Peer to Peer Overlay Network in IoT: An Overview

Sofia Munawar
Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan
hmunawar252@gmail.com

***Abstract*– Within the quickly advancing scene of the Internet of Things (IoT), where computing and communications situations need centralized control, Peer-to-Peer (P2P) overlay systems have risen as a promising arrangement. These overlays serve as an establishment for large-scale information sharing, substance dispersion, and application-level multicast functionalities. This paper presents a comprehensive study and comparison of structured and Unstructured P2P overlay systems, categorizing them based on their plan range. The investigation starts with a foundational definition of P2P and a diagram of common operational methods. To pick up bits of knowledge into viable P2P models and conventions, execution measurements are talked about. The paper advance digs into a nitty gritty classification and comparison of current P2P structures, emphasizing question look conventions inside the comparing P2P systems. Furthermore, the consider surveys existing P2P demonstrating yields, laying out common approaches. Novel applications established in P2P strategies are investigated, providing a see into long term of P2P overlay systems. The objective of this paper is to offer a clear and intensive study of P2P systems, following their advancement and advancement, and clearing the way for future investigate headings in this energetic field.**

***Keyword*– Information Sharing, Structured and Unstructured P2P Overlay Systems, Security Issue Challenges in IoT, Investigation, Strategy and Solution Survey**

I. INTRODUCTION

WITHIN the energetic scene of conveyed frameworks, Peer-to-Peer (P2P) and overlay systems have risen as essential standards, revolutionizing the way data is shared and handled. This term paper points to investigate the prospects of P2P and overlay systems, particularly within the setting of the Internet of Things (IoT). As the IoT environment proceeds to extend, the integration of decentralized communication ideal models gets to be progressively significant for versatile, strong, and effective frameworks.

Building on the establishments laid by the comprehensive outlines of P2P and overlay systems, this investigates dives into their potential applications and challenges inside the IoT system. By differentiating the conventional client-server models with the symmetrical parts of P2P systems, we point to reveal how the transformative highlights of P2P and overlay systems can enhance the communication and information administration capabilities of IoT gadgets.

Much just like the natural arrangement of P2P overlay systems on the Web Convention, the IoT scene is characterized by differing gadgets with changing capabilities and network. The investigation of P2P and overlay systems within the setting of IoT includes understanding their versatility to unsteady network, unusual IP addresses, and the independence required to function viably exterior centralized control.

This term paper not as it were builds on the structural complexities and authentic advancement of P2P systems but also looks for to extrapolate their potential inside the IoT domain. By tending to the challenges particular to IoT, such as gadget heterogeneity, information security, and asset optimization, we point to supply bits of knowledge that are priceless for analysts, engineers, and decision-makers exploring the advancing crossing point of P2P, overlay systems, and the Internet of Things.

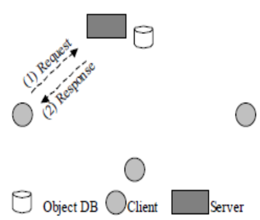

Figure 1 Traditional C/S model

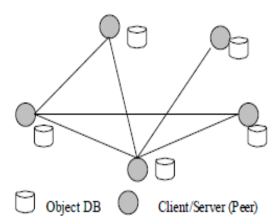

Figure 2 General P2P model

Model	Role of node	Sharing Relationship	Central Control
C/S	Client or Server	C<->S	Yes (Server)
P2P	Servent*	Peer<->Peer	No

Table 1 Comparison of P2P and C/S model
(*Client and Server)

