Analyzing Internet Censorship in Pakistan

Giuseppe Aceto, Alessio Botta, Antonio Pescapé
University of Napoli Federico II (Italy),
and NM2 S.r.l. (Italy),
{giuseppe.aceto, a.botta, pescape}@unina.it

M. Faheem Awan, Tahir Ahmad, Saad Qaisar
National University of Science and Technology, NUST (Pakistan),
{10mscsemawan,11msccstahmad,saad.qaisar}@seecs.edu.pk

***Abstract*—Internet Censorship is unceasingly increasing in many countries worldwide in order to restrict web contents within the country premises. According to latest Open Net Initiative (ONI) report, almost 50 countries are involved in web censorship, including Pakistan. This paper presents the methodology and the measurement analysis based on publicly available censored URLs in Pakistan, providing both qualitative and quantitative results to gauge how major ISPs are censoring web content in Pakistan. This is the first study in literature analyzing and comparing the behaviour of five ISPs in Pakistan using automated detection methods based on active probing measurements. Our results show that (i) WiTribe, PTCL, and Nayatel block content by using DNS tampering while (ii) Wateen and Qubee apply filtering, using HTTP tampering. We comment on these results by considering the evolution over time of the forced censorship mechanisms. Finally, we performed a University closed survey in order to find out circumvention techniques adopted by users in Pakistan and we report that Pakistani users try to evade censorship by using web proxies, Tor and VPN.**

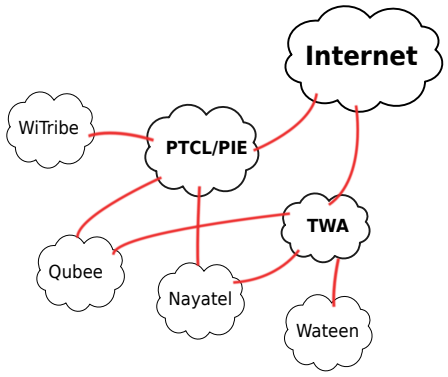

Fig. 1: Internet architecture in Pakistan, limited to ISPs considered in this study (from public BGP peering data).

I. Introduction

Internet censorship can be defined as: "the intentional impairing of a client application in communicating with its server counterpart, enforced by a third party (neither the user, nor the server operator)" [1]. This practice has been found applied to different extent and in different ways in almost 50 countries worldwide [2], [3], regardless of their form of government or their economic development. A number of characteristics of censorship, including its visibility, side-effects, and the accountability of the censors, depend on the details of implementation of the censorship techniques. This leads to the necessity of censorship *detection*, i.e., the procedure of investigating network data aimed at revealing impairments in access to data or services due to a third party (neither the host nor the client) and cannot be termed as an outage [1]. In this paper, we present results of a censorship detection campaign in Pakistan, over a time span of 6 months. The study aimed at investigating difference over time in application of censorship for major Internet service providers in the country, characterized by different access technologies offered to an end user and diverse upstream connection to Internet. Figure (1) shows the Internet connectivity in Pakistan and the position in the network hierarchy of the ISPs considered in this paper.

Pakistan Telecommunication Authority (PTA) is responsible for auditing and regulation of ISPs while the Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW) [4] is responsible for monitoring and blocking Web sites containing blasphemous, pornographic, or anti-state material. Due to its religious-based law, the governmental control on communications, and its communication infrastructure, Pakistan constitutes a valuable observation point for studying the phenomenon of Internet censorship. In this paper we present analysis results of a censorship detection experimental campaign run from inside five Pakistani ISPs: WiTribe, Nayatel, PTCL, Qubee, Wateen; we show how censorship techniques vary across ISPs and in time, over a period of 6 months. We complement the censorship analysis with a survey on circumvention techniques adopted by University campus users.

The rest of the paper is organized as follows. We give a brief background on Internet censorship detection, and known facts on censorship in Pakistan, in Section II. We then analyze related work in Section III. The measurement metrics and the approaches employed for our study are discussed in Section IV. Section V presents the experimental results of our tests and survey. We finally conclude the paper in Section VI.

