent holders can keep an eye on potential infringement globally and adapt their strategies depending on different countries'

patent laws. This objective extends to understanding interoperability challenges, portfolio management, and dispute resolution, vital for both established players and newcomers seeking to leverage IoT technologies without violating the rights of others.

Fourth, this research aims to understand how standard essential patents (SEPs) affect both innovation and competition in the growing Internet of Things (IoT) industry. SEPs are patents that protect important technologies necessary for devices to work together seamlessly according to set industry standards, like Wi-Fi or 5G. Given the importance of global interoperability standards in enabling device connectivity across manufacturers and platforms, SEPs have become central to IoT's progress. The objective here is to dissect how SEP licensing regimes i.e., Fair, Reasonable, and Non-Discriminatory (FRAND) terms affect access to critical technologies, market entry, and the incentives for continued innovation. The study will also evaluate potential legal disputes and policy developments that arise from the interaction between SEP holders, implementers, and regulators, considering implications for fair competition and technological diffusion around the world. It will also consider the experiences of those who hold these patents and those who must use them to build IoT products. Understanding their challenges, such as licensing agreements and potential disputes, is vital to finding a balance that supports progress while protecting rights. Moreover, the objective is to deliver clear insights into how SEPs shape the future of IoT innovation, competition, and business practices in a way that anyone can understand.

Overall, the research objective is to develop a holistic framework for understanding the patenting of IoT, recognize the recurring obstacles and opportunities, and suggest actionable pathways for stakeholders navigating this vibrant and constantly shifting field. By examining eligibility criteria, abstract idea interpretations, infringement mitigation strategies, and SEP dynamics, the research aspires to illuminate best practices, anticipate future trends, and support responsible, forward-thinking innovation in the IoT domain

RESEARCH METHODOLOGY

This is doctrinal research which involves studying existing laws, regulations, legal principles, and court decisions to understand the legal framework around a topic. For patenting in the Internet of

Things (IoT), this means carefully looking at current patent laws, guidelines, and cases that discuss how patents apply to IoT inventions. The research would begin by collecting and reviewing relevant statutes and patent office rules that affect IoT technologies. It will analyze how the law defines patent eligibility and what kinds of IoT inventions qualify for protection. Since IoT combines hardware, software, and network systems, the study will investigate how these different aspects fit within patent law.

Since IoT involves smart devices connected to the internet, such as smart home gadgets, wearable health devices, and industrial sensors, the research focuses on how patent law treats things like hardware parts, software, and methods for communication within these networks. This research aims to clarify tricky legal points such as what kinds of IoT inventions can be patented, what rules inventors must follow, and how courts handle disputes.

Next, the research examines court decisions interpreting these laws, especially focusing on how judges handle issues like abstract ideas in IoT patents. This helps reveal legal trends and clarifies what courts consider patentable in the IoT context. The study will also include scholarly articles and expert opinions to provide broader insights into challenges and best practices for IoT patenting.

The research looks at legal decisions to understand how courts interpret patents concerning IoT inventions, especially whether software or algorithms embedded in devices meet the patent criteria. By using doctrinal research, the study also reviews how patent offices examine IoT patent applications and the challenges faced during the application process. The approach includes analyzing the wording of patent claims to ensure they cover the invention properly without being too broad or too narrow.

REVIEW OF LITERATURE

The review of literature on patenting of Internet of Things (IoT) reveals a rapidly growing field marked by fragmented patent holdings and vigorous filing activity across diverse technology areas. This review of literature expands the ideas of predominant authors, famous books and important judgements which give a knowledgeable insight regarding the topic:

