Received: 03 January 2022, Revised: 07 February 2022, Accepted: 08 February 2022, Online: 28 February 2022

DOI: https://dx.doi.org/10.55708/js0101003

A State-of-the-Art Survey of Peer-to-Peer Networks: Research Directions, Applications and Challenges

Frederick Ojiemhende Ehiagwina[*,1], **Nurudeen Ajibola Iromini**[2], **Ikeola Suhurat Olatinwo**[3], **Kabirat Raheem**[1], **Khadijat Mustapha**[1]

[1]Department of Electrical/Electronic Engineering, The Federal Polytechnic Offa, Offa, Nigeria
[2]Department of Computer Engineering, The Federal Polytechnic Offa, Offa, Nigeria
[3]Department of Computer Science, The Federal Polytechnic Offa, Offa, Nigeria

*Corresponding author: Frederick O. Ehiagwina, Department of Electrical/Electronic Engineering, +2348051645819 & frederick.ehiagiwna@fedpoffaonline.edu.ng

ABSTRACT: Centralized file-sharing networks have low reliability, scalability issues, and possess a single point of failure, thus making peer-to-peer (P2P) networks an attractive alternative since they are mostly anonymous, autonomous, cooperative, and decentralized. Although, there are review articles on P2P overlay networks and technologies, however, other aspects such as hybrid P2P networks, modelling of P2P, trust and reputation management issues, coexistence with other existing networks, and so on have not been comprehensively reviewed. In addition, existing reviews were limited to articles published in or before 2012. This paper performs a state-of-the-art literature survey on the emerging research areas of P2P networks, applications and ensuing challenges along with proposed solutions by scholars. The literature search for this survey was limited to the top-rated publisher of scholarly articles. This research shows that issues with security, privacy, the confidentiality of information and trust management will need greater attention, especially in sensitive applications like health services and vehicle to vehicle communication ad hoc networks. In addition, more work is needed in developing solutions to effectively investigate and curb deviant behaviours among some P2P networks.

KEYWORDS: Bitcoin, file-sharing, hybrid P2P, overlay network, peer-to-peer network, privacy, security

1. Introduction

There have been increasing attention given to peer-to-peer (P2P) file-sharing network, due to the fact that centralized file-sharing system suffers from poor reliability and scalability, and single point of failure [1]. Most are scalable, anonymous and decentralized [2], and according to [3], P2P networks are flexible, autonomous, and cooperative. However, peer-to-peer networks have unpredictable network topology and complex management owing to their decentralized structure.

So efforts are on to overcome emerging issues such as searching of participating peers and high rate of site failures, which may be due to loss of power or wireless network link. Other issues with P2P system have to do with balancing the load in the peer-to-peer based systems [4], [5]; management of the trust, provision of incentive mechanisms to encourage peers participation, forensic investigation, and so on.

In [6], [7], a survey of P2P overlay networks was done. In [8] indexing in P2P networks was examined. In [9], the author did a "state-of-the-art survey on P2P overlay networks in pervasive computing environments", where Literature publish on P2P overlay network up to 2012 were reviewed. In addition, ref. [10] discussed peer-to-peer technology in 2008. This paper performs a state-of-the-art literature survey on the emerging research areas of P2P networks, applications and ensuing challenges along with proposed solutions by scholars. To the best of our knowledge, there have not comprehensive survey of the P2P network and related research areas. In addition, to reviewing articles before 2012, more attention will be given to literature published between 2012 and 2017.

The rest of this article is arranged as follows: Section II presents research in the different areas of interest in P2P networks such as hybrid P2P systems, security issues, multimedia file sharing, P2P modelling and coexistence with other networks, and so on. Relevant P2P applications are also highlighted. In section III research on forensic investigation and management of P2P network are presented. Section IV highlights emerging challenges and future trends of peer-to-peer networks, and finally, the conclusions reached are presented in section V.

2. Peer-to-Peer Research Areas

The author in [11] highlighted P2P network research areas, which have been put in a tabular form as shown in Table 1.

Table 1: P2P research areas, an extension of [11]

P2P Research areas	Hybrid P2P system [12]–[15]
	P2P overlay network [16]–[20]
	Knowledge-based application and management [14], [19-22]
	Security issues in P2P [19-33]
	Multicasting and multimedia file sharing [34]–[45]
	P2P architecture and protocols [13], [26], [36], [41], [46]–[49], [50-53]
	Data and index structure [54-55]
	Semantic routing and search [56–62]
	P2P based wireless and mobile networks [21], [37], [41], [63–64]
	Coexistence and converge of P2P and other networks [44], [65-68]
	Modelling of P2P systems [22], [38], [69-77]
	System analysis, design and development [78-82]

The following discussion presents a survey of relevant literature on P2P research.

2.1. P2P Overlay Network

By conception, an overlay network is networking riding on another network, and in this case, nodes are connected by virtual links. The P2P overlay network is built on top of the previously existing internet. Peer-to-peer overlay networks are grouped into structured network (Chord [15], [83]–[85], Tapestry, Pastry, Viceroy, and Kademlia [26-27], [86]); and unstructured network (Freenet [28-31], Gnutella [50-51], KazaA [31], BitTorrent [78-79],[87-88], and eDonkey [89]). Research discussing the structure and applications of the P2P overlay network is reported in [16]–[20]. FastTrack and eDonkey request for username and password for network access. Hence, they are not anonymous [2].

Meanwhile, in [42], the authors developed an overlay network that functions by connecting smaller structures in an unstructured manner and, peers can be connected to several rings. But, the proposed overlay network is less expensive in comparison with hierarchical structured P2P systems. Furthermore, unstructured peer-to-peer networks are not efficient and scalable, although, they are very resilient. Nodes interconnect randomly in unstructured P2P networks, therefore, the diameter of the network cannot be precisely determined. In contrast, structured peer-to-peer networks are based on DHT. Since its structure is rigid on the overlay network, performance is degraded and potential for attack when nodes are removed [18]. 1n 2019, the author in [90] created a non-DHT-based structured P2P network using residue class (RC). It was a pyramid tree structure based on interests. In this tree, node I represent a group of peers who are interested in a resource of type i. Because there are many paths between most of the nodes in a complete pyramid tree, a P2P architecture was chosen for this project. From the standpoint of creating load-balanced as well as robust communication protocols, such a structural property can be beneficial. Furthermore, the tree diameter limits the search latency for its intergroup data lookup technique, which is independent of the number of distinct resource kinds and the total number of peers in the system. Furthermore, every intra-group data lookup communication just requires a single overlay hop. In a discussion of structured and unstructured P2P networks, [19] pointed out that an exact and exhaustive search can be done on a structured overlay network. They further attempted to address security issues in gossip-based protocols by using a probabilistic approach to determine the best candidate for gossip. Conceptually, gossip-based protocols are designed for unstructured P2P networks, owing to their ability to form dynamic structures with the aid of the view of the node. When it comes to routing of large distributed infrastructure, there are associated security challenges such as trust and reputation management, privacy and anonymity.

Overlay networks depend on Distributed Hashing Table (DHT), however, many hash functions do not consider the interconnections between item sets, thereby making them ineffective for related items. Owing to this realization, the authors in [91] developed a distributed array by adapting a DHT, with a resultant reduction in the number of messages needed to access elements.

Furthermore, to improve the data rate in sharing files, [16] developed a peer-to-peer overlay network over optical fibre, which uses dense wavelength division multiplexing. With this privacy and the high data rate needed for multimedia communication can be ensured. In [17], the authors sought to enhance multicast communication by developing a generic method, which is used to optimize multicast tree depth in structured and unstructured peer-to-peer systems. The proposed system further helps to manage the latency issue of the overlay network. Features of group communication were incorporated into the system, leading to a multicast system that is based on a distributed algorithm.

2.2. Hybrid P2P System

According to [92], "*a hybrid architecture attempts to strike a balance between the accuracy of the centralized architecture and the lower load of the pure architecture. An example of hybrid P2P structure is super-peer P2P systems.*" Figure 1 shows a general architecture of a super-peer P2P network. As indicated by the following literature, there are ongoing efforts to maximize the advantages of P2P and that of other systems, leading to the development of more robust hybrid systems [12]–[14], [70]. The authors in [14] presented the development of a scalable, efficient and fault-tolerant hybrid of P2P network and wikis, an application of web 2.0 for use in content repositories. Also, discussed were the key blocks that enable peer-to-peer data management at the system non-volatile storage layer for repositories. The authors noted that many internet-based repositories do not use user comments to classify and organize their contents. For some that do, they rely on a centralised web server and seek to make a profit from users comments and tagging.

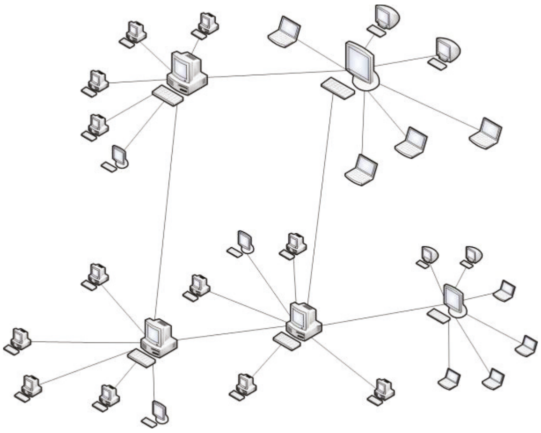

Figure 1: super-peer peer-to-peer network [92]

Video sharing is a critical application of P2P systems. An architecture that integrates the merits of peer-to-peer and Ethernet passive optical network (EPON) architecture was proposed in [93] for addressing the problem of low-cost large-scale video sharing. The proposed architecture included a mechanism that adds downstream bandwidth at the optical live terminal. The researchers in [13] presented a hybrid live peer-to-peer network based on tree and mesh topologies. This was necessitated by the requirement to ensure smooth media playback. The developed hybrid system sought to maximize the merit of either topology, although trading off some data rates. Table 2 shows the merits and demerits of tree and mesh topologies.

Table 2: Comparison of tree and mesh topologies

The Merit of tree topology	**The merit of mesh topology**
Minimized transmission delay	Immunity to node failures
Demerit of tree topology	**Demerit of mesh topology**
Failure of nodes close to the root negatively affects traffic	Prone to unpredictable latencies

2.3. P2P Architecture and Protocols

Examples of literature discussing P2P architecture and protocols are [13], [36], [41], [46]–[49], [52]. In designing efficient P2P protocol and architecture, it is essential to consider churn. Conceptually, churn refers to the dynamics of peers, in terms of how peers join and leaves the network, which may result in network instability. It usually split the network into smaller units, leading to loss of communication or node failure and undesirable consequential data loss.

Monitoring network communication for violations of data security regulations and monitoring data at endpoints to determine whether it was correctly transported from one node to the other might be used to avoid data loss between nodes. For safe inter-node communication, the data might also be encrypted. Incorporating the idea of least privilege is another viable answer. That is, at any abstraction layer of a computer environment, each node must have access to just the information and resources required for its legal function. The authors in [80] modelled churn both as degree-dependent and degree-independent node failures using random graphs. Peer-to-peer protocols were evaluated in [48] while analyzing several factors in connection with churn.

Efficient routing in P2P networks is an issue that has also attracted the attention of researchers such as [47], who noted that existing routing algorithms were based on a random selection of neighbour nodes. Subsequently, a novel routing algorithm based on iterative self-organizing data analysis technique clustering topology for improved routing efficiency. Also, a typical peer-to-peer file-sharing network is not topology-aware. And this constraint leads to its having lower efficiency. With this challenge in view, [41] proposed a P2PMesh that is aware of its topology and allows for efficient data sharing. It involves the use of three strategies depicted in Figure 2.

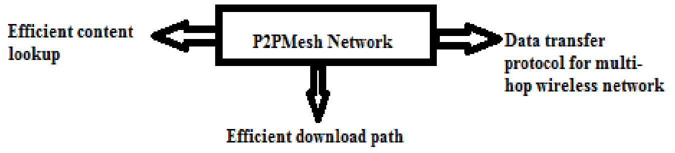

Figure 2: P2PMesh topology-aware strategies proposed by [41]

Distributed denial-of-service attacks (involving exhaustion of connections), server bottlenecks and centralization of the server are examples of problems encountered by internet protocol (IP) voice call technologies. Hence, in [26], the authors presented improved Kademlia protocol to achieve high-level security, rapid addressing and discovery in P2P voice communications. This resulted in a peer locating efficiency increase of up to 20%. Figure 3 depicts a super and normal nodes structure of the proposed I-Kademlia protocol. Also, in a centralized system, servers can break down or operates at a low level of performance, owing to excessive multimedia loading [11].

