A Survey of Fast File Sharing System in Network

[1]Suthir S, [2]Dr.S.Janakiraman

[1]Research Scholar, [2]Assistant Professor

[1]Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India
[2]Banking Technology [IT], Pondicherry University, Pondicherry, India

---

***Abstract* — The Phenomenal survey for file sharing in network is done based on some of the characteristics like speed and security. Perhaps, our protection loom not only considers the shrinking the size of network traffic that wishes to survive traced but also investigate to get better sustainability of the structure. File deduplication is a procedure for abolish replica photocopy of file, and has been broadly used in database storage to shrink database free space and upload bandwidth. On the other hand, there is simply single large number of clients used copy for every record stock up in database archive. As an outcome, deduplication method progresses storage consumption while dropping consistency. Protection Examination exhibit that our deduplication method is safe in conditions of the characterization mentioned in the planned security representation. For future achievement, all the characteristics of Peer-to-Peer file sharing with Speed, Security and Deduplication together enhance its exhibitions and procedures distributed in the literature.**

***Index Terms*—Fast file sharing, File security, Deduplication**

---

1. Introduction and Survey of Fast File Sharing, Security and Deduplication

In the peer-to-peer systems, a peer can acts as both client and server besides sharing responsibilities among the parties. We can search, upload and download is sharing with all the peers connected. Peer-to-Peer is noticeably more benefit from the point of examination of consistency, healthiness and scalability. For long distance connections, we cannot give assurance for speed on the network. In this paper, we present a broad review of fast file sharing, security and deduplication performances study in the peer-to-peer paradigm. We split speed, security and deduplication areas taken as survey separately for facilitate us to understand the concept.

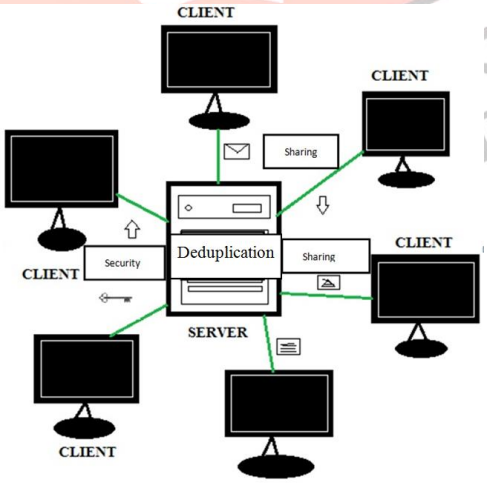

Figure 1: Overview of File Sharing, Security and Deduplication in Peer-to-Peer Paradigm

1.1 Related Survey of Fast File Sharing

The Peer-to-Peer overcomes measurability drawbacks of normal client/server approach. BitTorrent was quickly accepted by all content providers as measurable way to decrease load on congested severs and fast deliver of content. BitTorrent is 2nd generation of peer network called Torrent. Any application using Peer-to-Peer will require two function supported as:
1) Search function which makes peer to locate the interested content among the networks and

2) To download once it is located.
BitTorrent does not provide search, but expect peer to search from central based search using supporting websites. It uses file sharing policy instead of direct sharing [1].

Here, centralized server serves the requests among the clients in a radical manner by using load-balancing algorithms for equalizing the load among nodes. Based on their level of operation, the approaches are classified as object placement, routing protocol, and underlay. The classification of load balancing mechanisms has two approaches such as overlay specific solutions and overlay independent approach that are more advantageous than prior one. Approaches to Distributed Hash Table (DHT) load balancing mainly interfere with namespace, request rate, and routing such as object placement, routing concerns, traffic next to the stage of the underlay network. Some examples of DHT overlays are chord, Content Addressable Network (CAN). There are some widely accepted approaches for network proximity such as Topology based IDs, proximity routing. Load balancing is used to rise up whenever a system comprises multiple components contributing to achieve a common goal. Tackling at best one or several of the balancing objectives might jeopardize the efficiency of another one [2].