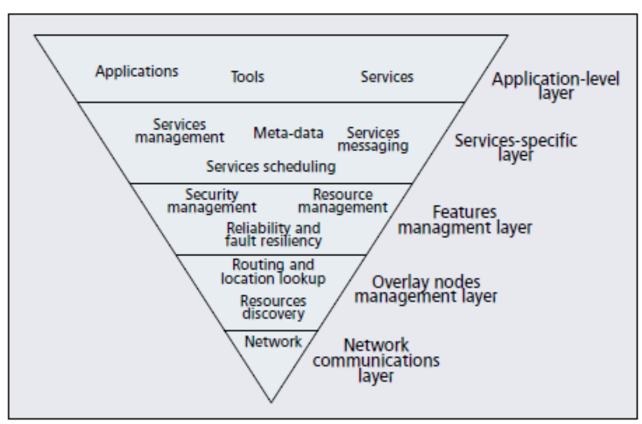

Fig. 3: An abstract P2P overlay network architecture

The Application-level layer within the setting of the Internet of Things (IoT) centers on devices, applications, and administrations executed with particular functionalities built upon the fundamental P2P overlay foundation. P2P overlay systems can be categorized into two classes: Structured and Unstructured.

Structured P2P Overlay Networks: Inside the domain of IoT, structured P2P overlay networks include relegating interesting identifiers (keys) to information things and structured peers into a chart that partners each information key with a peer. This structured chart encourages effective revelation of information things utilizing their individual keys. In any case, in its essential shape, this lesson of frameworks may need back for complex questions. It gets to be vital to store a duplicate or a pointer to each information question at the peer capable for the information object's key.

Within the setting of IoT, the structured P2P overlay systems play a vital part in overseeing and getting to information effectively, adjusting with the conveyed and interconnected nature of IoT gadgets and applications. The structured chart makes a difference in streamlined information recovery based on particular keys, contributing to the by and large viability of IoT frameworks.

Unstructured peer-to-peer (P2P) overlay Network: Play a pivotal part in decentralized communication frameworks, empowering coordinate communication between hubs without depending on a central server. It's suited for applications with energetic and eccentric situations.

Within the setting of the Internet of Things (IoT), unstructured P2P overlay systems contribute to the adaptability and proficiency of communication among IoT gadgets. These overlays permit gadgets to communicate specifically with each other, encouraging real-time information trade without the required for mediators. This decentralized approach adjusts with the disseminated nature of IoT environments, where gadgets are regularly geologically scattered and associated in an energetic way.

IoT gadgets produce endless sums of information, IoT gadgets can collaboratively handle and share data, contributing to progressed decision-making and responsiveness in IoT applications.

In addition, the integration of unstructured P2P overlays with cloud computing upgrades the in general capabilities of IoT frameworks. Cloud assets can be utilized to store and prepare information collected by IoT gadgets, whereas the unstructured P2P overlay encourages coordinate communication between gadgets, lessening inactivity and reliance on centralized cloud framework.

In pith, the collaboration between unstructured P2P overlay systems and IoT empowers a more flexible, versatile, and responsive communication system. This collaboration empowers IoT gadgets to function effectively in energetic situations, leveraging the benefits of both decentralized peer-to-peer communication and cloud computing assets.

Structured and un-structured P2P overlay schemes: Then we endeavor to utilize the taking after scientific classifications to form comparisons between the different talked about structure and un-structured P2P overlay plans:

- ***Decentralization:*** look at whether the overlay framework is conveyed.
- ***Engineering:*** portray the overlay framework design with regard to its operation.
- ***Lookup protocol:*** the lookup inquiry convention received by the overlay framework.
- ***System parameters:*** the specified framework parameters for the overlay framework operation.
- ***Routing performance:*** the lookup steering convention execution in overlay steering.
- ***Routing state:*** the directing state and versatility of the overlay framework.
- ***Peers join and leave:*** portray the behavior of the overlay framework when churn and self-organization happened.
- ***Security:*** see into the security vulnerabilities of overlay frameworks.
- ***Reliability and fault resiliency:*** look at how strong the overlay framework is when subjected to deficiencies.

At last, we conclude with a few considerations on the relative appropriateness of each lesson to a few of the investigate issues that emerge in ad-hoc, location-based, and substance conveyance systems.