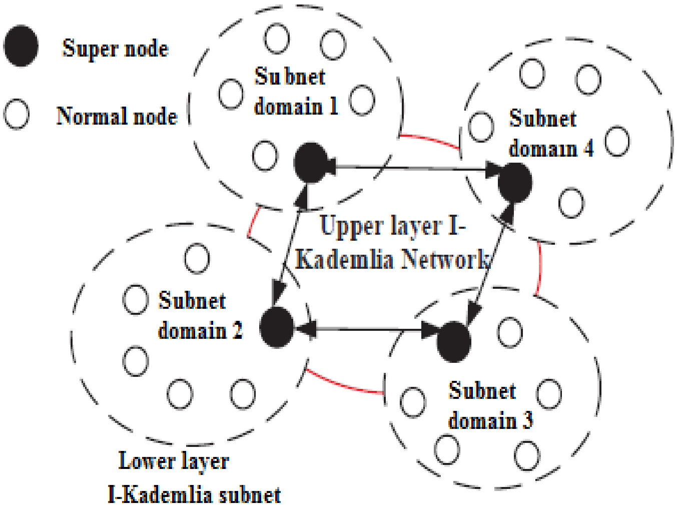

Figure 3: Double layer structure of I-Kademlia protocol consisting of supernodes and normal nodes [26]

In [49], the authors presented a strategy for the detection of P2P botnet traffic. The authors used a more accurate 2-tuple conversation-based methodology that is oblivious of port and protocol, in contrast to 5-tuple based methodology, which is flow-based. The desirable protocol should ensure efficient scheduling of video data dissemination among peers that will reduce the number of hops, delays, and improve the user-perceived quality of video streaming is challenging in P2P video streaming. Owing to this, agent-based scheduling has been proposed such as the belief-desire-intention (BDI) agent architecture in [36], which aid in partner selection, and Net Logo for simulating the modified Gnutella protocol [75].

2.4. Security and Trust Issue in P2P Networks

Since P2P networks are largely anonymous and decentralized, security is a major issue attracting the interest of researchers such as [2], [19]–[25], [52]. The authors in [2] examined the effect of anonymity on P2P users deviant tendencies. Instances of deviant behaviour include peers distributing illegal pornography such as CSA, bestiality, rape and incest, and copyrighted materials. Consequently, queries and query hits were intercepted and analyzed.

Researchers such as [20] noted that effective identity management is key to addressing these issues with P2P overlay networks for large distributed infrastructure routing. One approach for ensuring anonymity, while giving identities via the active operation of two trusted third parties, which internally certify users. Protection against the following can be achieved Sybil attack [27], [32], eclipse attack [20], [92], [94] and whitewasher. Eclipse attack constitutes one of the most disruptive attacks on P2P networks, in which an entity uses "multiple identifiers for the purpose of cutting off traffic to and from a particular node, thereby eclipsing them from the network" [92]. Figure 4 shows a depiction of an eclipse attack on a hybrid P2P system.

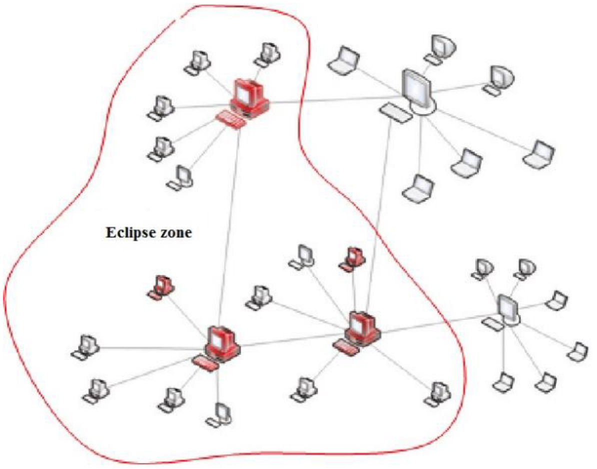

Figure 4: An eclipse attack [92]

More so, in P2P several trust mechanisms can hardly prevent peers with bad behaviour from gaining access to the network and hindering trusted activities in the network. Thus, in [95], the authors presented a meta-reputation system that evaluates peer reputation by examining the behaviour of peers it has invited to join, and not just its behaviour. In so doing, bad peers are not merely marginalized but pushed out. Ref. [96] developed a trust-based admission control model that manages the manner, in which nodes can join the system and help nodes in demanding services more efficiently because nodes with the highest evaluation may not be available for all service requests and do not necessarily provide the best service.

The authors noted in [79] that owing to BitTorrent traffic volume, it is a potential candidate for hidden data carrier, in a report of StegTorrents. The authors further noted that hiding information in network steganography can be for non-malicious intent such as organizations afraid of corporate espionage. Another use will be to conceal communications between journalists and information sources. Meanwhile, a P2P based network capable of detecting local man-in-the-middle attack targets at secure socket layer (SSL) and transport layer security (TLS) was proposed in [25]. The design neither rely on centralized notary service nor owners of websites, rather, the proposed design authenticate certificate via retrieving them at various points on the network. Owing to the need to realize a decentralized and scalable system coupled with the privacy-aware feature, several strategies were integrated into the design called Laribus as shown in Figure 5.

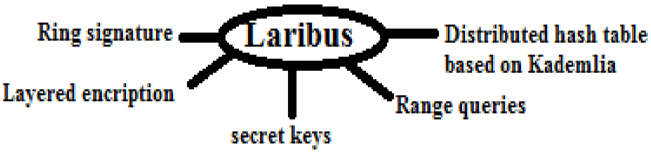

Figure 5: Strategies of Laribus (adapted from [25])

Peer-to-peer traffic is typically not friendly to other sources of traffic in a network, emphasizing the need to identify them. Effects of P2P traffic on network anomaly detector is still a subject of research, in spite of the work in [61], who attempted to minimize the reduction of accuracy to traffic anomaly detectors owing to the presence of P2P traffic by identifying the properties of malicious traffic that do not overlap with peer-to-peer traffic, which is then used to design a traffic preprocessor used by the detector to improve its accuracy.

Furthermore, in order to check for the integrity of files during sharing, many networks depend on several quantities of hash values. Thus, the authors in [88] examined how these hash values can be used to identify unknown data remnants and file fragments. The proposed methods, was, however, not tested on hard drives. Figure 6 shows a typical file content in torrent.

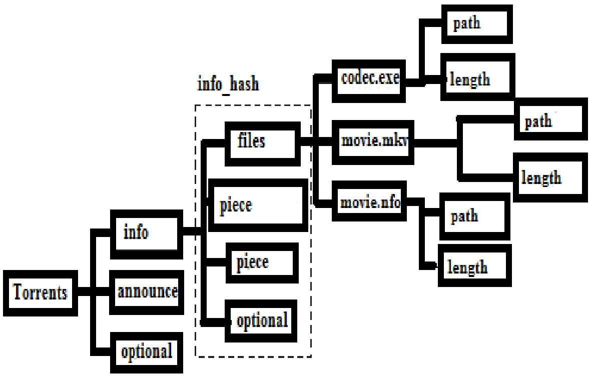

Figure 6: Constituent of torrent file [88]

2.5. Multicasting and Multimedia File Sharing

Multimedia file sharing is a key application of the P2P system. However, the following challenges exist the need to have a pause-free video quality, effective bandwidth utilization, lowering of jump latency, scalable video for heterogeneous platforms, and so on. Some of these challenges depend on the length of the video file. For video with playback time <10 minutes, the challenges encountered are (a) peers can jump to other pages faster or close to the page, and (b) greater overhead is created in establishing an overlay network. Owing to these, the authors in [97] proposed a peer-to-peer based online short video sharing policy that integrates interest-based peers, clustering strategies, short video caching and streaming source peers algorithm, and VoD popularity factor. Other researches on multicasting and multimedia file sharing applications and solutions are presented in [34]–[42], [98-99]. The authors in [100] developed an algorithm for finding frequent itemsets within a P2P network. For QoS constraint services such as live streaming, neighbour peer selection must be done efficiently in terms of reduced playback delay, startup delay, end-to-end delay in the network, distortion and frame loss ratio is decreased. This is in view of the influence of overlay construction and scheduling tactics on the performance of P2P live streaming [101]. Consequently, random peer selection, decentralized mechanism, and specialized protocol where peers regularly exchange information about their status have been proposed. In[101], it was observed that despite the fact that a great number of scheduling techniques have been created, none of them is broad enough to address live streaming concerns. At the receiver end, there is a significant latency and poor visual quality. Therefore, the researchers proposed a new start-up–based selection technique and a slack time–based scheduling strategy. The start-up buffer location for a new peer was defined by the start-up selection procedure, and the scheduling scheme picks both the chunk and the peers. Both push and pull priority-based techniques were used in the scheduling strategy with a significant improvement in network performance and video quality at the receiver end as the result.

However, the researchers in [102], observing that peers are not equally endowed with resources such as battery life, network connectivity, available bandwidth, and online permanence time, introduced a fitness parameter f_i, defined in equation (1) and the parameters are defined in Table 3. The aforementioned resources are critical when the files to be shared are multimedia.

$$f_i = f\left(g_i, h_i\right) = \frac{g_i\left(\boldsymbol{r_s}\right)}{k_0 + h_i\left(\boldsymbol{r_m}\right)} \quad k_0 > 0 \quad \boldsymbol{r_s} \in R_s^{m_i} \quad \boldsymbol{r_m} \in R_p^{n_i} \qquad (1)$$

where $g\colon R_s^m \to R \quad m \in N$

$g\colon R_p^n \to R \quad n \in N$

In [40], a system that delivers live multimedia streaming using a P2P network was proposed. Components of the multimedia system are shown in Figure 7.

Table 3: Fitness parameters notations

Notations	Definitions
R_s	Secondary resource set
R_p	Principal resource set
R	Domain of resources
	Principal resource of peer
	Secondary resource of peer
	Constant of proportionality

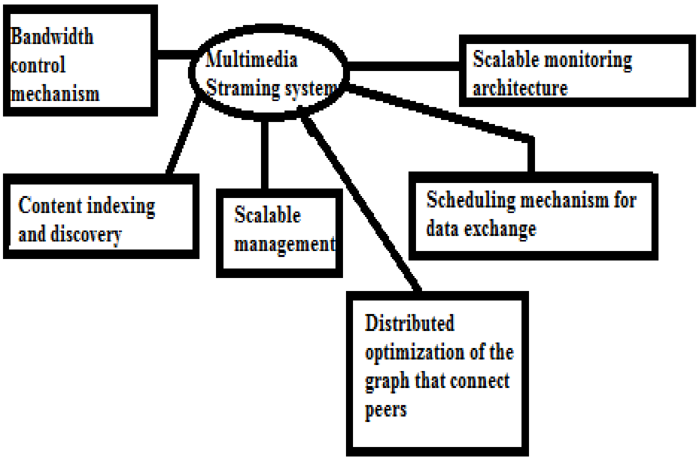
Bandwidth control mechanism
Multimedia Straming system
Scalable monitoring architecture
Content indexing and discovery
Scalable management
Scheduling mechanism for data exchange
Distributed optimization of the graph that connect peers

Figure 7: Components of the live multimedia streaming proposed by [40]

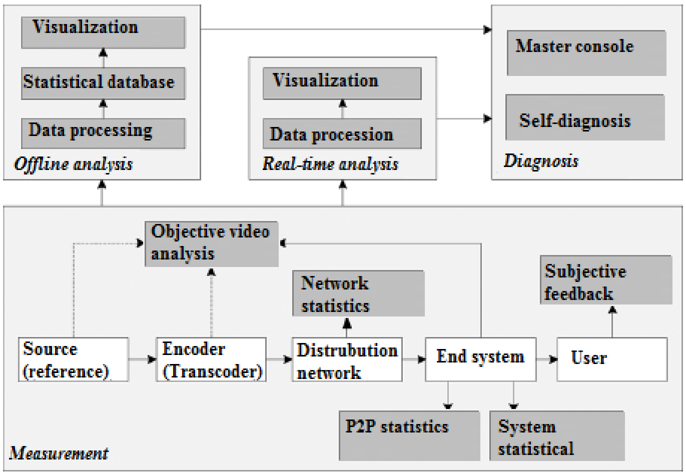

Figure 8: Proposed framework for multimodal quality of user experience for IPTV measurement [35]

In [35], it was observed that while some researchers have attempted to solve existing issues in P2P video file sharing such as transversal of firewall, flash crowds, network address translation, and authentication of contents. There is a need to develop a strategy to systematically assess the quality of P2P video service in terms of end-user perception. This was done by the authors while understudying the Lancaster Living Lab P2P based live video and video-on-demand service provider. Figure 8 shows the proposed multimodal quality of the user experience measurement framework.

The authors in [22] presented a new P2P management system for the high-speed quality of service-aware backbones. The system uses a module, which interfaces network peers and infrastructure used in communication. When a QoS constraint is about to be violated, a rerouting strategy is activated deploying virtual circuits, hitherto redundant. Another issue with P2P video streaming is a constraint in peer resources [102] coupled with a high rate of error under the P2P wireless mesh networks (WMNs) scenario.