II. Background

Several techniques have been used in order to gather data on censorship, differing on how network data has been collected, where, and with which specific objective. Regarding methods, passive ones can be used, i.e., considering network traffic independently generated by third party applications, or active ones, i.e., purposely generating "probe" traffic to elicit a specific response from the network under analysis. Regarding the point of observation, it can be on an end host (client-side, or server-side), when the considered traffic is originated from or addressed to such host, or in between. Different techniques for enforcing Internet censorship are possible, and detection methods have requirements and efficacy that depend on the addressed censoring method. In this paper we adopt client-based, active detection techniques. The outcome of the probing is analyzed to infer what a user would experience in

same netork in terms of blocked access to online resources; moreover the specific techniques adopted to block the access are inferred. A peculiar characteristic of our measurement campaign is the type of hosts we use as vantage points: we run the probing software on gateway routers at volunteers' homes. This setup allows us to share the same view of a home user, without being affected by performance and connectivity issues due to the LAN or WLAN, without interfering with user activities, and without being restricted to online time patterns of a personal device such as a desktop or tablet pc, or a smartphone, nor on the user time and attention. Deployment and run of tests, and collection and analysis of results, are all performed automatically, not requiring any intervention from the user and allowing for consistency of experimental conditions and results. To contextualize our contribution, we briefly describe hereafter the state of art in Internet censorship detection. One of most cited censorship detection tools is Herdict [5], a crowd-sourced censorship monitoring project. Its interface to the users is a website allowing the user to report of "inaccessibility" of URLs as they experience it; the URLs to be checked are provided by a few affiliated organizations or by the users themselves. The website also presents current and historical inaccessibility reports from all the users, aggregated per country and averaged on time. Due to the basic nature of the test, such results offer a superficial analysis of censorship, without insights about the applied censoring techniques, and are prone to a number of issues related with the manual and possibly subjective nature of the test. Nevertheless, it constitutes a much valuable resource in collection of censored URLs and promotion of awareness and accountability of Internet censorship. A platform specifically designed for continuous censorship monitoring by means of automated active measurements is presented in [6]. This platform, named CensMon, uses as vantage points the PlanetLab [7] measurement facility, composed of virtualized servers hosted in universities and research centers networks. Different tests are performed allowing the differentiation among a set of censoring techniques. The analysis of results obtained with CensMon regards a measurement period of two weeks, and are aggregated with country granularity. Finally, a complete framework for implementing censorship detection tests is OONI, presented in [8]. The main tool is in active development at the time of writing, and it is publicly available, equipped with several tests already implemented [9], While future additions are in development or planned, in the current state it consists of a manually operated software probe (a Python script) performing active measurements and local detection tests, leveraging the Tor anonymity overlay network [10]. Other tools and publications have addressed Internet censorship and its detection, proposing new detection techniques, or new detection platforms, or focusing on censoring systems of specific countries: we refer to [1] for an extensive analysis of these topics.

A. Internet Censorship in Pakistan

According to Open Net Initiative report [11], Pakistan is among the list of countries that restricts the Internet content, socially, politically and religiously. In 2006, Pakistan blocked 12 websites for hosting blasphemous content. Among blocked websites also include Blogspot. Because of lack in censorship techniques instead of blocking the content, the entire Blogspot was blocked. In 2008, Pakistan also blocked YouTube and made its services unavailable for approximate two hours, but this was due to false Border Gateway Protocol (BGP) advertisements and impact was worldwide. Pakistan, in 2010 made the world news to block Facebook and other URLs in reaction to blasphemy concerns. Similarly in 2012, an infinite ban on YouTube was imposed because of a controversial movie, which was later removed in January 2016. Internet filtering in Pakistan rests unpredictable and sporadic, with filtering mainly targeted to the content of what is considered a threat to national security and religious content which is considered as blasphemous.

III. Related Work

Other scientific works have discussed Internet censorship applied in different countries worldwide, including Pakistan, but few focus specifically on this country with an in-depth analysis: the most recent one is [12]. In this paper the authors leverage traffic traces captured at a non-disclosed ISP described as "medium-size ISP in a major city in Pakistan". The considered traffic traces derive from 6 captures whose duration ranges between 6 and 20 hours, unevenly distributed over about 22 months. With respect to this work, we provide a view based on more recent data, collected from vantage points serviced by 5 different ISPs. Besides the peculiar setup based on *passive* traffic analysis, the results described in [12] refer to the single non-disclosed ISP, not allowing for a generalization of the results or a comparison across different ISPs.