Here's a table summarizing the latest suggestions and recommendations for P2P overlay networks in IoT:

Table II: P2P Overlay Network in IoT: Recommendations

Aspect	Suggestion/Recommendation
Resource Discovery	Utilize hybrid approaches combining structured and unstructured overlays for way better versatility and productivity. Use content-aware directing methods to move forward look exactness based on information sort and gadget capabilities.
Security	Actualize strong believe administration instruments to set up secure communication channels between gadgets. Coordinated lightweight encryption conventions reasonable for resource-constrained IoT gadgets. Utilize blockchain innovation for tamper-proof information capacity and get to control.
Scalability	Design protocols that proficiently handle energetic arrange changes with gadgets joining and taking off as often as possible. Create dispersed directing calculations to play down overhead and optimize message sending.
Privacy	Execute differential security methods to anonymize information whereas protecting its measurable properties. Use mist computing to handle information locally on edge gadgets, minimizing delicate information presentation.
Interoperability	Create standardized conventions and APIs to encourage consistent communication between differing IoT gadgets and stages. Investigate the utilize of semantic advances for proficient information trade and translation over distinctive P2P overlays.

P2P Performance Metrics

To assess and compare the execution of proposed P2P networks, a few performance metrics can be characterized, centering on versatility, versatility, and query effectiveness. Furthermore, consolidating viewpoints related to the internet of Things (IoT), cloud computing, and other significant studies can improve the assessment. Here are a few recommended performance metrics:

Scalability

- ***Node Count:*** Degree the capacity of the arrange to handle an expanding number of hubs.

- ***Network Diameter:*** Assess how the normal remove between hubs changes as the arrange scales.
- ***Join/Leave Overhead:*** Assess the affect of hubs joining or clearing out the arrange on in general execution.

Resilience

- ***Query-Hit Ratio:*** Degree the rate of compelling questions, illustrating the flexibility of the organize against provider dissatisfactions or way disillusionments.
- ***Fault Tolerance:*** Assess the network's capacity to recoup from disappointments, considering both supplier and way disappointments.
- ***Redundancy:*** Evaluate the level of excess within the arrange to handle disappointments without critical disturbances.

Query Efficiency:

- ***Query EffiAverage Query Message Number:*** Assess the productivity of the protest inquiry calculation, considering the normal number of messages traded per inquiry.
- ***Average Query Path Length:*** Degree the normal number of jumps or steps taken by an inquiry to reach its goal.
- ***Query Processing Time:*** Evaluate the time taken to handle and total an inquiry, counting both ask and reaction times.

IoT Aspect:

- ✓ ***Device Compatibility:*** Assess how well the P2P arrange underpins an assortment of IoT gadgets with distinctive capabilities and imperatives.
- ✓ ***Energy Efficiency:*** Degree the vitality utilization of hubs partaking within the P2P arrange, significant for IoT gadgets with restricted control assets.
- ✓ ***Data Security:*** Evaluate the security measures in put to ensure IoT-generated information because it navigates the P2P structure.

Cloud Computing and Other Surveys:

Integration with Cloud Services: Assess the consistent integration of P2P systems with cloud computing administrations, guaranteeing proficient information capacity and recovery.

Resource Utilization: Survey how well the P2P arrange utilizes accessible assets, considering variables such as transmission capacity, capacity, and handling control.

Alignment with Industry Standards: Guarantee that the P2P arrange adjusts with set up measures and conventions within the field, encouraging interoperability and integration with other frameworks.

Peer to peer Classification:

Peer-to-peer (P2P) systems can be classified based on their question inquiry component and consistent topology. Here's a rearranged diagram:

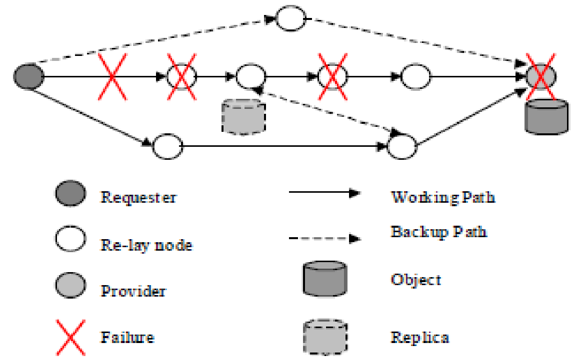

Fig. 4: P2P Object Search

Table III: Comparison table of P2P

P2P Fault	Scalability	Query Efficiency	Tolerance
1G P2P	Good	Bad	Poor
2G P2P	Fair	Good	Random
3G P2P	Fair	Good	Adversarial Attack

Centralized: All question list things are put away in a centralized server. Hubs must illuminate this server approximately the objects they hold, and other hubs inquiry the server for wanted objects. Illustration: Napster. This engineering is basic but inclined to single point of disappointment.