In [98], a Fibonacci ring overlay network with distributed chunk storage for peer-to-peer VoD streaming will reduce jump latency attributable to VCR-like operation. Under this scheme, video information is split into bits at peers local storage. To reduce jump latency, some neighbours are maintained in a set of concentric rings with Fibonacci radii, thus quacking peer discovery time. Furthermore, an overlay network, which distributes the stored chunks of video, is constructed to minimize the effect of churns.

Many existing studies gave more attention to uniform chunks during seeking operation in VoD. More so, the impact of a lot of seeking requests has not been adequately studied. The authors in [103] developed a scheme called D-splay used in indexing data chunks in peer-to-peer VoD networks. In [34], SeekStream that easily adapts to user bandwidth changes and behaviour was proposed. This will guarantee stable video streaming even under highly heterogeneous and frequent seeking operation scenarios, although increasing overhead by 4%.

Meanwhile, the telecommunication space is filled with heterogeneous devices such as mobile phones, computers, etc. with various playback capacities. Owing to that scalable video coding (SVC) have been recommended for use in obtaining homogenous, even when sources of the video are heterogeneous. Note that, SVC is used to modify the rate of flow from several sources so that availability upload capacities can be used to deliver homogeneous video quality from all sources. In SVC, video information is encoded into layers. Scalability can be spatial, temporal, and in terms of fidelity or combined scalability. Also, SVC can be used to provide differentiated video standards to peers with heterogeneous capacities [81], [104-108]. However, the quality of the delivered video is degraded by wireless streaming. Hence, the authors in [37] developed an adaptive unequal video protection strategy for small to large scale video streaming over P2P WMNs. Whereas, in [38], the authors proposed a distributed video-sharing algorithm among partner peers, along with a cross-layer design method for ensuring the video quality. Here, some problems associated with video sharing were modelled as a distortion-delay problem solved with a quality-driven scheduling algorithm. Factors considered in the models were (a) network congestions (b) encoding behaviour (c) automatic repeat request query (ARQ) (d) modulation (e) coding and finally (f) packet playback delay.

2.6. Semantic Routing and Search

Semantic routing and search are important aspects of P2P networks because they aid efficient peer discovery [56-60], [109]. The approach varies, depending on the type of overlay network, it could be structured or unstructured. The dynamic query is usually applied to unstructured P2P networks, aimed at reducing the necessary peers needed before reaching desired peers. Consequently, in [110] a dynamic query over DHT for performing a dynamic query over the structured P2P network. The searching algorithm also involves matching keywords with advertised ones. But, what if the keyword is wrongly spelt or incomplete? The authors in [109] developed a double Metaphone algorithm to phonetically match misspelt or incomplete keywords with the template.

The authors in [1] proposed a QoS-aware service discovery method implemented in two stages for unstructured P2P networks, namely; service registration stage-where functional and non-functional information is registered and service discovery stage. The proposed system, meant for elastic cloud computing was probabilistic.

In [58], the authors proposed a decentralized system for Semantic Web Services. In order to reduce overhead and complex computation, the approximate solution was sought via sampling-based method; with that assumption that a sample, which is independent and identically distributed, is present at a location to generate a set of candidate items set.

In P2P search, the efficiency of the process is highly desirable. But improving inter-peers trust could improve node searching efficiency. Owing, to this a trust-aware semantic-based query routing method for improved efficiency of the search was reported in [56]. Bloom filters were used to complete multi-keyword queries while lowering the query cost. Furthermore, in order to reduce workload overheads and enhance discovery in P2P networks, hierarchical architecture has been proposed [46]. However, for efficiency in searching, the ratio of the supernode to the ordinary node has to be optimal, to reduce the latency of lookup.

In [60], the researchers reported on an efficient technique for enhancing the effectiveness of cooperative searching of a large-scale distributed system in unstructured peer-to-peer networks. It was observed that traditional approaches do not guarantee the scalability needed to manage large and increasing semantic web services. Consequently, the authors proposed a method called 'similarity flooding' based on a scalable epidemic algorithm, which results in a high recall rate and lowered time to discover semantic web services (SWSs). Conceptually, flooding involves peers sending queries to other peers via an unstructured P2P network. The search terminates when the time-to-live of the query equals zero. The authors in [111] evaluated classic flooding, random walk and gossip-based resource searching algorithms for mobile P2P networks and methods for enhancing these algorithms with a view of using them in mobile ad-hoc networks (MANETs) was proposed. However, ref. [76] pointed out that flooding incurs large overhead. Owing to this, the researchers proposed a statistical matrix form of flooding, in which distance of transmission between neighbours, amount of shareable files, query service, and so on are incorporated into search algorithms.

In addition, research proposing bio-inspired search algorithms has been reported, such as in [57], [112]. The authors in [57] proposed maximizing search efficiency of peers' databases using a bio-inspired algorithm, reported to have better query and traffic response than both bee- and ant-inspired algorithms. A bio-inspired caching mechanism based on the Artificial Bee Colony (ABC) owing to its reliability was presented in [112]. Furthermore, the ABC algorithm was enhanced to help reduce single-point failure and over caching problems in the P2P network and also reduce energy consumption.

2.7. Peer-to-Peer Network Modelling

To effectively describe a peer-to-peer network, and to enhance its performance, there is a need to model it. The following discussion presents cases of P2P modelling in terms of the development of incentive mechanisms, optimization, trust and reputation management issues, etc. Table 4 shows a classification of the discussed models. In [72], an efficient social-like P2P method for discovering resources was proposed. The method mimics various human social behaviours, in which network connections are regarded as relationships, while peers are considered as people. Many file-sharing systems are based on unchoking algorithms or tit-for-tat. However, this reciprocal incentive scheme approach is not sufficient for designing heterogeneous P2P network, thus, the authors introduce an incentive scheme based on virtual nodes or clusters of trusted nodes that unify user devices since devices with enough resource can support devices that are poor in resources while maintaining game-theoretic properties of reciprocity [113]. There is also a need to provide incentives to peers so that they can share resources [114]. Many incentive systems and policies have been developed in recent years to balance the load and prevent free-riding in peer-to-peer (P2P) networks. One such approach is global peer ranking. Peers are rated using a metric called the contribution index in this approach. The contribution index is set up in such a way that peers are encouraged to share network resources. This strategy can achieve fairness in terms of upload to download ratio in each peer. The calculation of the contribution index, on the other hand, is not simple. It is computed in the network as a whole, distributively and iteratively, and it necessitates peer-to-peer clock synchronization. A slight clock synchronization problem can result in incorrect results [55]. Therefore, the authors in [55] suggested a simple incentive mechanism based on peer contributions that can balance the number of resources uploaded and downloaded by each peer. Because it does not require iterative calculation, it can be implemented with reduced message overhead and storage space while still maintaining strict clock synchronization.

It is worthy of note that existing P2P networks are bandwidth-intensive [115]; posing a financial burden on ISPs and deteriorating their networks. Proposed solutions such as the use of caching devices are limited in deployment by legal concerns; expansion of ISP infrastructure is not sustainable, and an increase in available bandwidth is consumed by the ever-expanding P2P network. Blocking of P2P traffic has also been suggested, but this violates the principle of net neutrality. Enforcing limits on bandwidth consumed via traffic shaping is also not effective because P2P peers can encrypt themselves.

Although predicting P2P traffic is challenging owing to the following non-linear properties of P2P networks: (a) self-similarity, (b) outburst continuity, and (c) multi-construct, some P2P networks contain harmful files, making it crucial to predict P2P traffic [116]. An architecture to measure, identify and optimize P2P, which can adapt to the unpredictable nature of the P2P network as shown in Figure 9 was proposed in [117]. However, the architecture involves traffic shaping and blocking strategies.

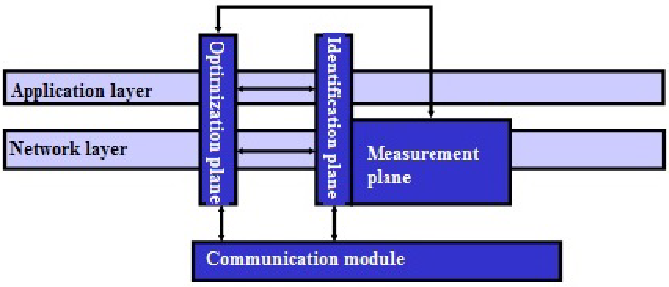

Figure 9: Architecture for P2P network prediction [117]

The authors in [118] highlighted various simple and easy to implement methods of message transmission targeted at increasing network resource utilization for low traffic scenarios. Ref. [116] used wavelet-analysis to handle the non-linear part of net traffic and Kalman filter to handle the linear part.

Both [119] and [120] address the issue of pricing of P2P content. In [120] optimal pricing files in the network was presented. Whereas, the authors in [119] discussed the issue of appropriate network pricing that benefits ISPs and peers in P2P networks without violating the principle of net neutrality, and without requiring deep packet analysis and shaping of the traffic. Knowing that identifying and monitoring traffic is crucial, the authors in [87] studied P2P network traffic using BitTorrent traffic as a case. The authors noted that the majority of P2P traffic monitors are either in favour of internet service providers (ISP) or user-centric. Therefore, a traffic control that satisfies both ISP and P2P users was proposed. One method of improving the efficiency of P2P content sharing is locality awareness, which helps to minimize inter-domain traffic and download times for ISPs and users respectively, resulting in a win-win situation. This is easily true for homogenous systems, but hardly so for real-life peer distribution.

Table 4: P2P model classification

Ref.	Description	Purpose
[23]	PSO	Peer selection strategy
[63]	Byzantine agreement	Minimizing bouts of exchange before faulty nodes can come to an agreement
[69]		Transparency and size scalability
[22], [114]	Evolutionary game	P2P incentive mechanism
[72]	Social network	P2P resource discovery
[87]	Case study of BitTorrent traffic	P2P traffic prediction
[115]		P2P traffic prediction
[116]	Wavelet analysis and Kalman filter	P2P traffic prediction
[119], [120]		P2P pricing by ISPs
[121]	LMD and GARCH	Flash P2P traffic prediction
[122],[123	Graph theory	Characterizing P2P botnets
[124]	Incomplete and dynamic game	P2P incentive mechanism
[125]		Credit incentives for quality video upload
[126]		P2P content availability
[127], [128]		P2P trust management
[43], [129]		Peer pollution in P2P

In [121], the authors studied the use of local mean decomposition (LMD) and generalized autoregressive conditional heteroscedasticity) GARCH in traffic prediction of flash P2P videos. LMD was used to decompose the long-related flow, whereas, the short-related flow is predicted using GARCH.

Determining the size of a peer-to-peer network is another aspect that has been modelled. In [122], it was observed that this along with determining the resilience of P2P botnets could be difficult. The researchers thus presented a graph-theoretic description of the basic vulnerabilities and inherent characteristics of peer-to-peer botnets. Also, several mitigation methods for determining the resilience of current P2P botnets were reported. Meanwhile, botnets are used by persons with malicious intent, in terms of commission of financial fraud, spam and denial-of-service attacks. The authors in [123] discovered major botnet characteristics in local network traffic for User Datagram Protocol (UDP) networks. The authors hope that this will help in botnet detection. To generate a live P2P network environment, a torrent program was used during the capturing procedure. The UDP handled the majority of data transfer in a network, providing marginal transport services, non-guaranteed datagram delivery, and direct access to the IP layer's datagram service for applications. For applications that do not require the TCP standard of service, UDP is employed. The majority of the botnet's attacks were carried out through TCP.

On the other hand, ref. [69] modelled the relationship between data transparency in peer-to-peer networks and size scalability, which will aid in evaluating the extent of scalability of the system considering overheads. In order to evaluate data transparency, the following were considered: bandwidth, CPU utilization, and frequency of data request.

Meanwhile, another issue in the P2P network is the Byzantine agreement problem, which occurs when non-faulty nodes are required to cooperate irrespective of the problem caused by faulty peers. However, several bouts of exchange are needed before non-faulty peers can agree. In [63], an algorithm for reducing the required bouts of exchange was developed.

Furthermore, the authors in [114] and [124-125] observed that peers are not generous enough to share their limited resources, such as bandwidth, in a practical mobile P2P network, but only want to download, owing to their being strategic and rational. This practice is known as "free-riding." Subsequently, there is a need to both design a mechanism to incentivize the peers to share resources and a framework for measuring the incentive mechanism for the MP2P system. In [124], a dynamic and incomplete game was developed. Whereas, a framework based on evolutionary game theory was developed in [114]. In [125], a credit incentive for peers in a network encourages the upload of multimedia files.