Traffic model and analysis of peer-to-peer framework technique based on mesh-pull model is explained. Survey of structure in peer network is explained. Flow of data is collected in single peer. The proposed system will classify the behavior of torrent client. It is cost effective with high bandwidth streams. Workload models are analyzed with real time control components in peer-to-peer control protocol. The statically classification motivation is recommended. Efficient input rate is provided sufficiently. It is used in android smart phones etc. Next bit torrent swarming model is used for tracers bit torrent traffic measurement in wimax performed as bus ride through secure connection. Loss due to handoff can get new IP address. Analysis of flow data exchange factor is explained. Classification of peer group via adjusts point investigation by paretto model, which uses random variables. Peer-to-Peer exchange pattern is analyzed by change point detection technique through segmentation of population. Linear structure of exchange in logarithm values is done. It is to produce integrity model and efficient awareness decimation protocol in this model. It is to suggest to less the overload of the traffic. It has limitations of single point. It is difficult in multi-point measurement [10].

Automated traffic for identification for traffic generator application interests the network operation to manage their networks. The packet based traffic classification is done based on payload of many packets in every flow or on basic flow without packet data. In this paper, automated technique is used to trace traffic with less computation and recollect base stamp. Quality of Service (QoS) in the internet is today's challenge for network developments. Before, the traffic classification was simple as it uses well defined port numbers signed Internet Assigned Number Authority (IANA). Many applications have been reused as voice over IP and peer-to-peer file sharing system. Many firewall routers have been used over dynamic port such as http, smtp [8].

1.2 Related Survey of File Security

DNS detect and uses command and control server. In this paper, they provide system to detect Advanced Persistent Threat (APT), which steals the sensitive data. It uses malicious Domain Name Service (DNS) analysis technique for detecting APT malware, as it is hard to detect. APT can be invading ant viruses passing by firewalls also. If change of IP address of command and control server into the malware binary, then it causes damage to system as it helps to hide the actual attack of the attacker. As APT malware depends on DNS for attack, it is to be removed. It is very different from bots and worms. APT controls the machines and steal confidential data, than to launch DOS attack and sent spam mails [4].

DNS is used for basic name resolution and many internet services. The traffic cannot be blowing out completely. DNS TXT record bases BOTNET communication DNS traffic and DNS TXT record. BOTNET –based attacks are similar to the DDOS attacks such as spam mails etc. BOTNET have command and control servers to BOTNET infected systems. The legitimate TXT records and malicious DNS traffic are categorized and actions are taken accordingly. Two form BOTNET communication such as via resolver, which uses DNS resolver and via non-resolver does not. The main goal is to detect DNS based BOTNET communication with TXT records and DNS resolver [3].

1.3 Related Survey of File Deduplication

The highlighting theme of the proposed system is minimization of incurred overhead in real time environments. The processes in the proposed system are file sharing primarily and can be split and crypt into segments by using Deduplication technique. The data retrieval can be done by using the secret shares from the minimized number of servers. This process leads to data integrity and tag consistency. This supports for fault tolerance and data storage efficiency as well as security [5].

Adverse behavior and security is to find the adversary introduce no of dummy users and prevent them accessing the personal details of clients, the goal of the simulator is to imitate every communication involving the two servers, and every communication from the non-adversarial server to the dummy users. Many implementation phases are used such as duplicating sharing is one of them. Computing difficulty, Interface difficulty, pre-computating difficulty is explained in the SPDZ (pronounced "Speedz") framework. This generic framework is suitable to deal with multi client transactions in malicious model securely with large amount of data computation efficiently [9].

Network operations there are two understanding roles of caching on the performance of phases. Firstly, Giving content locally, where in the conventional caching method replicating is used making the requested content close to the client. If client finds that it is nearby then the content is served as local. The central server only sends the requested file by simple orthogonal unit cast transaction. If more than one client then it uses the multicast stream. As making conventional cache memory remarkable by storing total content in local cache memory. Secondly, creating simultaneous coded-multicasting, it is followed to satisfy the request many clients with many different wants in single multicast stream. Decoding is enabled in local cache to find request areas in data streams, so by its actual client demands are known and designed carefully .It is used to reduce network congestion, it effects the average global cache size in large enough to store total content. Central server arranges the subset cache carefully not to overlap. Coordination in placement phase is not possible to eliminate rate reduction [7].