Decentralized, Unstructured: Protest inquiries are disseminated over an irregular, unstructured work of hubs. Inquiries navigate the work hop-by-hop until victory or timeout. Illustration: Gnutella. Whereas versatile to single focuses of failure, productivity may be low.

Decentralized, Structured: Question inquiries are conveyed, and the consistent P2P topology takes after a structure arrange like work, ring, or torus. These structure topologies frequently utilize Conveyed Hash Tables (DHT) for development. Inquiries navigate the structure topology hop-by-hop and are ensured victory after a deterministic number of jumps beneath perfect conditions.

P2P networks can also be categorized into generations:

1st Generation (1G): Early P2P networks like Napster and Gnutella focused on quick deployment but lacked scalability and efficiency.

2nd Generation (2G): Utilizing DHT techniques, 2G networks improved scalability and query efficiency while providing load balancing and deterministic search guarantees. However, they lacked resilience, especially against malicious attacks.

3rd Generation (3G): Recent P2P networks aim for high resilience, assuming nodes may fail. Techniques like object replication, increased node connections, and special structured topologies are employed for resilience. Both 2G and 3G networks are often distributed and structured overlays.

Table IV: Challenges of Peer-to-Peer (P2P) Overlay Networks in IoT

Challenge	Description
Scalability	Overseeing a huge number of gadgets and the energetic nature of the IoT environment can strain P2P systems.
Security	P2P systems are powerless to assaults such as Sybil assaults (where a single hub mimic different personalities) and listening stealthily. Securing communication and guaranteeing believe between gadgets is significant.
Resource Constraints	IoT gadgets regularly have constrained handling control, memory, and battery life. P2P conventions ought to be lightweight and energy efficient.
Heterogeneity	IoT gadgets come in different sorts with distinctive capabilities and communication conventions. P2P systems got to be versatile to this heterogeneity.
Discovery	Productively finding and interfacing to neighboring gadgets in a energetic organize can be challenging.
Fault Tolerance	The arrange should be flexible to gadget disappointments and organize disturbances.
Data Consistency	Keeping up steady information over all gadgets within the organize can be complex, particularly for habitually changing information.
Privacy	Ensuring the security of delicate information collected by IoT gadgets is basic. P2P systems ought to execute instruments for secure information sharing and get to control.

In the context of IoT, P2P overlay networks can leverage existing protocols or utilize modified versions for device communication. Here's a table outlining some potential protocols:

Table V: P2P Overlay Network Protocols for IoT

Layer	Protocol	Description	Benefit for IoT P2P
Application	MQTT	Lightweights publish-subscribe messaging protocol	Effective information trade between gadgets with negligible overhead
Application	CoAP	Constrained Application Protocol, designed for resource-limited devices	Effective information trade with low power utilization
Transport	UDP	User Datagram Protocol, connectionless and faster	Speedier information conveyance for time-sensitive applications
Overlay	Kademlia	Distributed hash table (DHT) for efficient resource discovery	Proficiently located gadgets based on IDs within the dynamic IoT environment
Overlay	Chord	Another DHT protocol for scalable lookups	Offers adaptability for large-scale IoT deploy arrangements
Security	DTLS	Secure variant of TLS for constrained devices	Gives secure communication for delicate information trade/transfer
Security	SRP	Secure Remote Password protocol	Allows devices to securely verify each other's identity without needing a central server.