Furthermore, the authors in [71] presented an analysis methodology based on an evolutionary game for verifying the efficiency of an incentive mechanism for peers. Here, the client-server relationship was modelled as a game, while, considering its asymmetric properties. Inter-swarm collaboration and sharing of resources have been proposed, which involves sharing of storage and bandwidth among swarms, leading to optimized usage of resources and better content availability, although this requires content preloading. However, content preloading and coordination of inter-swarm results in additional overheads. In [125], the authors reviewed existing strategies on multi-swarm collaborations in P2P content sharing. For content to be shared, it has to be available, hence, the probability (P_k) that content is not available to a peer is given by eqn. (2) [126] and the definition of parameters are shown in Table 5.

$$P_k = \frac{1/r_k}{E\left[B_k\right] + 1/r_k} \tag{2}$$

where $E\left[B_k\right] = \dfrac{e^{r_k u_k} - 1}{r_k}$

Table 5: Parameter definition used for content unavailability

Notations	Definitions
r_k	Content publisher's rate of arrival
u_k	Average resident time of publisher
k	Number of files bundled for sharing

The dynamics of churn and infrastructure failure lower content availability in the P2P network. So, developing a fault-tolerant system such as the decentralized scheduling algorithm for peer-to-peer grid proposed in [82] is desirable. In the proposed system, when the node fails, the algorithm reallocates jobs of grid resources considering the cost of computation and communication required for the job.

A task select node of the grid with the smallest workload is called a computing field *com I* .

$$com\,I = \frac{\sum_{i=1}^{n} T_i}{A \times C_{mips}} \tag{3}$$

where T_i is the amount of computation needed by the *ith* task on queue, the number of processing elements in the node's grid is A and C_{mips} is million instructions per second that a processing element of the P2P grid resource can execute?

Trust is yet another factor that determines a peer's willingness to share a file. Furthermore, the danger of P2P networks spreading viruses and garbage data exists. Researchers are developing various trust models and architectures that will improve the file-sharing capabilities of peers [127-128]. Hence, the Eigen Trust reputation management system, which depends on a collection of pre-trusted peers, which is a major limitation, since some honest peers are ranked low have been proposed [128]. In [128], the authors presented a trust management system, in which honest peers (h) contributes to computing the overall reputation of the other peers. The maximum reputation value was given in the form of eqn. (4).

$$t_h^{(k)} = \max\left(t_1^{(k)}, t_2^{(k)}, \ldots, t_n^{(k)}\right), \text{for h} \in \text{A}_\text{i} \tag{4}$$

A model to integrate forgiveness into the Eigen Trust reputation system, which aids in amending the break-down of trust occasioned by unintentional mistakes, was proposed in [73-74]. According to [73], the following four factors should be considered in the forgiveness based model, such as (a) frequency of offence (b) current offence' severity (c) compensation (d) reciprocity of the offender.

Equations (5) and (6) from [73] show expressions for calculating direct trust and normalizing local trust respectively *i* to *j*. .

$$dt_{ij} = \begin{cases} \left(1-\alpha^{s_{ij}}\right).sat(i,j)/tr_{ij}, \ if \ s_{ij} \geq 0 \\ 0 \qquad , \text{ otherwise} \end{cases} \tag{5}$$

where s_{ij} is the local trust of i to j, α = the system parameters

$$c_{ij} = \frac{\max\left(dt_{ij}, 0\right)}{\sum j \max\left(dt_{ij}, 0\right)} \tag{6}$$

Another trust management issue has to do with peer pollution [43], [129]. That is peers deliberately generating, which results in the degraded network for other peers in the network. The authors in [129] noted that *"video segments might be altered by any peer before being shared"*. It was further mentioned that *"among existing proposals, reputation-based defence mechanisms are the most effective and practical solutions"*. Meanwhile, the authors in [43] proposed a trust management model given as eqn (7) and the notations are defined in Table 6:

$$T_{i,j}(t) = \alpha_{i,j} D_{i,j}(t) + \left(1 - \alpha_{i,j}\right) I_{i,j}(t) \tag{7}$$

Table 6: Pollution resistant trust management model parameter definition

Notation	Definition
$T_{i,j}(t)$	Trust that user i has on another user j at a time t ,with a value between distrust "0" and complete trust "1"
$D_{i,j}(t)$	Direct trust that user i has on user j at time t ,with a value between distrust "0" and complete trust "1"
$I_{i,j}(t)$	Indirect trust that user i has on user j at time t ,with a value between distrust "0" and complete trust "1"
$\alpha_{i,j}$	User i confidence of its direct trust over user j with value between distrust "0" and complete trust "1"
$s_{i,j}(t)$	Set of peers that have direct transactions with both peer i and peer j
$C_{i,k}(t)$	Credibility of peer k
$R_{k,j}(t)$	Peer k's recommendation value of user j based on previous interaction and experience

$$D_{i,j}(t) = e^{-\rho N^{p}_{i,j}(t)} \frac{N^{c}_{i,j}(t)}{N^{c}_{i,j}(t) + \eta} \tag{8}$$

Note that ρ and η are positive constant, $\rho > In\left(1 + \frac{1}{\eta}\right)$

$$I_{i,j}(t) \square \frac{\sum_{k \in S_{i,j}(t)} C_{i,k}(t) R_{k,j}(t)}{\sum_{k \in S_{i,j}(t)} C_{i,k}(t)} \tag{9}$$

In [23], the authors noting that optimal peer selection is difficult owing to variations in dynamic and heterogeneous capacities presented a PSO-based strategy for selecting peers. This resulted in decreased query delay and improved security.

The author in [130] thoroughly examined and expounded on numerous aspects relating to data communication, transaction propagation, and the likelihood of an interference attack that created a delay in transmission of a P2P based network. The authors also showed the impact of block size, consensus, and blockchain scalability, as well as the relationship between factors. The authors in [131] examined the use of blockchains among peers where members do not trust one another. Blockchains allow peers to interact with themselves without the use of a trusted intermediary, and in a verifiable manner.

In [132], noted that electronic voting (e-voting) is a time- and cost-effective method of conducting a voting procedure that has the advantages of allowing for large amounts of data in real-time while still requiring a high level of security. However, worries about network security and communication privacy for e-voting have grown. Securing electronic voting is a pressing issue that has become a hot topic in the field of communications and networking. How to use blockchain in a peer-to-peer network to increase e-voting security was shown. For the essential criteria of the e-voting process, a blockchain-based e-voting scheme on a P2P network is presented by combining the following ideas. A blockchain-based e-voting system for numerous candidates was been created on Linux systems in a P2P network to prove and verify the scheme. The implementation result demonstrated that it is a practical and secure e-voting system that addresses the issue of vote forgery during electronic voting. According to the author, the e-voting mechanism built on the blockchain may be immediately used for a number of networking applications.

In [133], the authors considered the issue of the privacy of transactions in Bitcoin P2P. Currently, the identity of the node that originates a communication is usually kept concealed to safeguard user privacy. However, an attacker watching the entire network can use the spread pattern of a transaction to track it back to its source via what is called rumour centrality, which is created by symmetry in the dissemination of gossip-like protocols. The authors further noted that recent research has attempted to address the problem by exploiting proxied broadcast and violating the symmetry of the Diffusion protocol, which is currently utilized in Bitcoin. However, the complexity of their design may make it difficult for them to be adopted in the actual world. Therefore, the authors suggested a transaction relay protocol with a simple yet effective design that secures the source of transaction messages. The approach does not involve the creation of propagation graphs and decreases the adversary's ability to acquire precision by opening many connections to the same node. Experimental data demonstrated that an eavesdropper adversary's deanonymization accuracy against the proposed scheme was up to ten times lower.

2.8. Coexistence and Convergence of P2P Network and Others

In [65], P2P and cloud computing were studied and, it was noted that both networks are large-scale distributed systems with potential application to *"backup, storage, streaming content distribution, online gaming, etc."* This has however become more cogent because, in recent times, P2P cloud networking is replacing traditional internet services in computing. P2P cloud networking is currently being used to offer resources with scalability to a large number of consumers. The aim and method of providing the service utilizing cloud technology can be used to classify P2P-based cloud systems [134].

In [44], the authors presented information-centric networking for P2P communications as a candidate solution for future internet-based applications. In [64] a P2P cost-effective and performance-enhancing file sharing arrangement that involves a wireless mesh network, in which the network operator makes provision for infrastructures such as mesh router, storage capacity and P2P awareness system was discussed. In addition, the authors determined the optimal number of replicas for each file to obtain minimal costs of files in the network.

Whereas, in [66] a brief overview of P2P networking and application on convergence peer-to-peer context awareness, pointing out that this became necessary because sensors and devices should be designed to offer services based on awareness of the environment and users' intention was presented.

In [68], it was noted that in a ubiquitous environment, an RFID-based sensor system with a P2P network can be quite useful. By merging computing devices with a range of sensors, the authors created a network capable of controlling its processing and network resources. The functioning of the sensor network required context-awareness. Hence, an RFID-based sensing system that uses a peer-to-peer network to receive contextual information about the user was created. The proposed system comprises a reader, 30 sample tags, and a sample middleware application for reading, writing, and testing RFID tags, as well as the fundamental RFID equipment needed to operate and test an RFID system. It could detect users entering and exiting a location, as well as to measure their distance from the device. In addition, it is capable of determining the state of the sensor installation.

Another system that is being converged with P2P is content delivery networks (CDNs), which enhance the user-perceived quality of service owing to their use of servers at the internet edge. CDN providers are tapping into the P2P networks of their users to lower the cost of servers. Examples of peer-assisted CDN include *"BBC iplayer, MSN video, Conviva". Others are "Kankan, Livesky, Akamai NetSession, Spotify, Tudou"* [67], etc. But offering failure recovering in this type of system is challenging, therefore, the authors in [135] developed a CDNpatch, which empowers peers to compute in advance some backup content providers by maintenance algorithm and efficient information exchange at regular intervals as a solution to the aforementioned challenge. Also, the CDNPatch provides an algorithm to minimize the interruption of playbacks.

Meanwhile, in [12], [70], the researchers developed a hybrid system of CDN and P2P, in which the merits of both systems were harnessed to address the routing and resource allocation with emphasis on the economics of content delivery. The CDN/P2P based economic routing was based on an oligopolistic mechanism used in managing the content demand on servers at the internet's edge. Furthermore, the contributions of subscribers are optimized using a truthful profit-maximizing auction. In [67], the authors noted that the future of peer-assisted CDN is challenged owing to copyright issues, low reliability of P2P network, etc. and consequently presented a way of classifying the research efforts in this regard.

The authors in [45] proposed hybrid P2P network architecture for interactive streaming media to solve the disadvantages of interactive streaming media in real-time transmission, control overhead, stability, and scalability in general P2P networks. The system uses a hierarchical structure that combines a CDN, a peer-to-peer network, and a tree-mesh structure. Streaming media data is delivered to the super-nodes tree after a method for super-node selection and super-nodes tree construction is built, reducing the strain on edge servers. Meanwhile, in the case of real-time streaming media transmission, a push-pull approach is used. The edge server provides streaming media data to the asking node, which then pulls the missing streaming media data to the super-nodes tree, improving data transmission in real-time. The system may dramatically reduce end-to-end delay, streaming media distortion, and control overhead when compared to traditional P2P and basic CDN-P2P architectures, according to the simulation.

The general P2P network and cloud computing architecture is different in functionality. But researchers are examining the possibility of fussing cloud computing with peer-to-peer systems [59], [136-137]. A hybrid of these two systems was proposed for multimedia streaming in [136-137]. In [137], a review of cloud-based P2P video streaming articles between 2009 and 2014 was done. However, the authors in [59] discussed papers on applications of P2P networking on the large-scale distributed cooperative environments on cloud and P2P networks. For large and increasingly dynamic web services, centralized servers for registering are not realistic, and efficient. Also, they do not support semantic description.

3. Investigation and Management of Peer-to-Peer Networks

When an offensive file is shared among peers in a network, there may be the need to trace the originator of that file. This is usually not easy owing to the decentralized architecture of the P2P network. However, the attention of researchers has been drawn to forensic investigation of malpractices that could occur. Examples of this include the work reported in [77], where a model to identify the peer who was the first to upload a file in a Chinese community file-sharing network called *Foxy* was proposed. This can aid P2P forensics since the technique used for investigating BitTorrent seeder are inadequate for *Foxy* based on the Gnutella 2 protocol.

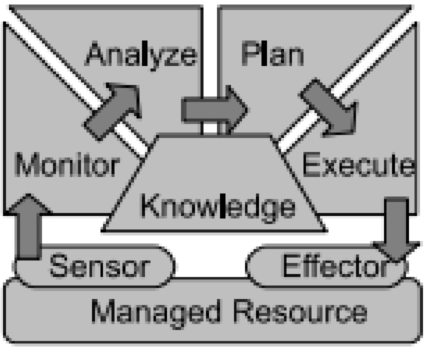

Figure 10: Autonomic Computing

Monitoring and management procedures must be used to control the quality of peer-to-peer systems. In large-scale networks with independent, unstable nodes, both tasks are difficult. A possible solution provides an extensive statistical depiction of the live state of a peer-to-peer network. The Autonomic Computing model is shown in Figure 10. In the event that a quality deviation is recognized, a predefined system state is approached by autonomous system re-configuration using autonomic computing concepts. A good monitoring scheme can prevent possible data loss when data are transferred from one node to another.