2. PERFORMANCE OF FAST FILE SHARING, SECURITY AND DEDUPLICATION

2.1 BitTorrent file sharing

BitTorrent which is quite famous approach in sharing large files using peer-to-peer method. It has mechanisms as tit-for-tat, rarest first to enable efficient distribution of files in network. TFT and rarest first mechanism is given important in BitTorrent success. The steps of file sharing by BitTorrent are explained in detail. It uses swarming technique, which breaks file into fixed size piece for file exchange. It uses pipelining for TCP protocol and generally it is split into 16 kilo bytes in size called chunks or blocks. Chocking is used for refusing of upload but connections are not closed. Mainly to maximize capacity of service. It also has piece selection strategy for providing strict priority, Rarest first, Random first piece policies. System like Slurpie, Fox are proposed by researches for BitTorrent like system. Slurpie for improving downloading rate. Fox to make stable connection. They proposed a central schedule file distribution for BitTorrent approach, which minimizes the end-to-end delay of file among multiple receivers. Homogeneous and Heterogeneous analytical models are proposed. Fluid-flow model is explained, peer arrival rate to torrent is decreased simultaneously and some other existing systems are analyzed in this paper. Improvement in BitTorrent of overlay Topology development and maintenance by proximity awareness and ISP-friendly technique [1].

2.2 Load Balancing Techniques

This study is applicable for direct peer-to-peer IP based peer-to-peer systems but not for mobile ad-hoc networks. Here, load relates to objects, peers or links whose load is induced based on its size and popularity. Each node has limited capacity, processing time, or bandwidth. The high level architecture includes set of nodes with some identifying space and that space is divided into set of overlapping ranges that are allocated to individual nodes. For fair distribution of nodes and keys among identifier space, one classical approach call as “Namespace Binding” with hash tables. The routing tables gives the list of outgoing links leading to immediate neighbors using a routing algorithm which select as next hop a neighbor node chooses the closest possible preceding neighbor to the destination as the next hop. Pastry is the methodology that is ring like structure where node id is derived by hashing an IP address or a user public key. This scenario has some causes of imbalance such as overlay namespace, requests at same frequency, routing and underlying topology. Referring to object placement, hash functions are used to map objects and for storing equal amount of information on each node and request rate balancing by using caching or replication. Coming to load balancing, peer-to-peer system has a good performance in terms of overlay and routing load. Proximity neighbor selection is used in the overlays, which allow multiple eligible nodes such as pastry, which selects closest node in terms of hop count, delay, geographical distance etc. These are to restrict the random location choice to an appropriate zone, called as Locality Community Area Network (CAN) [2].

2.3 Traffic Analysis

Different approaches are done in correct stage of traffic classification one of them is deep packet inspection, which identify protocol pattern of messages in different applications. Analyzing packet data in classified approach beats in unencrypted traffic. In this paper, laboratory research of artificial users and traffic in network is exampled and verify those methods to real time networks. Kiss algorithm where x^2 statistics as computation of first few bytes are appeared as very few promising it may achieve 99% accuracy in flow classification [11] [8]. Classification of traffic data is done in this model. This Markov graph tree models explains and improves the performance prediction with maximum depth. Random forest is another popular method used for the classification in individual decision tree data to take all decisions. Context Tree Weighting Method (CTW) method is used in worst cases in need. On other hand Deep Packet Inspection (DPI) approach uses less memory computation complexity with traffic class and number of used signature [12]. Traffic classification algorithm works differently in different networks. It is to filter out added noise in training set to work proposed made better. There are some limitations as proposed model depends on payload of network traffic, as encrypted network cannot handle itself where until today internet traffic is unencrypted. It is venerable to malicious used beyond that it guesses. Good performance in P2P traffic clarification in real time [8].

2.4 DNS Command and Control Performances

Behavior of APT is different from flux and DGA (Domain Generation Algorithm) such as short file as it does not include meaningful words. Here APT malware command and control server comprise dynamic Content Delivery Network (CDN). Moreover, engine is build to reside for check of IP addresses are infected or not. It checks the count of request in DNS network and very low frequency. Time To Live (TTL) is used to resolve cache response result for domain signature based detection in the feature. It plays important role in IDS mismatch of protocol and port values, which improve cause of APT attack improvement. Mismatch of uplink and downlink traffic, encrypted data transfer on used port. Heartbeat packet traffic who sends packets to client to other end one. Data training sets are important in machine less algorithm. Malicious DNS detector is classified and evaluation by sustainability of the system. In this paper, APT intrusion is feasible with high efficiency and accuracy [4].