Here are a few additional points to consider:

- ***Hybrid approaches:*** Combining P2P with existing cloud-based arrangements can use the qualities of both designs.
- ***Scalability:*** P2P protocols got to be planned for productive directing and asset revelation in dynamic IoT situations with possibly huge numbers of gadgets.
- ***Security:*** Securing communication and gadget verification is significant in P2P systems due to the need of a central specialist.

CAN (Content Addressable Network)

The Substance Addressable Arrange for the Internet of Things (IoT-CAN) speaks to a modern arrangement custom fitted to the complexities of IoT situations. At its center, IoT-CAN builds up a Structure peer-to-peer lookup benefit, optimizing information administration and steering inside IoT systems.

Beginning with identifier task, each IoT gadget gets a one-of-a-kind identifier, ordinarily determined from its equipment ID or created upon enrolment with the IoT-CAN arrange. This identifier experiences hashing, coming about in a position inside a multi-dimensional space associated to the standards of a Controller Zone Arrange (CAN).

Zone assignment may be an urgent perspective of IoT-CAN's usefulness. Upon joining the organize, an IoT gadget chooses an irregular point inside the multi-dimensional space. This choice assigns the gadget as dependable for overseeing information inside its distributed zone, adjusting with the particular locale comparing to the chosen point.

Information administration inside IoT-CAN spins around nearby capacity of related data by each IoT gadget inside its assigned zone. This seem include sensor readings, gadget statuses, or any other important IoT information. Keeping up a directing table guarantees gadgets have information of neighbouring gadgets inside the multi-dimensional space, encouraging effective directing.

Directing components in IoT-CAN prioritize vicinity, sending demands to zones closest to the target gadget or information. Utilizing a covetous sending calculation associated to CAN, messages explore towards the zone closest to the goal identifier, optimizing proficiency.

Versatility and blame resilience are vital contemplations. Comparable to CAN, IoT-CAN suits energetic gadget increments without critical arrange disturbance. When gadgets withdraw or fall flat, neighboring gadgets consistently expect obligation for influenced zones, guaranteeing continuous benefit.

Improvements custom fitted for IoT situations advance support IoT-CAN's adequacy. Procedures such as information replication and different hash working improve information accessibility, unwavering quality, and blame strength. These optimizations moderate inquiry idleness, support unwavering quality, and invigorate blame resilience, rendering IoT-CAN well-suited for mission-critical IoT applications.

IoT-CAN finds assorted applications inside IoT biological systems. From effective sensor information administration in large-scale arrangements to encouraging gadget disclosure and communication, IoT-CAN serves as a decentralized, versatile arrangement. In edge computing scenarios, IoT-CAN streamlines information directing, checking inactivity and Structure clog. Additionally, its blame resilience capabilities guarantee reliable operation in the midst of gadget disappointments or organize disturbances, supporting strong IoT Structure network models.

Chord

Chord may be a decentralized peer-to-peer (P2P) lookup benefit planned for distributed information storage, utilizing steady hashing to allot keys to peers. It utilizes a Chord ring, where each peer is dependable for a section of the identifier circle. Peers connect and leave the organize consistently, with keys reassigned to preserve consistency. The framework equalizations stack, guaranteeing each peer handles a comparable number of keys. Inquiries are settled by navigating the Chord ring through successor pointers until coming to the suitable peer. Chord accomplishes effective lookup with O(logN) directing jumps in an N-peer organize. Variations like Emissary and Multi-Ring exist, advertising encourage optimizations.

Tapestry

An inventive self-organizing directing and object area framework, offers similitudes with Pastry whereas joining decentralized arbitrariness to upgrade stack conveyance and directing proficiency. Not at all like Baked good, Embroidered artwork emphasizes organize territory and information question replication, a qualification advance illustrated in consequent segments.

Drawing from Plaxton et al.'s disseminated look method, Tapestry's design highlights a variation of the Plaxton work, optimized to bolster a organize overlay for finding named information objects. Not at all like Plaxton's single-root peer setup, Embroidered artwork utilizes different roots for each information protest to moderate single focuses of disappointment. Inside the Plaxton work, peers serve as servers, switches, and clients, utilizing neighborhood directing maps for effective message directing.