1. "Patent Law Challenges for the Internet of Things," highlights a key issue on patenting IoT: "One challenge for inventors of certain types of IoT applications will be overcoming the test for patent eligibility. Since IoT technology heavily relies on software, it will also be susceptible to patent eligibility challenges, especially when software merely implements an abstract idea without a technical contribution."[2]
2. "Study on the Global Internet of Things Industry Based on Patent Analysis," mainly emphasis on the concentrated patent activity among leading global players and stress the strategic importance of patent innovation in IoT's rapid development. They note, "The surge in patent applications, especially in China, reflects the nation's drive to dominate as a front-runner in IoT technology, emphasizing the need for strong intellectual property strategies to safeguard innovation and maintain competitive advantage"[3]
3. "The Internet of Things PatentBook™ aims to simplify patent licensing in the complex IoT ecosystem by providing a curated collection of essential and non-essential patents. As noted, 'Whether you are a developer, engineer, artist, or entrepreneur, having a high-level view of the different components and technologies that make up what we call the Internet will help you understand the possibilities and the current limitations of what you can do with the Internet of Things.' This underscores the importance of comprehensive patent management and clarity in protecting IoT innovations effectively."[4]
4. Standard essential patents and Internet of Things (IJFMR) on patenting of IoT states " Standard Essential Patents (SEP's) are indispensable for ensuring interoperability across IoT devices by implementing industry standards such as Wi-Fi, LTE, and 5G. However, the licensing of SEPs under Fair, Reasonable, and Non-Discriminatory (FRAND) terms faces challenges, including legal uncertainties and onerous burdens on smaller IoT innovators, necessitating balanced regulatory reforms to foster innovation and competition"[5]

[2] W. Keith Robinson, Patent Law Challenges for the Internet of Things, 15 Wake Forest J. Bus. & Intell. Prop. L. 655 (2015).
[3] Zhi Liping & Zhao Sijia, Study on the Global Internet of Things Industry Based on Patent Analysis, 1 East African Scholars J. Eng. Comput. Sci. 9 (2018)
[4] Internet of Things PatentBook™, PatentBooks Inc. (2025).
[5] Monisha M, Standard-Essential Patents and the Internet of Things: Analysing Licensing Challenges, 7 Int'l J. for Multidisciplinary Research 1, 1–10 (Mar.-Apr. 2025)

5. B. M. Gupta's view on patenting of the Internet of Things (IoT) as derived from his scientometric assessment of global IoT publications and patents (2005–2014) can be summarized in his emphasis on the rapid growth and diversity of research in this area. He stated, "The explosive growth in IoT research highlights the critical need for robust intellectual property frameworks to protect innovations that span hardware, software, and connectivity, ensuring sustainable advancement in this transformative domain".[6]
6. The U.S. Supreme Court's 2014 decision in Alice Corp. v. CLS Bank[7] established a two-step test for determining patent eligibility when an invention is potentially directed to an abstract idea. The Court requires that claims must show significantly more than a mere abstract idea to qualify for patent protection.

CONTENT OF THE RESEARCH

PATENT ELIGIBILITY CHALLENGES FOR IOT INVENTIONS

An invention in India must satisfy three essential patentability criteria under the Patents Act, 1970: novelty, inventive step (non-obviousness), and subject-matter eligibility. These legal checks exist to ensure only legitimate innovations gain patent protection.

NOVELTY

According to Sections 2(1)(j) and 2(1)(l) of the Patents Act[8], an invention qualifies as novel if it is not part of prior art, meaning it hasn't been previously disclosed anywhere in the world before the patent application date. Any form of public disclosure, whether by publication or use, removes the novelty. Leading cases, such as Bishwanath Prasad Radhey Shyam v. Hindustan Metal Industries[9], have affirmed this global standard for novelty.

[6] B. M. Gupta, S. M. Dhawan & R. Gupta, Internet of Things: A Scientometric Assessment of Global Output, 2005–2014, 4 J. Scientometric Res. 104 (2015).
[7] Alice Corp. v. CLS Bank Int'l, 573 U.S. 208 (2014)
[8] Patents act, 1970
[9] (1979) 2 S.C.C. 511 (India); AIR 1982 SC 1444

INVENTIVE STEP/NON-OBVIOUSNESS

Sections 2(1)(j) and 2(1)(ja)[10] specify that an inventive step involves a technical advancement or economic significance, which makes the invention non-obvious to a person skilled in the relevant field. This requirement ensures that patents are not granted for trivial or routine modifications of existing technology, but only for genuine advancements, a standard reinforced through consistent judicial interpretation.

SUBJECT-MATTER ELIGIBILITY

Sections 3 and 4 of the Patents Act[11] enumerate what cannot be patented, such as mere discoveries, abstract ideas, and business methods. A patentable invention must not fall within these statutory exclusions, ensuring that patent protection is reserved for substantial and practical advances with legal and technical legitimacy.