The monitoring tool shown in Figure 11 comprises of modified P2P client, a tool for message parsing, a database for archiving information collected, and a database query mechanism. A tool, which is inserted to modify a peer node in the network, shown in Figure 11 was developed in [138]. The node record logs data, timestamps and identification information.

Meanwhile, in [62], the authors developed a system that is capable of identifying P2P nodes operating in a network, through analysis of Net flow data, rather than via analysis of the properties of the content itself. Hence, cooperative communities in the network can be discovered or identified. Detecting cheating in Peer-to-peer based online gaming is challenging due to there being no central server for monitoring. Thus, the authors in [33] proposed a mechanism where players play with their deck, with no intervention from other peers. Features such as player dropout tolerance, usage for a variety of games, collusion prevention among peers were incorporated into the cheating detection mechanism.

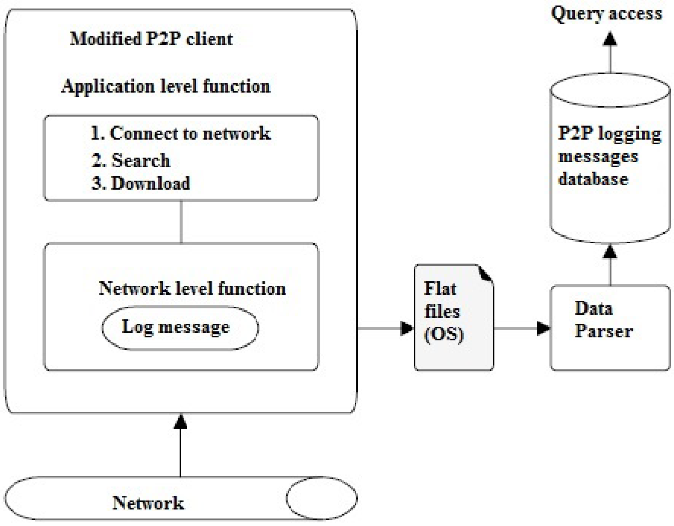

Figure 11: P2P monitor [138]

To optimize data gathering, a "trust-based minimum cost quality-aware" data collection strategy was presented in [139]. In [140], the authors proposed a P2P network-based smart grid model for edge computing, in which P2P networks were used at the edge computing layer. The model's innovation was that edge computing nodes can be utilized to gather, compute, and store data while being P2P connected, allowing them to communicate with one another after data processing. The experimental findings of the algorithm revealed that by utilizing the proposed model, there was a considerable improvement in terms of energy resource management in terms of lowering economic costs, boosting renewable energy usage, and real-time control capabilities.

Many child sexual abuse (CSA) monitoring tools in peer-to-peer networks depends on hash value databases of identified CSA-built over time via analysis of seized devices of offender media. Hence, new or previously unknown media cannot be detected. Another challenge of monitoring CSA related activities on P2P networks has to do with the sheer large amount of files that have to be monitored. To address these limitations, the authors in [39], [42] reported a filename and media scheme based on multiple features such as video and audio word, that flags unseen or previously unknown CSA media to law enforcement agencies. It was reported that previous approaches use of automatic image content analysis yield a fair rate of detection owing to their reliance on single feature description, and still others used marginally discriminative skin detection techniques. The work on CSA monitoring in the P2P network is part of the iCOP (identifying and catching originators in P2P networks) project, and an overview of the developed toolkit is shown in Figure 12.

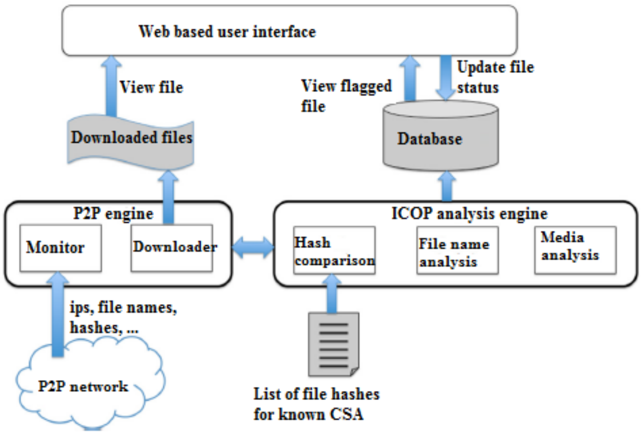

Figure 12: Structure of the iCOP toolkits adapted from [42]

4. Challenges In Peer-to-Peer Applications, Solutions and Future Trend

Whereas P2P networks have made files easily accessible and given a boost to online media streaming of video on demand, some challenges would need to be given greater attention. A pictorial description of identified research direction in P2P research is shown in Figure 13.

For instance, in [24], while highlighting the potential role of P2P network in energy-smart cities, noted the following concomitant security and privacy challenges ensuing:

- Privacy/confidentiality of wireless health services system;
- Privacy and security of ad hoc networks for vehicles, and;
- Development of effective trust models.
- Maintenance of anonymity of transactions in Bitcoin P2P in the face of an adversary, who is watching the entire network can evaluate a transaction's distribution pattern to track it back to its source.

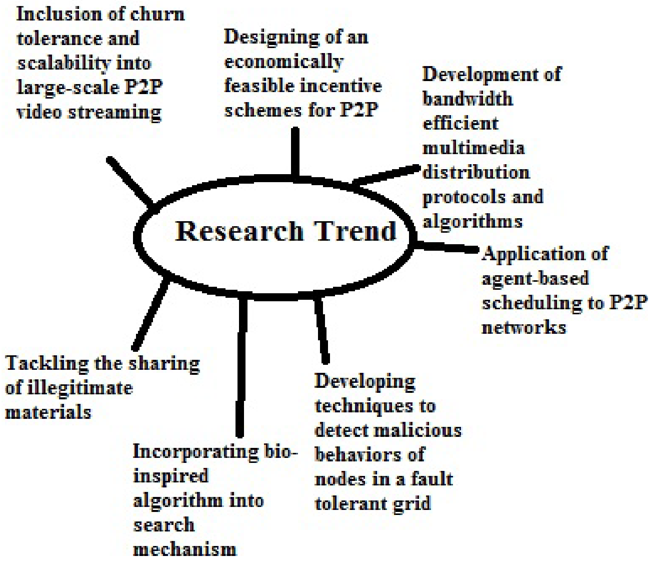
Research Trend
Inclusion of churn tolerance and scalability into large-scale P2P video streaming
Designing of an economically feasible incentive schemes for P2P
Development of bandwidth efficient multimedia distribution protocols and algorithms
Application of agent-based scheduling to P2P networks
Developing techniques to detect malicious behaviors of nodes in a fault tolerant grid
Incorporating bio-inspired algorithm into search mechanism
Tackling the sharing of illegitimate materials

Figure 13: P2P future research trend

Another area of concern is how to prevent attackers from utilising UDP to modify data transported by UDP to attack a P2P network. In addition, the following undesirable problems emanating from peer-to-peer file sharing include [54] (a) violation of copyright laws (b) phishing scams (c) breach of confidentiality in the form of a leak of confidential information, which will need ongoing research to effectively address them.

So far the following countermeasures have been proposed: (a) the use of digital right management (b) digital watermarking of content (c) index poisoning [54]. More applications of these measures to P2P networks are expected in the nearest future.

Conceptually, index poisoning is a methodology that changes the index of illegal files in order to make them unreachable by any unauthorized peer. The shared files that were indexed are distributed over the network in advance. But cost-effectively doing this for an unstructured P2P network was the objective of [54]. In contrast, digital watermarking involves concealing a message related to a digital signal such as image, audio, and video within the signal itself. Although related to steganography, it is different from it in terms of relatedness of the message being concealed to the actual digital signal [141].

Another area of concern is how to prevent attackers from utilizing UDP to modify data transported by UDP to attack a P2P.

Also, in the future bio-inspired algorithms could be augmented semantic techniques so that search queries are routed to the database, which possesses the most semantically matching search keyword [57]. Moreover, in terms of peer trust management, how do combining peer-trust values with file trust values affect the reputation of the management systems? This is a question that needs further research. In addition, metered access and techniques to observe malicious behaviour of grid's node could be incorporated into future fault-tolerant decentralized scheduling algorithms so as to improve nodes availability [82]. Related to this is an examination to see if attackers may use topological measurements in the P2P network to execute more successful purposeful attacks [53].

In sharing P2P files the issue of bandwidth bottleneck is common, hence, a novel algorithm for searching nodes would need to be developed. In addition, few pieces of research exist on the application of agent-based scheduling to a P2P network. Another related issue here is how to further minimise inter-peer search latency.

Further research should see the inclusion of churn tolerance and scalability into large scale P2P video streaming and the associated optimisation of "selection of supernodes and network interaction efficiency."

In addition, the design of economically feasible incentives for peer-assisted CDNs and unstructured P2P, in general, is still a subject of research.

5. Conclusion

Although, there are review articles on P2P overlay networks and technologies, additional topics such as hybrid P2P networks, modelling of P2P, trust and reputation management concerns, coexistence with other existing networks, and so on have yet to be thoroughly examined. Furthermore, existing reviews were restricted to works published in 2012 or earlier.

In this paper, a survey of current literature in the P2P network and associated emerging issues have been done. This included a state-of-the-art review of hybrid P2P, modelling and design of a peer-to-peer system, trust management issues and so on. In addition, challenges such as security and privacy constraints along with suggested solutions have been highlighted.

Finally, areas for future research have been recommended. These included the development of a more robust privacy and security scheme for P2P. We further, pointed out that copyright violations, phishing frauds and confidentiality breaches will necessitate continued research to successfully handle them.

References

[1] W. Lin, W. Dou, Z. Xu, and J. Chen, "A QoS-aware service discovery method for elastic cloud computing in an unstructured peer-to-peer network," *Concurr. Comput. Pract. Exp.*, vol. 25, no. 13, pp. 1843–1860, 2013. https://doi.org/10.1002/cpe.2993

[2] D. Hughes, J. Walkerdine, G. Coulson, and S. Gibson, "Peer-to-Peer : Is Deviant Behavior the Norm on P2P File- Sharing Networks?," *IEEE Distrib. Syst. Online*, vol. 7, no. 2, pp. 1–11, 2006. https://doi.org/10.1109/MDSO.2006.13

[3] F. Wang and Y. Sun, "Self-organizing Peer-to-peer social networks," *Comput. Intell.*, vol. 24, no. 3, pp. 213–233, 2008. https://doi.org/10.1111/j.1467-8640.2008.00328.x

[4] Q. Hofstätter, "Performance Impacts of Node Failures on a Chord-Based Hierarchical Peer-to-Peer Network," in *Networked Services and Applications - Engineering, Control and Management: 16th EUNICE/IFIP WG 6.6 Workshop*, F. A. Aagesen and S. J. Knapskog, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 256–258. https://doi.org/10.1007/978-3-642-13971-0_25

[5] M. Zhang, E. El Ajaltouni, and A. Boukerche, "A scheduling and load balancing scheme for dynamic P2P-based system," *Concurr. Comput. Pract. Exp.*, vol. 22, no. 10, pp. 1325–1334, 2010. https://doi.org/10.1002/cpe.1578

[6] E. K. Lua, J. Crowcroft, and M. Pias, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Commun. Surv. Tutorials*, vol. 7, no. 2, pp. 72–93, 2005. https://doi.org/10.1109/COMST.2005.1610546

[7] K. Dhara, Y. Guo, M. Kolberg, and X. Wu, "Overview of Structured Peer-to-Peer Overlay Algorithms," in *Handbook of Peer-to-Peer Networking*, X. Shen, H. Yu, J. Buford, and M. Akon, Eds. Boston, MA: Springer US, 2010, pp. 223–256. https://doi.org/10.1007/978-0-387-09751-0_9

[8] P. Linga, "Indexing in peer-to-peer system," Cornell University, 2007.