Key mechanisms of Tapestry include:

- ***Failure Detection:*** Tapestry utilizes TCP timeouts and occasional UDP heartbeats with backpointers to identify connect and server disappointments, guaranteeing vigor amid typical operations.
- ***Root Assignment:*** Numerous roots are doled out to each protest, improving blame resistance and unwavering quality. A little, universally consistent arrangement of "salt" values is concatenated to each question ID some time recently hashing, encouraging the recognizable proof of fitting roots.
- ***Object Location:*** Tapestry utilizes a hashing handle to create a set of roots for looking objects, upgrading productivity and adaptability.
- ***Dynamic Operations:*** Tapestry bolsters energetic operations, giving adaptability past the inactive operations of Plaxton.

Pastry Protocol

Pastry, associated to Tapestry, implements Plaxton-like prefix directing to develop a decentralized overlay network appropriate for IoT situations. Each hub is alloted a *128-bit peer* identifier (NodeID), encouraging productive steering of client demands and intuitive with neighborhood applications. Pastry guarantees adaptability and blame resistance, with directing to the numerically closest peer to a given key accomplished in less than logBN steps.

Routing and Maintenance

Each Pastry peer keeps up a directing table, neighborhood set, and leaf set. The directing table, organized with logBN rows, encourages productive steering by holding passages referencing peers with comparable NodeIDs. The neighborhood set contains peers closest in nearness, utilizing measurements like IP directing geographic separate. The leaf set comprises peers with numerically closest bigger and littler NodeIDs, guaranteeing blame versatility

Scalability and Reliability Comparison with tapestry

Pastry's versatility is movable by means of arrangement parameters, adjusting steering table measure and most extreme jumps required for steering. In spite of concurrent peer disappointments, Pastry ensures possible message conveyance with unwavering quality and blame strength, notwithstanding synchronous disappointment of adjoining peers within the leaf set.

Joining and Initialization: Unused peers joining the arrange initialize their steering tables and educate other peers of their nearness. Contact peers, recognized based on nearness measurements like RTT, help within the initialization prepare, improving execution.

Comparison with tapestry: Whereas sharing likenesses with Tapestry, Pastry contrasts strikingly in its approach to protest replication and steering. Pastry reproduces objects without proprietor control, putting copies on hubs closest to the object's identifier within the namespace. This contrasts Tapestry's approach of setting references to question areas on course bounces. Moreover, Pastry expect coordinate directing to protest copies based on objectIDs, posturing challenges in capacity overhead and questions with respect to security and consistency.

Table VI: Peer-to-Peer (P2P) Overlay Networks in IoT: Recent Research and References

Paper Title	Authors	Year	Focus
A Survey on P2P Overlay Networks for the Internet of Things: Characteristics, Design Issues, and Applications	Minyi Shao	2020	Gives a detailed overview of how P2P networks are made for IoT. It looks at the important features, problems in design, and possible uses.
Scalable and Reliable Data Dissemination in Dynamic IoT Networks using Hybrid P2P Overlays	Shweta Malik	2021	Suggests using a mix of P2P networks for easily spreading information in changing IoT networks.
Social Interest Overlay (SIO) Networks for Large-Scale Data Sharing in Social IoT	Yang Xiao	2018	Introducing the idea of Social Interest Overlays (SIO) for sharing lots of data in social IoT settings.