2.5 Performance of Deduplication system

Data security, data confidentiality, efficiency, as well as tag consistency are obtained by this performance of deduplication system. The deduplication techniques are used instead of convergent encryption. The supportive methodology for the proposed technique is usage of short cryptographic hash value for the sensitive computed information and can be forwarded to the storage server as the finger print fragment stored at every individual server. An outsource data storage technique called Storage Cloud Service Provider (S-CSP) will only stores a unique copy of all the files and retrieves the data content. Basically, there will be two kind of attackers: inside attacker, who have the details regarding partial process inside the system and outside attacker, who have the processing acknowledgement with the public channels. Here S-CSP is the security model, which improves confidentiality, Integrity and Message authentication code. The file-level distributed deduplication system are used for the efficient support of sensitive data by attaching security related tags while file uploading and downloading. Two methods are used for Deterministic secret sharing schemes whereas in the first method, the secret key sharing and second method is used for system setup and attack detection. Enhanced deduplication System with proof of ownership enable the weakness of security in traditional duplication system. Convergent encryption ensures the data privacy in deduplication. Harnik et al [13] illustrated the number of attacks that leads to data leakage while Ateniese et al [14] gave the concept of data possession. Secret sharing scheme and Tag generation scheme are the building blocks for the proposed system. Reliable data duplication techniques are prominently used for retrieval of data and to reduce the network as well as storage overhead. Ramp secret sharing scheme is incur for small encoding and decoding techniques and operations too [5] [15].

Table 1: Performance of Measure based- Studies File Sharing and Security

Reference Papers	Traffic	Routing	Efficiency	Compatibility	Load balance
Survey on Load Balancing in Peer-to-Peer Distributed Hash [2]	Imbalance in underlying network	Path redundancy is good, have linked reorganization	High	Medium	Efficient
A Survey of Bit Torrent Performance [1]	More in downloading	Rarest First	Less	Offline Compatible	-
Analysis of Via-Resolver DNS TXT Queries and Detection Possibility of Botnet Communications [3]	Full time cannot be blown out	-	Medium	-	-
Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis [4]	Mismatch of uplink and downlinks	Using DNS	High	High	-
Decentralized Coded Caching Attains Order-Optimal Memory-Rate Tradeoff [7]	Shifts Traffic	Less	-	High	-

Efficient Methods for Early Protocol Identification [8]	Automatic Identification	Firewall based	Very High	High	-

2.6 Security with multiple servers and multiple clients

The security for the computation of two non-colliding external servers. Security is given base on collaborative filters. Adversal control server cannot interrupt recommendation process such that incorrect recommendation cannot be detected by clients. Secured multi-party computation which is cryptology paradigm where single secure computation is performed and deleted. Two servers do not collaborate and many users are involved online. In practice, two servers could be service provider which provides particular services. Lack of sufficient generic use of other applications. The main goal of securing the system is not to allow servers to learn how personal details of the clients be malicious model. This model corrects the client output is good preserved as output cannot be corrupted by server itself. Prevention to deduce the personal data than protocol outputs by dummy users by malicious server is shown as not possible in this model. We use SPDZ framework network for secure multi-party transaction. SPDZ is extended to client-server model to produce secure protocols to clients. Client secure integrity division protocol by SPDZ. The solution should be independent, non-corruptible which takes all inputs on process privately from different clients in network. The goal preprocessing is to remove the complexity and interaction from the actual computation as much as possible, which results to makes this computation extremely efficient [9].

2.7 Caches in Network

The proposed algorithm can work in placement phase with unknown number of clients placed in remote networks and act independent to each other. Thus algorithm is decentralized .In delivery phase some clients are connected through a narrow way link. Firstly informed the set of active clients and their request and cache contents. Conventional coded scheme will improve the decentralized algorithm. The algorithm compact by way of unidentified phases as with no caching, local and universal gain. We can see the shared content close to network but not directly connected. It has to be flexible. It caused caching in indirect coded and network coding. Caching random linear caching is not efficient. First to spread available content over different caches. The performance of system is optimized between these two objective struck. It is highly suboptimal. In online code caching the LRU eviction scheme is used which is not possible in multicasting stream. So decentralized algorithm is used to solve this problem [7].