[9] A. Malatras, "State-of-the-art survey on P2P overlay networks in pervasive computing environments," *J. Netw. Comput. Appl.*, vol. 55, pp. 1–23, 2015. https://doi.org/10.1016/j.jnca.2015.04.014

[10] S. Ganguly and S. Bhatnagar, "P2P Technology," in *VoIP*, John Wiley & Sons, Ltd, 2008, pp. 87–102. https://doi.org/10.1002/9780470997925.ch7

[11] J. Han, "Distributed hybrid P2P networking systems," *Peer-to-Peer Netw. Appl.*, vol. 8, pp. 555–556, 2015. https://doi.org/10.1007/s12083-014-0298-7

[12] M. Garmehi and M. Analoui, "Envy-Free Resource Allocation and Request Routing in Hybrid CDN–P2P Networks," *J. Netw. Syst. Manag.*, vol. 24, no. 4, pp. 884–915, 2016. https://doi.org/10.1007/s10922-015-9359-3

[13] C. Hammami, I. Jemili, A. Gazdar, and A. Belghith, "Hybrid Live P2P Streaming Protocol," *Procedia Comput. Sci.*, vol. 32, pp. 158–165, 2014. https://doi.org/10.1016/j.procs.2014.05.410

[14] U. Bartlang and J. P. Müller, "A flexible content repository to enable a peer-to-peer-based wiki," *Concurr. Comput. Pract. Exp.*, vol. 22, no. 7, pp. 831–871, 2010. https://doi.org/10.1002/cpe.1465

[15] Y.-H. Chen, E. J.-L. Lu, Y.-T. Chang, and S.-Y. Huang, "RDF-Chord: A hybrid PDMS for P2P systems," *Comput. Stand. Interfaces*, vol. 43, pp. 53–67, 2016. https://doi.org/10.1016/j.csi.2015.08.008

[16] A. Polar, M. Bunruangses, K. Luangxaysanam, S. Mitatha, and P. P. Yupapin, "Overlay Fiber Network Based MNRs for P2P Networks," *Procedia Eng.*, vol. 32, pp. 482–488, 2012. https://doi.org/10.1016/j.proeng.2012.01.1297

[17] M. Amad, A. Meddahi, D. Aïssani, and G. Vanwormhoudt, "GPM: A generic and scalable P2P model that optimizes tree depth for multicast communications," *Int. J. Commun. Syst.*, vol. 25, no. 4, pp. 491–514, 2012. https://doi.org/10.1002/dac.1275

[18] W. Liu, J. Song, and J. Yu, "An Overlapping Structured P2P for REIK Overlay Network," *Physics Procedia*, vol. 33, pp. 1022–1028, 2012. https://doi.org/10.1016/j.phpro.2012.05.168

[19] A. Srivastava and P. Ahmad, "A Probabilistic Gossip-based Secure Protocol for Unstructured P2P Networks," *Procedia Comput. Sci.*, vol. 78, pp. 595–602, 2016. https://doi.org/10.1016/j.procs.2016.02.122

[20] J. Caubet, O. Esparza, J. L. Muñoz, J. Alins, and J. Mata-Díaz, "RIAPPA: A Robust Identity Assignment Protocol for P2P overlays," *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2743–2760, 2014. https://doi.org/10.1002/sec.956

[21] X. Lu and P. Hui, "A Mobile Peer to Peer Content Dissemination Model to Minimize Load on Cellular Network," *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI).* pp. 272–275, 2015. https://doi.org/10.1109/IIKI.2015.65

[22] E. P. Duarte Jr, P. Elias, Z. G. Lisandro, J. N. S. Luci Pirmez, C. A. Rossana, T. Liane, B. C. Reinaldo, and L. Alexandre, "GigaManP2P: An overlay network for distributed QoS management and resilient routing," *Int. J. Netw. Manag.*, vol. 22, no. 1, pp. 50–64, 2012. https://doi.org/10.1002/nem.785

[23] S. M. Nallakannu and R. Thiagarajan, "PSO-based optimal peer selection approach for highly secure and trusted P2P system," *Secur. Commun. Networks*, vol. 9, no. 13, pp. 2186–2199, 2016. https://doi.org/10.1002/sec.1478

[24] H. Li, H. Zhu, B. Jun, and D. Choi, "Guest editorial : Security and privacy of P2P networks in emerging smart city," *Peer-to-Peer Netw. Appl.*, vol. 8, pp. 1023–1024, 2015. https://doi.org/10.1007/s12083-015-0393-4

[25] K. Fuchs, D. Herrmann, A. Micheloni, and H. Federrath, "Laribus : Privacy-preserving detection of fake SSL certificates with a social P2P notary network," *Eurasip J. Inf. Secur.*, vol. 2015, no. 1, pp. 1–17, 2015.

[26] L. Chen, W. S. Soh, and A. Hu, "An improved Kademlia protocol with double-layer design for P2P voice communications," *2014 Communications Security Conference (CSC 2014)*. pp. 1–8, 2014.

[27] R. Pecori, "Trust-based storage in a Kademlia network infected by Sybils," *2015 7th International Conference on New Technologies, Mobility and Security (NTMS).* pp. 1–5, 2015. https://doi.org/10.1109/NTMS.2015.7266529

[28] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, "Thwarting traceback attack on Freenet," *2013 IEEE Global Communications Conference (GLOBECOM).* pp. 741–746, 2013. https://doi.org/10.1109/GLOCOM.2013.6831161

[29] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, "A Traceback Attack on Freenet," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99. p. 1, 2015. https://doi.org/10.1109/TDSC.2015.2453983

[30] S. Roos, F. Platzer, J. M. Heller, and T. Strufe, "Inferring obfuscated values in Freenet," *2015 International Conference and Workshops on Networked Systems (NetSys).* pp. 1–8, 2015. https://doi.org/10.1109/NetSys.2015.7089062

[31] K. Suto, H. Nishiyama, N. Kato, T. Nakachi, T. Fujii, and A. Takahara, "THUP: A P2P Network Robust to Churn and DoS Attack Based on Bimodal Degree Distribution," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9. pp. 247–256, 2013. https://doi.org/10.1109/JSAC.2013.SUP.0513022

[32] F. D. A. López-Fuentes and S. Balleza-Gallegos, "Evaluating Sybil Attacks in P2P Infrastructures for Online Social Networks," *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*. pp. 1262–1267, 2015. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.252

[33] M. A. Simplicio, M. A. S. Santos, R. R. Leal, M. A. L. Gomes, and W. A. Goya, "SecureTCG: a lightweight cheating-detection protocol for P2P multiplayer online trading card games," *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2412–2431, 2014. https://doi.org/10.1002/sec.952

[34] K. Deltouzos, I. Gkortsilas, N. Efthymiopoulos, M. Efthymiopoulou, and S. Denazis, "SeekStream: Adapting to dynamic user behavior in P2P video-on-demand," *Int. J. Commun. Syst.*, vol. 29, no. 8, pp. 1365–1394, 2016. https://doi.org/10.1002/dac.3105

[35] M. Mu, J. Ishmael, W. Knowles, M. Rounce, N. Race, and M. Stuart, "P2P-Based IPTV Services : Design, Deployment, and QoE Measurement," *IEEE Trans. Multimed.*, vol. 14, no. 6, pp. 1515–1527, 2012. https://doi.org/10.1109/TMM.2012.2217119

[36] S. Yildirim, M. Sayit, and G. Kardas, "A belief-desire-intention agent architecture for partner selection in peer-to-peer live video streaming applications," *Expert Syst.*, vol. 32, no. 3, pp. 327–343, 2015. https://doi.org/10.1111/exsy.12086

[37] H. R. Ghaeini, B. Akbari, B. Barekatain, and A. Trivino-Cabrera, "Adaptive video protection in large scale peer-to-peer video streaming over mobile wireless mesh networks," *Int. J. Commun. Syst.*, vol. 29, no. 18, pp. 2580–2603, Dec. 2016. https://doi.org/10.1002/dac.3088

[38] H. Luo, W. An, S. Ci, and D. Wu, "A distributed utility-based scheduling for peer-to-peer video streaming over wireless networks," *Wirel. Commun. Mob. Comput.*, vol. 16, no. 12, pp. 1556–1569, 2016. https://doi.org/10.1002/wcm.2614

[39] C. Peersman, C. Schulze, A. Rashid, M. Brennan, and C. Fischer, "iCOP : Automatically Identifying New Child Abuse Media in P2P Networks," In *2014 IEEE Security and Privacy Workshops* (pp. 124-131). IEEE. https://doi.org/10.1109/SPW.2014.27

[40] N. Efthymiopoulos, S. L. Tompros, A. Christakidis, K. Koutsopoulos, and S. Denazis, "Enabling live video streaming services realization in telecommunication networks using P2P technology," *Int. J. Commun. Syst.*, vol. 24, no. 10, pp. 1354–1374, 2011. https://doi.org/10.1002/dac.1250

[41] A. Alasaad, S. Gopalakrishnan, and V. C. M. Leung, "Extending P2PMesh: topology-aware schemes for efficient peer-to-peer data sharing in wireless mesh networks," *Wirel. Commun. Mob. Comput.*, vol. 13, no. 5, pp. 483–499, 2013. https://doi.org/10.1002/wcm.1115

[42] C. Peersman, C. Schulze, A. Rashid, M. Brennan, and C. Fischer, "iCOP: Live forensics to reveal previously unknown criminal media on P2P networks," *Digit. Investig.*, vol. 18, pp. 50–64, 2016. https://doi.org/10.1016/j.diin.2016.07.002

[43] X. Kang and Y. Wu, "Fighting Pollution Attack in Peer-to-Peer Streaming Networks: A Trust Management Approach," in *Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference*, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 537–542. https://doi.org/10.1007/978-3-642-30436-1_45

[44] A.-C. G. Anadiotis, C. Z. Patrikakis, and A. Murat Tekalp, "Information-centric networking for multimedia, social and peer-to-peer communications," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 4, pp. 383–391, 2014. https://doi.org/10.1002/ett.2814

[45] H. Yang, M. Liu, B. Li and Z. Dong, "A P2P network framework for interactive streaming media", *Proc. 11th Int. Conf. Intell. Hum.-Mach. Syst. Cybern. (IHMSC)*, vol. 2, pp. 288-292, 2019. https://doi.org/10.1109/IHMSC.2019.10162

[46] J. Li, C. Li, Z. Fang, H. Wang, and Y. Wu, "Optimal layer division for low latency in DHT-based hierarchical P2P network," *Int. J. Netw. Manag.*, vol. 26, no. 2, pp. 95–110, 2016. https://doi.org/10.1002/nem.1922

[47] Y. Ma, Z. Tan, G. Chang, and X. Wang, "A New P2P Network Routing Algorithm Based on ISODATA Clustering Topology," *Procedia Eng. Adv. Control Eng. Inf. Sci.*, vol. 15, pp. 2966–2970, 2011. https://doi.org/10.1016/j.proeng.2011.08.558

[48] D. Yang, Y. Zhang, H. Zhang, T.-Y. Wu, and H.-C. Chao, "Multi-factors oriented study of P2P Churn," *Int. J. Commun. Syst.*, vol. 22, no. 9, pp. 1089–1103, 2009. https://doi.org/10.1002/dac.1001

[49] P. Narang, S. Ray, and C. Hota, "PeerShark : Detecting Peer-to-Peer Botnets by Tracking Conversations," In *2014 IEEE Security and Privacy Workshops* (pp. 108-115). IEEE, 2014. https://doi.org/10.1109/SPW.2014.25

[50] K. Althobaiti, S. J. Alotaibi, and H. Alqahtani, "Random walk with jumps: A new query search method based on analysing Gnutella protocol," *2015 World Congress on Internet Security (WorldCIS)*. pp. 125–130, 2015. https://doi.org/10.1109/WorldCIS.2015.7359427

[51] S. Corigliano and P. Trunfio, "Exploiting sleep-and-wake strategies in the Gnutella network," *2014 International Conference on Collaboration Technologies and Systems (CTS)*. pp. 406–412, 2014. https://doi.org/10.1109/CTS.2014.6867596

[52] L. Chen, W. S. Soh, and A. Hu, "An improved Kademlia protocol with double-layer design for P2P voice communications," in *Communications Security Conference (CSC 2014)*, pp. 1–8. https://doi.org/10.1049/cp.2014.0727

[53] Y. Gao, J. Shi, X. Wang, Q. Tan, C. Zhao and Z. Yin, "Topology measurement and analysis on Ethereum P2P network", *Proc. IEEE Symp. Comput. Commun.*, pp. 1-7, 2019. https://doi.org/10.1109/ISCC47284.2019.8969695

[54] Y. Ookita and S. Fujita, "Cost-effective index poisoning scheme for P2P file sharing systems," in 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS). https://doi.org/10.1109/ICIS.2016.7550732

[55] S. K. Awasthi, and Y. N. Singh, "Simplified Biased Contribution Index (SBCI): A mechanism to make P2P network fair and efficient for resource sharing". Journal of Parallel and Distributed Computing, vol. 124, pp. 106-118, 2019. https://doi.org/10.1016/j.jpdc.2018.10.002

[56] Q. Wang, J. Wang, J. Yu, M. Yu, and Y. Zhang, "Trust-aware query routing in P2P social networks," *Int. J. Commun. Syst.*, vol. 25, no. 10, pp. 1260–1280, 2012. https://doi.org/10.1002/dac.1320