Leveraging Blockchain for Secure and Efficient P2P Energy Trading in Smart Grids	Muhammad Asif Naeem	2020	Studying how to use P2P networks with blockchain to safely and effectively trade energy in smart grids.
Privacy-Preserving Trust Management for P2P Data Sharing in the IoT	Zhiguo Ding	2019	Deals with privacy issues in sharing data for IoT by suggesting a way to manage trust while protecting privacy.
A Blockchain-Based Trust Management Scheme for Secure and Efficient P2P Data Sharing in IoT	Liu	2024 (In Press)	Managing security and trust in peer-to-peer Internet of Things using blockchain technology.
Lightweight Resource Discovery for Dynamic P2P IoT Networks	Sun	2023	Finding things quickly in a changing P2P IoT world
Socially-Aware Routing for Content Dissemination in P2P IoT Overlays	Chen	2023	Sharing information through social media in a peer-to-peer network for the Internet of Things.
Fog-Assisted Secure P2P Communication for Delay-Sensitive IoT Applications	Zhang	2023	Protected P2P talk with fog computing for IoT applications that need fast processing.
Scalable and Self-Organizing P2P Overlay for Collaborative Edge Computing in IoT	Wang	2022	P2P overlay for teamwork in IoT that can grow and organize on its own.

II. CONCLUSION

In conclusion, this paper has given a comprehensive examination and juxtaposition of structured and unstructured Peer-to-Peer (P2P) overlay systems inside the burgeoning scene of the Internet of Things (IoT). Through a systematic categorization based on their structural scope, this consider explains the significant part of P2P overlays as a foundation for large-scale information sharing, substance dispersal, and application-level multicast functionalities in IoT situations.

Starting with a foundational definition of P2P and an diagram of common operational ideal models, the paper dug into execution measurements to gather experiences into viable P2P models and conventions. By conducting a detailed classification and comparison of modern P2P systems, with a specific accentuation on inquiry lookup components, this think about pointed to supply a nuanced understanding of their functionalities and restrictions. Besides, the examination overviewed existing P2P modeling results, depicting predominant approaches, whereas moreover investigating novel applications established in P2P strategies, in this way advertising a see into the long-term direction of P2P overlay frameworks.

Future Directions

Looking ahead, the dynamic field of P2P overlay systems in IoT presents bunch openings for assist investigation and development. Future inquire about endeavors might center on refining existing P2P conventions to upgrade adaptability, robustness, and productivity, especially within the setting of resource-constrained IoT gadgets. Furthermore, there's scope for creating novel decentralized calculations and designs to address rising challenges such as security, protection, and interoperability in heterogeneous IoT biological systems.

In addition, as IoT proceeds to advance and proliferate across differing domains, counting smart cities, healthcare, and mechanical automation, there's a squeezing require for intrigue collaborations to tackle the complete potential of P2P overlay systems. Intelligent between P2P frameworks and rising advances such as edge computing, blockchain, and counterfeit insights display captivating roads for investigation, promising to reshape the scene of IoT organizations.

In rundown, this consider lays the foundation for future research headings in P2P overlay systems within IoT, underscoring the significance of proceeded advancement and collaboration to realize the total potential of decentralized structures in forming long term of associated situations.

REFERENCES

[1]. C. Plaxton, R. Rajaraman, and A. Richa, "Accessing Nearby Copies of Replicated Objects in a Distributed Environment," Proc. 9th Annual ACM Symp. Parallel Algorithms and Architectures, 1997.

[2]. L. Breslau et al., "Web Caching and zipf-like Distribution: Evidence and Implications," Proc. IEEE INFOCOM, 1999.

[3]. D. R. Karger et al., "Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web," Proc. ACM Symp. Theory of Comp., May 1997, pp. 654–63.

[4]. F. Dabek, R. Cox, F. Kaashoek, and R. Morris. Vivaldi: A decentralized network coordinate system. In *SIGCOMM '04*.

[5]. B. Das and V. Bharghavan. Routing in ad-hoc networks using minimum connected dominating sets. In *ICC (1)*, pages 376–380, 1997.

[6]. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. Next century challenges: scalable coordination in sensor networks. In *MobiCom'99*.

[7]. R. A. Ferreira, S. Jagannathan, and A. Grama. Enhancing locality in structured peer-to-peer networks. In *ICPADS*, 2004.

[8]. P. Francis, S. Jamin, V. Paxson, L. Zhang, D. Gryniewicz, and Y. Jin. An architecture for a global Internet host distance estimation service. In *INFOCOM'99*.

[9]. Gnutella Protocol Development. http://www.the-gdf.org, 2005.