The Internet of Things (IoT) creates unique challenges for traditional patentability tests, such as novelty, inventive step, and subject-matter eligibility, due to its convergence of software, hardware, and multiple technological domains.

BARRIERS TO NOVELTY AND INVENTIVE STEP COMPLIANCE

IoT inventions often combine known components (sensors, processors, connectivity modules) in new configurations. Determining novelty under Section 2(1)(j)[12], is complicated because much prior art exists globally in fragments, making it difficult to assess whether a combination truly lacks anticipation. Inventive step under Section 2(1)(ja)[13] is challenged in IoT because many IoT inventions use software algorithms and networking protocols. Indian law excludes algorithms per se from patentability (Section 3(k))[14], so inventions must show a technical advance beyond just software execution to qualify as non-obvious and patentable. This means the invention should solve a technical problem or improve device functionality, not just automate processes with code Courts find it difficult to distinguish real technical innovations from mere combinations or

[10] Patents act, 1970
[11] Patents act, 1970
[12] Patents act, 1970
[13] Patents act, 1970
[14] Patents act, 1970

automation. In Blackberry Limited v. Assistant Controller of Patents and Designs[15] , patent claims for wireless systems were denied because they lacked inventive hardware and were mostly algorithmic instructions, excluded by law.

SUBJECT-MATTER ELIGIBILITY ISSUES

Section 3(k) of the Patents Act,1970 excludes mathematical methods, business methods, computer programs per se, and algorithms from patent protection. Given that many IoT inventions center on data processing or algorithmic control, applicants must demonstrate a "technical effect" or tangible advancement to overcome statutory exclusions. The Delhi High Court's contrasting rulings in the Blackberry Limited cases[16] illustrate ongoing inconsistencies: one IoT-related application was rejected for being merely software, while another was accepted after proving enhancement in device functionality.

LEGAL AND PRACTICAL IMPLICATIONS

IoT patent claims often span multiple devices and involve ecosystem-level coordination. This presents complications in infringement actions, as claims crossing several entities or device types make enforcement and drafting challenging. Legal provisions such as Section 9 and 10[17] require precise definitions in specifications, while industry-wide interoperability standards bring issues of cross-licensing and increased legal exposure, especially for small entities.

The IoT's cross-disciplinary nature and reliance on software disrupt traditional tests for patent protection under India's Patents Act, demanding adaptive legal frameworks and clearer judicial standards to ensure both protection and innovation.

MIXED NATURE OF IOT INVENTIONS

IoT inventions typically combine hardware components (like sensors and processors), software algorithms, and communication protocols. This mix complicates how inventions are classified and

[15] C.A. (COMM.IPD-PAT) 229/2022 (Delhi High Ct. Aug. 30, 2024).

[16] C.A. (COMM.IPD-PAT) 229/2022 (Delhi High Ct. Aug. 30, 2024).

[17] Patents act, 1970

characterized, making it difficult to clearly define the invention's technical boundaries. This diversity affects not only patentability but also enforcement because different technological elements may be subject to different legal interpretations.

DISTRIBUTED SYSTEMS AND DIVIDED INFRINGEMENT

IoT systems are often distributed over multiple devices and actors, raising potential issues of divided infringement—where different parties perform separate elements of the patent claim. This complicates enforcement because proving infringement requires attributing the actions of multiple parties to a single infringing entity or coordinating joint infringement claims.

COMPLEXITY OF PRIOR ART

The prior art landscape in IoT is extraordinarily intricate. Relevant prior art can come from various fields, including established technical standards, software repositories, and existing product implementations. This cross-domain prior art complicates novelty and inventive step assessments because piecing together these fragments to anticipate an invention is challenging

ABSTRACT IDEA INTERPRETATIONS IN IOT CONTEXT

The abstract-idea problem in software-related patents refers to the difficulty in patenting inventions that are considered too general or conceptual without a concrete technical application. This issue is significant because patent laws aim to protect true innovations, not just ideas or mental processes that anyone could perform without special technology. In software patents, many claims involve algorithms, mathematical formulas, or business methods, which courts often classify as abstract ideas. For example, simply automating a manual task or organizing data digitally might be seen as abstract and thus not eligible for patent protection. To qualify for a patent, software inventions must demonstrate a specific technical improvement or solve a concrete problem through inventive steps. This issue is highly relevant to the Internet of Things (IoT) because many IoT innovations incorporate software algorithms and data processing methods. IoT systems often rely on software to control hardware devices, network communications, and data analysis. However, if the software portion of an IoT invention is viewed merely as an abstract idea, it could

be excluded from patentability under laws like Section 3(k) of the Indian Patents Act or similar provisions worldwide.