Another work that analyzes censorship in Pakistan is [13], where a Python script is used to perform censorship tests of different nature, from desktop computers, at night time. The process of test execution, collection and analysis of results are manual and the number of measurements performed is not disclosed. Different from [13], we employed an automatic deployment, collection and analysis procedure; our probing algorithm is running on home gateway routers, in 15 private houses of volunteers. This allows us to collect a high number of measurements, evenly distributed in the whole day, and spanning six months; thanks to this measurement setup in the analysis algorithm we account for transient errors or anomalous conditions by requiring consistency of results over 70% of measurements. Moreover, unlike [13] that used a stale list of blocked URLs, we employed an updated list of URLs, collected by volunteers in the censored country, integrated with URLs automatically retrieved from [5]. Finally, we analyze a set of ISPs operating with different access technologies, including Fiber-To-The-Home, ADSL, Wi-MAX, showing that the possibly different setups and access technologies do not significantly affect censorship enforcement effects.

Different anti-censorship practices have been developed to circumvent the aforesaid technical filtering methods. An analysis of anti-censorship applications and circumvention methods is described in [14], that we have used as a basis for the creation of our closed survey.

We have provided preliminary data on Pakistan in a previous work [15] introducing the analysis performed by means of the UBICA platform; with respect to such work, the results presented in the current paper are based on a different dataset, deriving from a targeted measurement campaign focused on Pakistan only, considering a set of ISPs chosen to maximize coverage of connectivity market and variety of access

technologies, and almost doubling the timespan of collected measurements.

IV. Censorship Measurement

In this Section, we describe the setup adopted to collect data, the active probing performed, and the analysis method adopted for detection of Internet censorship in Pakistan.

A. Measurement Setup

We implemented our probing tests as `bash` script, employing publicly available, standard network tools such as `netcat`, `curl`, and `nslookup` to generate probe traffic. We leverage the automated management system of the BISMark project [16] to deploy our probing software on home gateway routers, that run a modified version of OpenWRT linux distribution. The measurements were taken from each vantage point up to six times a day, each time addressing a limited number of target URLs, in order to complete the measurement process in a time span ranging from 40 to 220 seconds. The interval was empirically tested to not impact on user experience. Measurement outcomes were automatically uploaded to a management server, where they were processed and stored in a SQL database. Periodically, the censorship detection algorithm is applied to stored data. Table I provides details on the measurement points, the time period for which these tests were performed and the ISP hosting the probes.

TABLE I: Summary of Measurements.

ISP	Measurements	Time span
PTCL	409,353	Nov. 2013 – Mar. 2014
WiTribe	270,408	Oct. 2013 – Mar. 2014
Wateen	54,388	Nov. 2013 – Mar. 2014
Qubee	183,413	Nov. 2013 – Mar. 2014
Nayatel	375,661	Oct. 2013 – Dec. 2013

B. Censorship Tests

In the following, we describe active measurements performed from the vantage points.

DNS resolution: In order to collect evidence for tampering with DNS resolution phase, a DNS type A query for the domain of the target URL was issued towards the default resolver. The potential results from this query can be [17]:

- NXDOMAIN: Non existing domain
- NO ERROR: No error observed for a queried domain
- SERVFAIL: Server cannot process the query
- NOANSWER: Server replies with no answer
- TIMEOUT: Server goes silent and did not reply back

In order to check for different techniques of DNS tampering, the same query was also issued to open resolvers, named as control resolvers [13]: difference in outcome between the default resolver and the control ones are a symptom of DNS hijacking, likely performed at ISP DNS servers, while same results in correspondence of censorship are a symptom of DNS injection, a Man-in-the-middle attack performed by means of a middlebox.

TCP Reachability: After the DNS test, TCP reachability has been evaluated, in order to check whether censorship is triggered by IP destination address and transport port of a target. The test was executed starting a three way handshake with the host addressed with the IP returned by the default resolver at previous step. The potential outcomes from this test can be:

- Open: SYN+ACK received
- RST: Connection reset
- Timeout: Timeout expires before any answer
- Network error: Target not accessible.