3. SUMMARY

The summary of this paper is to provide methods to find solutions to previous paper limitations. Tackling at best one or several of the balancing objectives might jeopardize the efficiency of another one. Coming to load balancing peer-to-peer system has a good performance in terms of overlay and routing load. There are three widely accepted approaches for network proximity such as Topology based IDs, proximity routing. Load balancing is used to rise up whenever a system comprises multiple components contributing to achieve a common goal. The high-level architecture includes set of nodes with some identifying space and that space is divided into se of overlapping ranges that are allocated to individual nodes. Distribution of nodes and keys in identifier space, one classical approach is “namespace binding” using hash tables.

Next comes to traffic, the traffic cannot be blow out completely. DNS TXT record bases BOTNET communication DNS traffic and DNS TXT record. BOTNET based attacks are similar to the DDOS attacks such as spam mails etc. BOTNET have command and control servers to BOTNET infected systems. The legitimate TXT records and malicious DNS traffic are categorized and actions are taken accordingly. The paper identifies the DNs TXT record have 99.5% are legitimate. Domain flux or fast flux techniques are used in future work.

Next comes security, As APT malware depends on DNS for attack, it is to be removed. It is very different from bots and worms. APT controls the machines and steal confidential data, than to launch DOS attack and sent spam mails. In this paper, IDNS is proposed to detect APT malware, which is placed on network edge. It is only reduces network traffic not improving sustainability. Here Deduplication techniques are used for distributing the data chucks across multiple cloud servers. Data security, data confidentiality, efficiency as well as tag consistency are obtained by the proposed system. The deduplication techniques are used instead of convergent encryption. The highlighting theme of the proposed system is minimization of incurred overhead in real time environments.

Table 2: Summary of Analysis based studies of Security and Deduplication

Reference papers	Techniques used	Merits	Demerits
Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis [4]	IDNS, TTL	Improves sustainability, High efficient and ease identification of malicious software	Sometimes may generate false priorities, complex computational procedure
Secure Distributed Deduplication Systems with Improved Reliability [5]	S-CSP	Eliminate duplicate copies of minimum storage, maximizes confidentiality and integrity.	Large data encoding is complex.
A Framework for Secure Computations with Two Non-Colluding Servers and Multiple Clients, Applied to Recommendations [9]	SPDZ framework	Collaborative filtering, Efficient computation.	Pre-computational complexity
New Algorithms for Secure Outsourcing of Large-Scale Systems of Linear Equations [6]	Full homographic encryption, Spare matrix	Avails large capital and hardware	Suffers from privacy security challenges

The processes in the proposed system are file sharing primarily and can ne spitted and cryptic into segments by using deduplication technique. Ramp secret sharing scheme is incur for small encoding and decoding techniques and operations too. Prevention to deduce the personal data than protocol outputs by dummy users by malicious server is shown as not possible in this model. We use SPDZ framework network for secure multi-party transaction. SPDZ is extended to client-server model to produce secure protocols to clients. This generic framework is suitable to deal with multi client transactions in malicious model securely with large amount of data computation efficiently.

Next comes to BitTorrent is approach for sharing large files using P2P method it has mechanisms as tit-for-tat, rarest first to enable efficient distribution of files in network. In this paper, the analyzing, survey of BitTorrent is explained. The P2P overcomes measurability drawbacks of normal client/server approach. Chocking is used for refusing of upload but connections are not closed, mainly to maximize the capacity of service. Interested set of peer transaction are made, TFT uses to identify and prefer peers with best downloading rates in peer selection strategies. In this paper they mentioned the various mechanisms which support BitTorrent approach. This paper it is mainly mentioned it is tried to shift some traffic from high traffic zones to no traffic zones. In online code caching the LRU eviction scheme is used which is not possible in multicasting stream. So decentralized algorithm is used to solve this problem. Many firewall routers have been used over dynamic port such as HTTP, STMP. Different approaches are done in correct stage of traffic classification. These are well-known besides having some disadvantages such as it requires more storage for computation and scanning of packet payload, keeping it update will bend difficult. For more data, it is not practical. Wang et al introduced secured algorithm for large scale linear equation. But it is expensive as others as clients does not trust server, Goke, Mironove introduce the ringers concept to solve this method for verifiable computation but it is inefficient for practical issues. The proposed algorithm users spare matrix to examine server-client in large system of linear equation. It should have strict diagonally dominant matrix. In this paper, any traffic model and analysis of peer-to-peer framework technique based on mesh-pull model is explained. Survey of file sharing with security and avoid duplication of files in peer network is explained. The proposed system will collect these features and enhance the characteristics of Peer-to-Peer file sharing with Speed, Security and Deduplication.