For IoT patents, it is crucial to show how the software contributes to a tangible technical effect—for example, improving device performance, reducing energy consumption, or enhancing data security—rather than just performing generic data processing. Courts and patent offices tend to allow patents when the software is tied closely to hardware or produces measurable technical benefits. Legal decisions such as the U.S. Supreme Court's Alice Corp. v. CLS Bank case[18] have established tests to distinguish patent-eligible inventions from abstract ideas. These tests require applicants to prove an "inventive concept" that transforms an abstract idea into a practical and novel invention.

Courts and patent examiners usually analyze IoT claims using a two-part test derived from the Alice Corp. decision: (a) determining if the claim is directed to an abstract idea, and (b) assessing whether the claim adds "significantly more" or a technical solution beyond the abstract idea.

TWO-PART ANALYSIS

First, adjudicators ask whether the claim covers an abstract idea, which typically means a fundamental concept such as a mathematical formula, a business practice, or a mental process rather than a concrete technical solution. If the claim isn't directed to an abstract idea, it may be patent-eligible. But if it is, the examiners proceed to the second part, where they check if the claim contains additional features that transform it into something patent-worthy, often called an "inventive concept." This includes specific technical advancements beyond generic computer use.

INDICATORS FOR TECHNICAL IMPROVEMENTS

Courts look for signs of technical progress, such as:

- Tangible hardware integration, like sensors or processors linked with software
- Claims that are narrowly focused on particular technical implementations

[18] 573 U.S. 208 (2014)

- Concrete system architecture rather than broad, generalized ideas

CLAIM FEATURES THAT REDUCE ABSTRACTNESS

Certain features can help IoT claims show they are not abstract ideas:

- Processing data from sensors that controls physical devices with measurable system improvements
- Introducing new communication protocols solving concrete network issues like packet handling or timing
- Machine-learning models embedded on devices that cut down network latency or bandwidth use compared to cloud-only models

DRAFTING RECOMMENDATIONS

To overcome abstract-idea rejections, patent drafts should:

- Highlight specific technical steps and the tangible system setup supporting them
- Include flowcharts, pseudocode connected to hardware, error handling details, and quantified benefits
- Prepare claims from different angles—device-centered, cloud-centered, or user-interaction-based—to handle diverse examiners' views

INFRINGEMENT RISK MITIGATION STRATEGIES FOR IOT PATENT HOLDERS

IoT infringement risks are shaped by its distributed architecture, broad patent landscapes, and global supply chains. Addressing these risks requires comprehensive patent strategies, careful claim drafting to reduce divided infringement issues, thorough licensing agreements, and coordinated international enforcement efforts to protect IoT innovations effectively

- Divided Infringement: IoT inventions often involve several actors performing different parts of a patented system. For example, one company may make sensors, another operates communication networks, and a third processes data. Legal challenges arise because

proving infringement usually requires one party to perform all claim elements, complicating enforcement.

- Overlapping Patents (Patent Thickets): IoT technologies integrate hardware, software, and communication patents owned by different entities, creating dense "patent thickets." Navigating this web of overlapping rights increases the risk of unintentional infringement and complicates product development.
- Component-Level Licensing: Licensing in IoT often occurs at the component level, with varied patent owners holding rights on different parts of an IoT device. This piecemeal licensing can create costly and complicated negotiations, and potential gaps in coverage.
- Cross-Border Enforcement Complexities: IoT devices are manufactured, deployed, and used globally, resulting in enforcement challenges. Differences in patent laws, jurisdictions, and the decentralized use of IoT technology create legal complexities and higher costs in pursuing infringement claims across borders.