Up to three attempts are made by sending a SYN packet, until either one of aforementioned outcomes occurs. The first time a packet flagged with SYN+ACK is returned (if ever), the target is considered reachable at the TCP layer.

HTTP reachability: Once TCP level connectivity is checked, an HTTP GET request for the URL is issued towards the target, and response is collected. In case a response code of type `30`*X* (HTTP redirect) is received, redirection URL is followed, issuing a new request. Headers and content of the last response are saved, together with last URL requested and number of redirects. The request eventually ends with one of the following outcomes:

- HTTP 200 OK: no error
- HTTP error: an error code is returned
- Network error: target unreachable
- Maximum number of redirects: 50 redirects performed
- Timeout: No response in 15 seconds.

C. Censorship detection algorithm

An analysis engine, written in Python, periodically processes database, considering for each target URL results from multiple probes over varying time span. These results include percentages of NO error, percentages of non-existing domains, percentage of open TCP ports and similarly percentages of blocked pages for different ISPs in Pakistan. From which we infer the censorship techniques employed by different ISPs in Pakistan. During first phase, DNS censorship detection is performed; if a certain URL has same result of non-existing domain more than 70 percent of times, it is marked as DNS tampered, otherwise the process goes into second phase and looks into open/closed TCP ports. The algorithm also looks into DNS blocked pages percentage and similarly inferring whether the URL is DNS tampered or not. In case, if the results of TCP reachability are greater than 70 percent, the URL is marked as TCP tempered. After TCP check the algorithm checks for HTTP content size to that of a version of the resource obtained through a probe located outside the analyzed country (in USA). If the content size is less than one half of the reference content size, the URL is marked as HTTP content tampered. Figure 2 shows the pseudocode of decision making algorithm.

V. Experimental Results

This section presents results showing how different ISPs implement censorship in Pakistan.

WiTribe. WiTribe provides its services using WiMax. Our experimental results were gathered for duration of approximately six months. We present the results for censorship

```
for each URL
    if domain resolved as NX_Domain > 70% measurements
        then mark as "DNS tampering"
    else if resolved as blockpage IP > 70% measurements
        then mark as "DNS tampering with blockpage"
    else if TCP not reachable in > 70% measurements
        then mark as "TCP Non Reachability"
    else if HTTP size < 50% reference content size
        then mark as "HTTP tampering"
```

Fig. 2: Pseudocode of censorship detection algorithm.

detection in case of a user, using WiTribe Pvt. Limited as broadband service provider. Figure 3 gives different results showing that WiTribe performs selective filtering. In case of

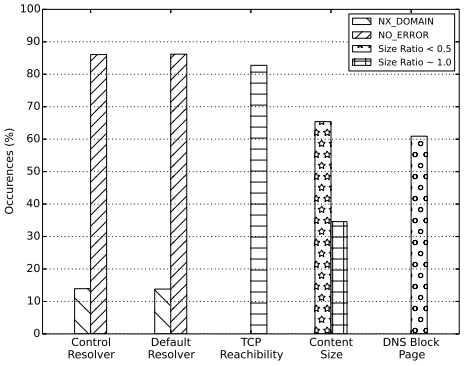

Fig. 3: DNS, TCP, HTTP results: WiTribe.

DNS tests, figure 3 shows greater percentage of occurrence for NO_Error while less percentages of NX_domain were being observed. This means that the ISP is not applying censorship at DNS level. In case of TCP reachability tests, most of the ports seems to be open, i.e., percentage of occurrences was about 80 percent, resulting in clue that TCP ports are open and filtering is not applied at TCP level. While looking into content size and DNS block pages, the occurrence percentages of DNS block pages was above sixty percent, which gives a hint that the corresponding ISP is blocking the Internet content by tampering DNS. WiTribe performs DNS tampering by providing explicit block pages to users.