[57] H. A. Kurid, T. S. Alnusairi, and H. S. Almujahed, "OBAME: Optimized Bio-inspired Algorithm to Maximize Search Efficiency in P2P Databases," *Procedia Comput. Sci.*, vol. 21, pp. 60–67, 2013. https://doi.org/10.1016/j.procs.2013.09.010

[58] A. Adala and N. Tabbane, "Discovery of semantic Web Services with an enhanced-Chord-based P2P network," *Int. J. Commun. Syst.*, vol. 23, no. 11, pp. 1353–1365, 2010. https://doi.org/10.1002/dac.1110

[59] L. Ricci, A. Iosup, and R. Prodan, "Large scale distributed cooperative environments on clouds and P2P," *Peer-to-Peer Netw. Appl.*, vol. 9, pp. 1126–1127, 2016. https://doi.org/10.1007/s12083-016-0447-2

[60] A. Boukhadra, K. Benatchba, and A. Balla, "Similarity Flooding for Efficient Distributed Discovery of OWL-S Process Model in P2P Networks," *Procedia Comput. Sci.*, vol. 56, pp. 317–324, 2015. https://doi.org/10.1016/j.procs.2015.07.214

[61] S. Ali, K. Wu, and H. Khan, "Traffic Anomaly Detection in the Presence of P2P Traffic," in *39th Annual IEEE Conference on Local Computer Networks*, 2014, pp. 482–485. https://doi.org/10.1109/LCN.2014.6925822

[62] J. Jusko and M. Rehak, "Identifying peer-to-peer communities in the network by connection graph analysis," *Int. J. Netw. Manag.*, vol. 24, no. 4, pp. 235–252, 2014. https://doi.org/10.1002/nem.1862

[63] H. Hsieh and M. Chiang, "Improvement of the Byzantine Agreement Problem under Mobile P2P Network," *IERI Procedia*, vol. 10, pp. 45–50, 2014. https://doi.org/10.1016/j.ieri.2014.09.089

[64] A. Alasaad, S. Gopalakrishnan, and V. C. M. Leung, "Replication schemes for peer-to-peer content in wireless mesh networks with infrastructure support," *Wirel. Commun. Mob. Comput.*, vol. 15, no. 4, pp. 699–715, 2015. https://doi.org/10.1002/wcm.2376

[65] H. Kavalionak and A. Montresor, "P2P and Cloud : A Marriage of Convenience for Replica Management," In: *Kuipers F.A., Heegaard P.E. (eds) Self-Organizing Systems. IWSOS 2012. Lecture Notes in Computer Science, vol 7166. Springer, Berlin, Heidelberg*, pp. 60–71, 2012.. https://doi.org/10.1007/978-3-642-28583-7_6

[66] S. Jo, G. Kim, and J. Han, "Convergence P2P context awareness," *Peer-to-Peer Netw. Appl.*, vol. 9, pp. 461–464, 2016. https://doi.org/10.1007/s12083-015-0419-y

[67] N. Anjum, D. Karamshuk, M. Shikh-Bahaei, and N. Sastry, "Survey on Peer-assisted Content Delivery Networks," *Comput. Networks*, 2017. https://doi.org/10.1016/j.comnet.2017.02.008

[68] Y. Lee, and J. Cho, "RFID-based sensing system for context information management using P2P network architecture", Peer-to-Peer Networking and Applications, vol. 11, no. 6, pp. 1197-1205, 2018. https://doi.org/10.1007/s12083-018-0636-2

[69] E. Mousavi Khaneghah, S. L. Mirtaheri, M. Sharifi, and B. Minaei Bidgoli, "Modeling and analysis of access transparency and scalability in P2P distributed systems," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 2190–2214, 2014. https://doi.org/10.1002/dac.2467

[70] M. Garmehi, M. Analoui, M. Pathan, and R. Buyya, "An economic mechanism for request routing and resource allocation in hybrid CDN–P2P networks," *Int. J. Netw. Manag.*, vol. 25, no. 6, pp. 375–393, 2015. https://doi.org/10.1016/j.csi.2015.08.008

[71] G. Cui, M. Li, Z. Wang, J. Ren, D. Jiao, and J. Ma, "Analysis and evaluation of incentive mechanisms in P2P networks: a spatial evolutionary game theory perspective," *Concurr. Comput. Pract. Exp.*, vol. 27, no. 12, pp. 3044–3064, 2015. https://doi.org/10.1002/cpe.3207

[72] L. Liu, N. Antonopoulos, S. Mackin, J. Xu, and D. Russell, "Efficient resource discovery in self-organized unstructured peer-to-peer networks," *Concurr. Comput. Pract. Exp.*, vol. 21, no. 2, pp. 159–183, 2009. https://doi.org/10.1002/cpe.1329

[73] M. Li, J. Wang, K. Lu, C. Guo, and X. Tan, "A Novel Reputation Management Mechanism with Forgiveness in P2P File Sharing Networks," *Procedia Comput. Sci.*, vol. 94, pp. 360–365, 2016. https://doi.org/10.1016/j.procs.2016.08.055

[74] K. Lu, J. Wang, L. Xie, Q. Zhen, and M. Li, "An EigenTrust-based Hybrid Trust Model in P2P File Sharing Networks," *Procedia Comput. Sci.*, vol. 94, no. Bdstc, pp. 366–371, 2016.

[75] H. Alharbi and A. Hussain, "An Agent-Based Approach for Modelling Peer to Peer Networks," *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*. pp. 532–537, 2015. https://doi.org/10.1109/UKSim.2015.47

[76] C. H. Lin, J. J. Zseng, and S. Y. Hsieh, "Improving the Search Mechanism for Unstructured Peer-to-Peer Networks Using the Statistical Matrix Form," *IEEE Access*, vol. 3. pp. 926–941, 2015. 10.1109/ACCESS.2015.2444872

[77] R. Ieong, P. Lai, K.-P. Chow, F. Law, M. Kwan, and K. Tse, "A Model for Foxy Peer-to-Peer Network Investigations," in *Networked Services and Applications - Engineering, Control and Management: 16th EUNICE/IFIP WG 6.6 Workshop*, G. Peterson and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 175–186.

https://doi.org/10.1007/978-3-642-04155-6_13

[78] C. Vélez-Rivera, E. Arzuaga-Cruz, A. A. Irizarry-Rivera, and F. Andrade, "Global data prefetching using BitTorrent for distributed smart grid control," *2016 North American Power Symposium (NAPS)*. pp. 1–6, 2016. https://doi.org/10.1109/NAPS.2016.7747904

[79] P. Kopiczko, W. Mazurczyk, and K. Szczypiorski, "StegTorrent : A Steganographic Method for the P2P File Sharing Service," in *IEEE Security and Privacy Workshops*, 2013. https://doi.org/10.1109/SPW.2013.11

[80] B. Mitra, S. Ghose, N. Ganguly, and F. Peruani, "Stability analysis of peer-to-peer networks against churn," *Pramana*, vol. 71, no. 2, pp. 263–273, 2008. https://doi.org/10.1007/s12043-008-0159-0

[81] S. Huang, E. Izquierdo, and P. Hao, "Adaptive packet scheduling for scalable video streaming with network coding," *J. Vis. Commun. Image Represent.*, vol. 43, pp. 10–20, 2017. https://doi.org/10.1016/j.jvcir.2016.11.014

[82] P. Chauhan, "Fault Tolerant Decentralized Scheduling Algorithm for P2P Grid," vol. 6, pp. 698–707, 2012. https://doi.org/10.1016/j.comnet.2014.12.009

[83] X. Meng and D. Liu, "GeTrust: A guarantee-based trust model in Chord-based P2P networks," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99. p. 1, 2016. https://doi.org/10.1109/TDSC.2016.2530720

[84] A. Ullah, "mSCTP & P2P (2-layered CHORD) supported decentralized seamless mobility framework," *2015 International Conference on Emerging Technologies (ICET)*. pp. 1–5, 2015. https://doi.org/10.1109/ICET.2015.7389214

[85] Z. M. Ding and Q. Qian, "A chord-based load balancing algorithm for P2P network," *ICINS 2014 - 2014 International Conference on Information and Network Security*. pp. 91–96, 2014. https://doi.org/10.1049/cp.2014.1271

[86] J. Skodzik, P. Danielis, V. Altmann, and D. Timmermann, "HaRTKad: A hard real-time Kademlia approach," *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*. pp. 309–314, 2014. https://doi.org/10.1109/CCNC.2014.6866588

[87] H. Y. Lee and A. Nakao, "Approaches for Practical BitTorrent Traffic Control," in *38th Annual IEEE Conference on Local Computer Networks Approaches*, 2013, pp. 382–389. https://doi.org/10.1109/LCN.2013.6761270

[88] S. Neuner, M. Schmiedecker, and E. R. Weippl, "PeekaTorrent : Leveraging P2P hash values for digital forensics," *Digit. Investig.*, vol. 18, pp. S149–S156, 2016. https://doi.org/10.1016/j.diin.2016.04.011

[89] S. Heymann and B. L. Grand, "Monitoring user-system interactions through graph-based intrinsic dynamics analysis," *IEEE 7th International Conference on Research Challenges in Information Science (RCIS)*. pp. 1–10, 2013. https://doi.org/10.1109/RCIS.2013.6577695

[90] I. Roy, B. Gupta, B. Rekabdar, and H. Hexmoor, "A Novel approach toward designing a non-DHT Based Structured P2P network architecture", in *Proceedings of 32nd International Conference on*, vol. 63, pp. 182-188, 2020.

[91] D. Fukuchi, C. Sommer, Y. Sei, and S. Honiden, "Distributed Arrays: A P2P Data Structure for Efficient Logical Arrays," *IEEE INFOCOM 2009*. pp. 1458–1466, 2009. https://doi.org/10.1109/INFCOM.2009.5062062

[92] F. D. A. López-fuentes, I. Eugui-de-alba, and O. M. Ortíz-ruiz, "Evaluating P2P Networks against Eclipse Attacks," *Procedia Technology*, vol. 3, pp. 61–68, 2012. https://doi.org/10.1016/j.protcy.2012.03.007

[93] I. Hwang and A. T. Liem, "A Hybrid Scalable Peer-to-Peer IP-Based Multimedia Services Architecture in Ethernet Passive Optical Networks," *J. Light. Technol.*, vol. 31, no. 2, pp. 213–222, 2013. https://doi.org/10.1109/JLT.2012.2227941

[94] D. Germanus, H. Ismail, and N. Suri, "PASS: An Address Space Slicing Framework for P2P Eclipse Attack Mitigation," *2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS)*. pp. 74–83, 2015. https://doi.org/10.1109/SRDS.2015.14

[95] M. Kellett, T. Tran, and M. Li, "Trust by association: A meta-reputation system for peer-to-peer networks," *Comput. Intell.*, vol. 27, no. 3, pp. 363–392, 2011. https://doi.org/10.1111/j.1467-8640.2011.00388.x

[96] W. Liu, P. Ren, D. Sun, K. Liu, and J. Wu, "TrustP2PNet: P2P Social Network with Admission Control Model based on Trust," *AASRI Procedia*, vol. 5, pp. 281–286, 2013. https://doi.org/10.1016/j.aasri.2013.10.090

[97] L. Yan, C. Zhuo, and Z. Hua, "Improving Sharing Efficiency in Online Short Video System through Using P2P Based Mechanism," *Procedia Engineering*, vol. 29, pp. 3207–3211, 2012. https://doi.org/10.1016/j.proeng.2012.01.467

[98] P. Liu, G. Huang, J. Cheng, S. Feng, and J. Fan, "Fibonacci Ring Overlay Networks with Distributed Chunk Storage for P2P VoD Streaming," *Procedia Comput. Sci.*, vol. 9, pp. 1354–1362, 2012. https://doi.org/10.1016/j.procs.2012.04.149

[99] F. Song, W. Gao, G. Zhang, D. Gao, and H. Jiang, "A P2P Based Video on Demand System for Embedded Linux," *Procedia Eng.*, vol. 29, pp. 3070–3074, 2012. https://doi.org/10.1016/j.proeng.2012.01.442

[100] S. Datta and H. Kargupta, "A communication efficient probabilistic algorithm for mining frequent itemsets from a peer-to-peer network," *Stat. Anal. Data Min.*, vol. 2, no. 1, pp. 48–69, 2009. https://doi.org/10.1002/sam.10033

[101] K. Pal, M. C. Govil, and M. Ahmed, "Slack time–based scheduling scheme for live video streaming in P2P network", International Journal of Communication Systems, vol. 31, no. 2, e3440, 2018. https://doi.org/10.1002/dac.3440

[102] M. Picone, M. Amoretti, and F. Zanichelli, "An Evaluation Criterion for Adaptive Neighbor Selection in Heterogeneous Peer-to-Peer Networks," pp. 144–156, 2009. https://doi.org/10.1007/978-3-642-04994-1_12

[103] H. Guo, J. Liu, and Z. Wang, "Frequency-Aware Indexing for Peer-to-Peer On-Demand Video Streaming," *2010 IEEE International Conference on Communications*. pp. 1–5, 2010. https://doi.org/10.1109/ICC.2010.5502373

[104] R. S. Cruz and M. S. Nunes, "A P2P streaming architecture supporting scalable media," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 5, pp. 758–776, 2015. https://doi.org/10.1007/s12083-014-0284-0

[105] Y. Liu, J. Liu, J. Song, and A. Argyriou, "Scalable 3D video streaming over P2P networks with playback length changeable chunk segmentation," *J. Vis. Commun. Image Represent.*, vol. 31, pp. 41–53, 2015. https://doi.org/10.1016/j.jvcir.2015.05.012

[106] U. Cuajimalpa, "P2P Video Streaming Strategies based on Scalable Video Coding," *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 113–124.