PREVENTIVE AND PROACTIVE PATENT STRATEGIES

- First, comprehensive freedom-to-operate (FTO) searches are crucial. These searches analyze existing patents to ensure a new product or technology does not infringe others' rights. Continuous portfolio monitoring helps track new patent filings, allowing early risk identification and strategic response.
- Second, building a modular claim portfolio is effective. Instead of focusing on just one part, companies patent core components like chips and firmware, interfaces such as APIs and communication protocols, and inventive system-level interactions. This layered approach provides broad but precise protection across the IoT ecosystem.
- Third, defensive filings and strategic continuation practices play a key role. Filing related patent applications and continuation patents expand coverage, reinforce blocking positions against competitors, and allow adapting claims to future technological changes.
- Lastly, participation in standard-setting organizations (SSOs) offers strategic advantages. By contributing to defining essential technologies and standards, companies can influence technology directions and reduce future patent disputes. Being part of SSOs also enables

negotiating fair, standardized licensing terms critical in the interconnected IoT environment.

COMMERCIAL AND CONTRACTUAL STRATEGIES

The Internet of Things (IoT) brings unique commercial and contractual challenges that influence how companies manage patents and intellectual property.

LICENSING APPROACHES

Cross-licensing between companies is a common strategy where parties exchange rights to use each other's patented technologies. This approach can reduce litigation risks and foster collaboration within the IoT ecosystem. Patent pools, where multiple patent holders collectively license their patents as a package, also streamline licensing and help avoid fragmented rights. Platform-level licensing further shifts the licensing burden upstream to component suppliers, meaning manufacturers of chips, firmware, or modules handle licensing conflicts, reducing risks for end-product makers.

OPEN-SOURCE DILIGENCE

Many IoT projects incorporate open-source software components, which can bring risks of license contamination—unintended obligations or limitations due to open-source licenses. To prevent these problems, companies need clear contributor licensing agreements and dedicated processes to review open-source code inclusion carefully. This diligence ensures proprietary IP rights remain protected and prevents harmful downstream licensing obligations.

CONTRACTUAL PROTECTIONS

IoT companies often negotiate contracts with suppliers and Original Equipment Manufacturers (OEMs) that include insurance clauses to cover patent infringement risks, escrow agreements to safeguard source code and technical details, and indemnity provisions requiring suppliers to bear costs or liabilities arising from IP disputes. These clauses help mitigate financial and operational exposure if patent-related conflicts emerge.

PREVENTIVE AND PROACTIVE PATENT STRATEGIES

Effective patent strategies begin with comprehensive Freedom-to-Operate (FTO) searches—detailed investigations into existing patents to ensure new products do not infringe competitors' rights. Continuous portfolio monitoring helps companies track new filings to anticipate and manage emerging threats. Developing a modular patent portfolio is another key strategy. Companies patent critical hardware components like chips and firmware, interfaces such as APIs and communication protocols, and inventive system-level integrations, thus protecting innovation at multiple layers. Defensive filings, including continuation applications, are used to build extensive claim families that block competitors and secure adaptable patent coverage as technology evolves.

Participation in standard-setting organizations enables companies to influence key technical standards, which can reduce future patent disputes and promote easier licensing negotiations in essential technology areas.

ENFORCEMENT AND DISPUTE-RESOLUTION PLAYBOOK FOR IOT PATENTS

Enforcing patents in the Internet of Things (IoT) space requires a strategic, tiered approach due to the complexity and distributed nature of IoT systems.

TIERED ENFORCEMENT STRATEGY

The first step is continuous monitoring of the market and competitors' activities to detect potential infringements early. When a possible infringement is identified, companies often begin with a notice-and-negotiate phase, providing evidence of patent rights to the infringer and seeking a resolution without litigation. If the technology falls under standard-essential patents or other frameworks, FRAND (Fair, Reasonable, and Non-Discriminatory) royalty negotiations may be pursued to establish licensing terms. Litigation is reserved for cases where negotiation fails or when infringement significantly threatens business interests.

USE OF TECHNICAL CLAIM CHARTS AND EVIDENCE

Because IoT inventions often involve multiple devices and actors, proving infringement can be challenging. Patent holders utilize detailed technical claim charts that map every patent claim element to specific system components or processes. These charts provide clear, step-by-step evidence of direct or induced infringement. For example, if multiple parties perform different steps of a patented method across a network, evidence must demonstrate control or direction of the entire process by a single defendant to establish liability.