4. CONCLUSION AND FUTURE WORK

In conclusion of the survey paper, firstly we had taken survey of some supporting papers based on network sharing, security and Deduplication methods. We have discussed some of the network problems as traffic, high load balance and security issues. The traffic in the network causes the delay in the file sharing which may cause security attack by attacker as it takes more time to transfer the files or data. Therefore, to improve the fast file sharing latest techniques are paused in p2p networks many techniques such as decentralized code caching algorithm, S-CSP etc… are discussed with their advantages and disadvantages. Secondly, security is one of the main thing in network due to unauthorized viewers can view the data from network, techniques like SPDZ, C&C Server etc… framework used to secure the data. It is surveyed how these techniques useful in providing the security in network Layer by using all these techniques from all the survey papers we further will be develop a system with all these features to implement. Finally, based on these survey my proposed system will focus on P2P file sharing by enhance the characteristics of Speed, Security and Deduplication.

REFERENCES

[1] Raymond Lei Xia and Jogesh K. Muppala, "A Survey of BitTorrent Performance" in IEEE Communications Surveys & Tutorials, vol. 12, no. 2, second quarter 2010.

[2] Pascal Felber, Member, IEEE, Peter Kropf, Member, IEEE, Eryk Schiller, and Sabina Serbu, "Survey on Load Balancing in Peer-to-Peer Distributed Hash Tables" in IEEE communications surveys & tutorials", vol. 16, no. 1, first quarter 2014.

[3] Hikaru Ichise, Yong Jin and Katsuyoshi Iida, Tokyo Institute of Technology, Japan "Analysis of Via-Resolver DNS TXT Queries and Detection Possibility of Botnet Communications" in IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), 2015.

[4] Guodong Zhao, Ke Xu, Lei Xu And Bo Wu, "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis" in IEEE Access Special Section On Big Data For Green Communications And Computing- August 2015.

[5] Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang, Yang Xiang, Senior Member, IEEE, Mohammad Mehedi Hassan, Member, IEEE, and Abdulhameed Alelaiwi, Member, IEEE, "Secure Distributed Deduplication Systems with Improved Reliability", in IEEE Transactions on Computers, vol. 64, no. 12, December 2015.

[6] Xiaofeng Chen, Xinyi Huang, Jin Li, Jianfeng Ma, Wenjing Lou, and Duncan S. Wong, "New Algorithms for Secure Outsourcing of Large-Scale Systems of Linear Equations", in IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, January 2015.

[7] Mohammad Ali Maddah-Ali, Member, IEEE, and Urs Niesen, Member, IEEE, "Decentralized Coded Caching Attains Order-Optimal Memory-Rate Tradeoff in IEEE/ACM Transactions on Networking", vol. 23, no. 4, August 2015.

[8] Bela Hullar, Sandor Laki, and Andras Gyorgy, "Efficient Methods for Early Protocol Identification in IEEE Journal on Selected Areas in Communications", vol. 32, no. 10, October 2014.

[9] Thijs Veugen, Robbert de Haan, Ronald Cramer, and Frank Muller, "A Framework for Secure Computations with Two Non-Colluding Servers and Multiple Clients, Applied to Recommendations", in IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, March 2015.

[10] Philipp M. Eittenberger Udo R. Krieger Faculty WIAIOtto-Friedrich-University96045 Bamberg, GERMANY Natalia ,M. Markovich Institute of Control Sciences Russian Academy of Sciences,117997 Moscow, RUSSIA, "Teletraffic Modeling of Peer-To-Peer Traffic", in IEEE Proceedings of the Winter Simulation Conference 2012.

[11] A. Finamore, M. Mellia, M. Meo, and D. Rossi, "Kiss: Stochastic packet inspection," in Proc. 1st Int. Workshop TMA, 2009, pp. 117–125.

[12] Opendpi Webpage. [Online]. Available: http://www.opendpi.org/

[13] D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage," IEEE Secur. & Privacy, vol. 8, no. 6, pp. 40–47, Nov./Dec. 2010.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[15] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proc. ACM Conf. Comput. Commun. Secur., 2011, pp. 491–500.