[107] F. A. Lopez-Fuentes, "P2P video streaming strategies based on scalable video coding," *J. Appl. Res. Technol.*, vol. 13, no. Feb., pp. 113–124, 2014.

[108] M. S. Raheel, R. Raad, and C. Ritz, "Achieving maximum utilization of peer's upload capacity in p2p networks using SVC," *Peer-to-Peer Netw. Appl.*, pp. 1–21, 2015. https://doi.org/10.1007/s12083-015-0406-3

[109] M. R. Haque, R. Ahmed, and R. Boutaba, "QPM: Phonetic aware P2P search," *2009 IEEE Ninth International Conference on Peer-to-Peer Computing*. pp. 131–134, 2009. https://doi.org/10.1109/P2P.2009.5284536

[110] D. Talia and P. Trunfio, "Dynamic Querying in Structured Peer-to-Peer Networks," in *Managing Large-Scale Service Deployment: 19th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management*, F. De Turck, W. Kellerer, and G. Kormentzas, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 28–41.

https://doi.org/10.1007/978-3-540-87353-2_3

[111]A. Arunachalam and O. Sornil, "Issues of Implementing Random Walk and Gossip Based Resource Discovery Protocols in P2P MANETs & Suggestions for Improvement," *Procedia Comput. Sci.*, vol. 57, pp. 509–518, 2015. https://doi.org/10.1016/j.procs.2015.07.374

[112]J. Loganathan, Logitha, and A. Veronica, "Distributed resource management scheme using enhanced artificial bee-colony in P2P," *2015 2nd International Conference on Electronics and Communication Systems (ICECS).* pp. 1035–1039, 2015. https://doi.org/10.1109/ECS.2015.7124737

[113]R. Julius, M. Wichtlhuber, P. Heise, and D. Hausheer, "vINCENT : An Incentive Scheme Supporting Heterogeneity in Peer-to-Peer Content Distribution," in *39th Annual IEEE Conference on Local Computer Networks*, pp. 19–27, 2014. https://doi.org/10.1109/LCN.2014.6925752

[114]K. Lu, S. Wang, G. Cui, M. Li, and H. Liaqat, "Multi-reciprocity Policies Co-evolution Based Incentive Evaluating Framework for Mobile P2P Systems," *IEEE ACCESS*, vol. 5, pp. 3313 - 3321, 2016. https://doi.org/10.1109/ACCESS.2016.2630736

[115]G. Goth and T. Commission, "ISP Traffic Management: Will Innovation or Regulation Ensure Fairness?," *IEEE Distributed Systems Online*, vol. 9, no. 9, pp. 1–4, 2008. https://doi.org/10.1109/MDSO.2008.27

[116]H. Zhi-jie, W. Ru-chuan, and D. Xiao-yang, "A Novel P2P traffic Prediction Algorithm Based on Hybrid Model," *Phys. Procedia*, vol. 25, no. 1, pp. 1218–1225, 2012. https://doi.org/10.1016/j.phpro.2012.03.223

[117]I. Dedinski, H. DeMeer, L. Han, L. Mathy, D. P. Pezaros, J. S. Sventek, and X. Y. Zhan, "Cross-Layer Peer-to-Peer Traffic Identification and Optimization Based on Active Networking," in *Active and Programmable Networks: IFIP TC6 7th International Working Conference*, D. Hutchison, S. Denazis, L. Lefevre, and G. J. Minden, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 13–27. https://doi.org/10.1007/978-3-642-00972-3_2

[118]C.-H. Hsu, C.-G. Hsu, S.-C. Chen, and T.-L. Chen, "Message transmission techniques for low traffic P2P services," *Int. J. Commun. Syst.*, vol. 22, no. 9, pp. 1105–1122, 2009. https://doi.org/10.1002/dac.1010

[119]Z. Li and Q. Liao, "Network pricing: can both ISP and P2P benefit?," *Int. J. Netw. Manag.*, vol. 24, no. 6, pp. 433–449, 2014. https://doi.org/10.1002/nem.1869

[120]R. Casadesus-Masanell and A. Hervas-Drane, "Peer-to-Peer File Sharing and the Market for Digital Information Goods," *J. Econ. Manag. Strateg.*, vol. 19, no. 2, pp. 333–373, 2010. https://doi.org/10.1111/j.1530-9134.2010.00254.x

[121]J. Yimu, Y. Yongge, Z. Chuanxin, J. Chenchen, and W. RuChuan, "Research of a Novel Flash P2P Network Traffic Prediction Algorithm," *Procedia Comput. Sci.*, vol. 55, pp. 1293–1301, 2015. https://doi.org/10.1016/j.procs.2015.07.140

[122]C. Rossow, D. Andriesse, T. Werner, and F. Fkie, "SoK : P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets," in *IEEE Symposium on Security and Privacy*, 2013. https://doi.org/10.1109/SP.2013.17

[123] N. Z. M. Safar, N. Abdullah, H. Kamaludin, S. Abd Ishak, and M. R. M. Isa, "Characterising and detection of botnet in P2P network for UDP protocol" *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 3, pp. 1584-1595, 2020. https://doi.org/10.11591/ijeecs.v18.i3

[124]J.-S. Hua, S.-M. Huang, D. C. Yen, and C.-W. Chena, "A dynamic game theory approach to solve the free riding problem in the peer-to-peer networks," *J. Simul.*, vol. 6, no. 1, pp. 43–55, 2012. https://doi.org/10.1057/jos.2011.11

[125]X. Kang and J. Yang, "Viewing experience optimization for peer-to-peer streaming networks with credit-based incentive mechanisms," *Comput. Networks*, vol. 114, pp. 67–79, Feb. 2017. https://doi.org/10.1016/j.comnet.2017.01.005

[126]Z. Wang, C. Wu, L. Sun, and S. Yang, "Strategies of collaboration in multi-swarm peer-to-peer content distribution," *Tsinghua Sci. Technol.*, vol. 17, no. 1, pp. 29–39, 2012. https://doi.org/10.1109/TST.2012.6151905

[127]Z. Yulan and J. Chunfeng, "Research of Trust Model in P2P File-Sharing System," *Procedia Environ. Sci.*, vol. 12, pp. 1208–1212, 2012. https://doi.org/10.1016/j.proenv.2012.01.409

[128]H. A. Kurdi, "HonestPeer : An enhanced EigenTrust algorithm for reputation management in P2P systems," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, no. 3, pp. 315–322, 2015. https://doi.org/10.1016/j.jksuci.2014.10.002

[129]M. Tauhiduzzaman and M. Wang, "Fighting pollution attacks in P2P streaming," *Comput. Networks*, vol. 79, pp. 39–52, 2015.

[130] S. Rahmadika, S. Noh, K. Lee, B. J. Kweka, and K. H. Rhee, "The dilemma of parameterizing propagation time in blockchain P2P network". Journal of Information Processing Systems, vol. 16 no. 3, pp. 699-717, 2020. https://doi.org/10.3745/JIPS.03.0140

[131]K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2294–2303, 2016. 10.1109/ACCESS.2016.2566339

[132]H. Yi . "Securing e-voting based on blockchain in P2P network". EURASIP Journal on Wireless Communications and Networking, vol. 1, pp. 1-9, 2019. https://doi.org/10.1186/s13638-019-1473-6

[133]F. Franzoni, and V. Daza, "Clover: An anonymous transaction relay protocol for the bitcoin P2P network", Peer-to-Peer Networking and Applications, vol. 15, no.1, pp. 290-303, 2022. https://doi.org/10.1007/s12083-021-01241-z

[134] S. Jo, and J. Han, "Convergence P2P cloud computing". Peer-to-Peer Networking and Applications, vol. 11, no. 6, pp. 1153-1155, 2018. https://doi.org/10.1007/s12083-018-0661-1

[135]C.-C. Wang and Y.-D. Lin, "CDNPatch: A cost-effective failover mechanism for hybrid CDN-P2P live streaming systems," *Int. J. Commun. Syst.*, vol. 29, no. 17, pp. 2517–2533, 2016.

[136]N. Thomas, M. Thomas, and K. Chandrasekaran, "Multimedia Streaming using Cloud-Based P2P Systems," *Procedia Comput. Sci.*, vol. 57, no. Icrtc, pp. 25–32, 2015. https://doi.org/10.1002/dac.3193

[137]N. Wahidah, B. Ab, K. Jenni, S. Mandala, and E. Supriyanto, "Review On Cloud Computing Application In P2P Video Streaming," *Procedia - Procedia Comput. Sci.*, vol. 50, pp. 185–190, 2015. https://doi.org/10.1016/j.procs.2015.04.082

[138]T. Myneedu and Y. Guan, "Evidence Collection in Peer-to-Peer Network Investigations," in *Advances in Digital Forensics VIII: 8th IFIP WG 11.9 International Conference on Digital Forensics*, G. Peterson and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 215–230. https://doi.org/10.1007/978-3-642-33962-2_15

[139]Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, "A trust-based minimum cost and quality aware data collection scheme in P2P network". *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2300-2323, 2020. https://doi.org/10.1007/s12083-020-00898-2

[140] W. Hou, Y. Jiang, W. Lei, A. Xu, H. Wen, and S. Chen, "A P2P network based edge computing smart grid model for efficient resources coordination". *Peer-to-Peer Networking and Applications*, vol. 13 , no. 3, pp. 1026-1037, 2020. https://doi.org/10.1007/s12083-019-00870-9

[141]M. Averkiou, "Digital Watermarking." *Department of Computer Science University of Cyprus*

Frederick Ojiemhende Ehiagwina was born in Benin City, Edo state, Nigeria. He obtained his Bachelor degree in Electrical Electronics Engineering from Ambrose Alli University, Ekpoma, Edo state, Nigeria in April 2010. He did his Masters Degree in Electrical Engineering (Electronics and Telecommunication option) from the university of Ilorin, Kwara state Nigeria. His research interests include optimization of telecommunication systems, design and characterization of electronics system, reliability assessment of electrical and electronics systems, and renewable energy. He is currently a Lecturer I in the Federal Polytechnic, Offa, Kwara state, Nigeria. Engr. Ehiagwina is a registered member of the Council for the Regulation of Engineering in Nigeria. He has about 50 conference and journal papers.

Nurudeen Ajibola Iromini obtained a Higher National Diploma in Computer Science from Osun State Polytechnic, Iree, Osun State in 2003. In 2008 he obtained a Bachelor of Technology in Computer Engineering from Ladoke Akintola University, Ogbomoso, Oyo State, Nigeria. He obtained a Masters Degree in Computer Science in 2012 from the the University of Ibadan, Oyo State. Engr. Iromini is a registered member of the Council for the Regulation of Engineering in Nigeria (COREN).

Ikeola Suhurat Olatinwo obtained his doctorate in computer science from the University of Ilorin in 2021. She had obtained her Bachelor's and Masters degree in Computer Science from Same University in 2000 and 2014 respectively. Her research interest is on adaptive learning style predictive model for the physically challenged student. She is a member of the following professional bodies: Computer Professional Regulation Council of Nigeria (CPN), Nigeria Computer Society (NCS), Nigeria Women in Information Technology (NIWIIT) and Academia in Information Technology Profession (AITP). She is currently a Senior Lecturer in the Federal Polytechnic, Offa, Kwara state, Nigeria

Kabirat Oyinlola Raheem obtained a Bachelor degree in Electrical/Electronics Engineering from Kwara State University in 2017. She is currently do her Masters Degree in Electrical/Electronics Engineering from same University. She is currently an Assistant Lecturer in the Federal Polytechnic, Offa, Kwara state, Nigeria.

Khadijat Oladoyin Mustapha obtained a Bachelor degree in Electrical/Electronics Engineering from Kwara State University in 2018. She is currently do her Masters Degree in Electrical/Electronics Engineering from same University. She is currently an Assistant Lecturer in the Federal Polytechnic, Offa, Kwara state, Nigeria