MULTI-ACTOR SCENARIOS

IoT systems may operate over distributed components sold or operated by different companies, creating a risk of divided infringement defenses. To overcome this, patent owners must strategically document how interactions across devices collectively infringe all claimed elements, and how the alleged infringer exercises control over these interactions.

SEP DYNAMICS, FRAND, AND EFFECTS ON IOT INNOVATION AND COMPETITION

Standard Essential Patents (SEPs) are patents that protect technologies essential to implementing industry-wide standards. These standards are created by Standard Setting Organizations (SSOs) to ensure that products from different manufacturers can work together seamlessly. SEPs play a crucial role in the Internet of Things (IoT) ecosystem because IoT devices heavily rely on standard communication protocols like Wi-Fi, Bluetooth, LTE, and 5G to exchange data and function together efficiently. SEPs matter for IoT primarily because of interoperability. With millions of IoT devices interacting daily, it is vital that they speak a common technical language. SEPs ensure that these devices can connect, communicate, and operate together without compatibility issues, fostering a cohesive device ecosystem.

Another key reason SEPs are important in IoT is the large scale of connected devices. IoT encompasses a vast network of sensors, appliances, vehicles, industrial tools, and more. The broad adoption of standards protected by SEPs helps manufacturers produce devices that fit seamlessly into this extensive ecosystem. And also, IoT's reliance on wireless and communication

standards heightens the significance of SEPs. Many IoT innovations depend on patented technologies that enable efficient, reliable, and secure data transmission. SEPs covering these technologies are indispensable for market participation but must be licensed under Fair, Reasonable, and Non-Discriminatory (FRAND) terms to balance patent holders' rights and industry-wide access.

LICENSING MODELS AND THEIR IMPLICATIONS

Licensing models in the Internet of Things (IoT) significantly impact how companies manage patent rights across the complex supply chains of interconnected devices. Two primary licensing approaches dominate this landscape: upstream/component licensing and downstream/device-level licensing, each with distinct implications.

Upstream/Component Licensing involves patent holders licensing their technologies directly to component manufacturers such as chipmakers or firmware developers. By securing licenses at this level, these companies ensure that components incorporate the necessary rights before reaching device-makers. This model benefits from a smaller number of licensees, simplifying negotiations and reducing duplication of royalties. It also shifts the licensing burden upstream, protecting downstream device manufacturers from complex infringement risks and royalty costs. This approach enhances efficiency and legal certainty in IoT's fragmented supply chains.

On the other hand, Downstream/Device-Level Licensing requires licensing agreements with the manufacturers of the final IoT products. Here, device makers must negotiate licenses for all patented technologies embedded within their devices, which often consist of numerous third-party components. In highly fragmented IoT ecosystems with diverse players and manufacturers, this approach presents challenges. Device makers face uncertainty about which patents to license, risk double royalty payments ("royalty stacking"), and incur high transaction costs—often creating barriers to market entry, particularly for smaller firms.

To address these challenges, aggregation through patent pools serves as a potential solution. Patent pools collect patents from multiple holders and license them as a single package to implementers. This arrangement simplifies negotiations, reduces transaction costs, and offers licensees predictable and transparent royalty rates. Pools can balance the interests of licensors and licensees

by ensuring fair compensation and easing access to essential technologies, especially useful in IoT sectors characterized by multiple overlapping patents.

FRAND LICENSING

In the Internet of Things (IoT) ecosystem, FRAND (Fair, Reasonable, and Non-Discriminatory) licensing plays a vital role but also presents tension points affecting competition and innovation. One primary concern is the risk of hold-up, where patent holders with standard-essential patents (SEPs) demand excessively high royalties after their technology becomes mandatory in industry standards. This creates a barrier for smaller companies wanting to enter the market, stifling innovation and competition. Another issue is royalty stacking, which occurs when multiple SEP owners charge royalties on the same product. Cumulative fees can become prohibitively expensive, increasing costs for manufacturers and end-users and complicating the commercialization of IoT devices.

Licensing terms and royalty calculation methods materially impact IoT business models. A per-component royalty charges fees based on each patented component within a device, potentially leading to stacking issues when many patented parts coexist. Alternatively, per-device royalties simplify payments but might be less precise in capturing patent value. Royalties based on per-feature usage align payments with actual functionalities but require detailed tracking, raising administrative overhead.

These models affect how companies price their products, negotiate licenses, and plan R&D investments. For example, high royalties can discourage startups and smaller innovators from adopting essential technologies. In response, some companies negotiate global portfolio licenses or participate in patent pools to streamline access and reduce licensing complexity.

Balancing reasonable licensing fees with incentives for innovation is essential to ensure broad adoption of IoT standards, healthy competition, and the continued growth of the IoT market. Implementers, patent holders, and regulators play critical roles in refining FRAND frameworks to minimize tensions, reduce entry barriers, and support fair, transparent licensing practices.

POLICY AND LEGAL DEVELOPMENTS

Policy and legal developments around standard-essential patents (SEPs) and related technologies hold practical significance for the Internet of Things (IoT) ecosystem. Given the massive scale and interconnectivity of IoT, transparency in assertions of SEP essentiality is paramount. Clear and accurate disclosures ensure that companies, especially newcomers, understand which patents are genuinely necessary for implementing standards, reducing ambiguity about licensing needs.

Transparency also extends to royalty determination. Policymakers emphasize the importance of clear and predictable rules to calculate fair, reasonable, and non-discriminatory (FRAND) royalties. This clarity boosts confidence among innovators and manufacturers, enabling smoother licensing agreements that reflect the commercial realities of diverse IoT product markets. Well-defined guidelines help prevent excessive royalty demands or patent hold-up, which can stifle competition and innovation.

Dispute-resolution mechanisms are another critical focus area. Efficient, fair processes for resolving licensing and enforcement disputes support healthy standards adoption. Encouraging arbitration, mediation, or other alternative dispute resolution meant to limit costly litigation allows companies of all sizes to participate confidently in the IoT field. Standard-development organizations (SDOs) and policymakers play a vital role in these issues. Essentiality checks and patent registries managed or endorsed by SDOs improve the quality and reliability of patent disclosures. Issuing guidelines on transparency, essentiality assessments, and royalty frameworks also helps harmonize approaches across industries and jurisdictions.

CONCLUSION

Patenting Internet of Things (IoT) technology faces notable barriers due to the complex and interdisciplinary nature of the field, combining hardware, software, and communication protocols. One significant hurdle is navigating the abstract-idea challenge, where inventions involving software algorithms risk rejection unless they demonstrate technical specificity and real-world applications. To overcome this, inventors must draft patent claims that emphasize concrete technological improvements and tangible effects beyond generic software functionality. Prior-art search and cross-domain patent landscape analysis are critical to identify existing technologies and

avoid novelty conflicts, especially considering the fragmented nature of IoT patents. Practical ways to reduce infringement exposure include drafting claims narrowly focused on device-specific functions as well as broader system-level innovations, enabling enforcement even in distributed environments. Licensing models such as standard-essential patents (SEPs) with Fair, Reasonable, and Non-Discriminatory (FRAND) terms fit fragmented IoT markets well, facilitating interoperability while minimizing licensing disputes.

For inventors, companies, and policymakers, several actionable steps can enhance patent strategy and market success. Early cross-domain prior-art searches ensure novelty and reduce later conflicts. Drafting both device-specific and system-level claims captures a broad yet enforceable scope. Joining Standard Development Organizations (SDOs) helps influence and align with industry standards, reducing litigation risks. Where possible, prefer upstream licensing agreements with component suppliers to ease licensing complexity downstream. Preparing FRAND-compliant licensing offers supports fair access and reduces disputes. Maintaining a harmonized global filing strategy protects innovations across jurisdictions and leverages international patent treaties. Policymakers should encourage empirical studies on SEP licensing outcomes in the IoT sector, monitor comparative case law to harmonize patentability standards, and support pooled licensing initiatives that address fragmentation challenges in device-heavy industries.

Future research can focus on the effectiveness of pooled licensing models, analyzing how they simplify access while balancing patent holders' rights. Comparative jurisdictional studies of patent enforcement and abstract-idea interpretations will inform better legal frameworks tailored for IoT's evolving landscape. Overall, sustained efforts combining rigorous technical claim drafting, strategic licensing, and policy enhancements will support robust and fair innovation ecosystems essential for IoT's continued growth.