Nayatel. Nayatel provides its services to users via Fiber to the Home (FTTH), passive optical networks (PON). Our results show that Nayatel implements censorship by using DNS tampering. Figure 4 gives the results obtained for Nayatel. In case of DNS test, as in the case of Witribe, we observed greater percentages of NO_Error while less percentages of NX_Domain. This means that ISP is returning an IP correct or incorrect. As the IP was resolved in case of DNS resolution, than a check on IP and port was being observed. TCP results showed that ports were open and three way handshakes were properly completed resulting in establishment of connection. Similarly for the content size test, we found that about 70% URLs fell short in this test. The content size retrieved is about 50 percent to a size globally available. Looking into the content size, we found that most of the content sizes were even less than 100 KB showing the presence of DNS block pages. From this one can infer that Nayatel is blocking the Internet content

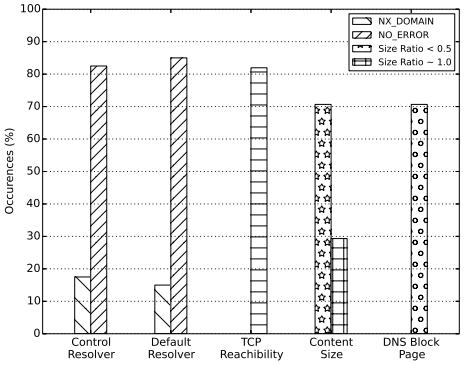

Fig. 4: DNS, TCP and HTTP results: Nayatel.

by using a technique referred as DNS tampering. Nayatel performs DNS tampering by providing blocked page to the user.

PTCL. PTCL provides its services to users using Asymmetric Digital Subscriber Line (ADSL). Figure 5 shows the results for a PTCL user. Our analysis showed that PTCL performs DNS tampering by providing failing IPs as well as providing blocked pages. As for the DNS analysis, results in good percentages of NX_domain means non existing domain. This shows PTCL is applying DNS tampering without any notification. The results were the same for both control resolvers and default resolvers which give clue that PTCL is observing DNS tampering. Similarly looking into TCP reachability it shows the ports were open for URLs which cleared the DNS tests. Similarly the percentage of blocked pages was almost about 60 percent, representing that PTCL also provides blocked pages. PTCL performs DNS tampering by providing blocked pages along with failing IPs.

Qubee. Qubee provides its services using WiMax. Our analysis showed that Qubee is applying discerning filtering over different web contents. The technique used by Qubee is HTTP tampering. Figure 6 shows the results. DNS test performed for Qubee shows that it is not filtering content by

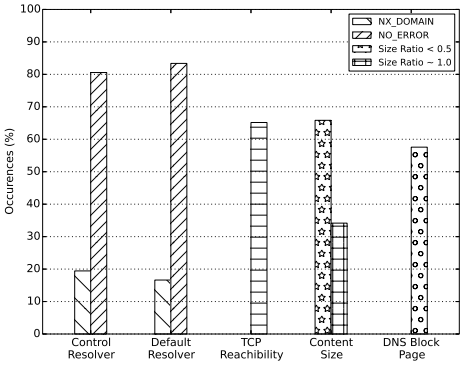

Fig. 5: DNS, TCP and HTTP results: PTCL.

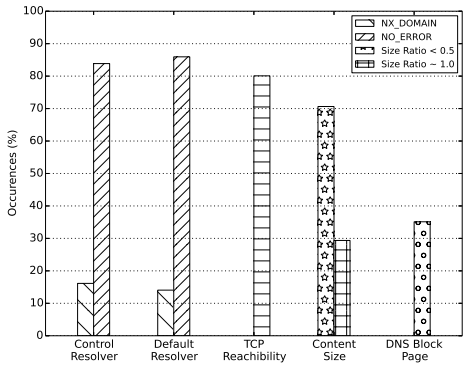

Fig. 6: DNS, TCP and HTTP results: Qubee.

DNS tampering. The results were the same for both control and default resolvers. This means that DNS resolution results in an IP for a respective URL. TCP reachability was almost 80 percent. Looking into content size, we found that the content fetched in Pakistan in case of Qubee was much less than the global content size. Blocked page occurrences were also less which gives the clue that Qubee is blocking the URL resources in Pakistan by HTTP tampering.

Wateen. Wateen provides its broadband services to users via WiMax. The results (see Figure 7) of Wateen infer that it is blocking content in Pakistan using HTTP tampering. Results showed that Wateen passes DNS test along with TCP

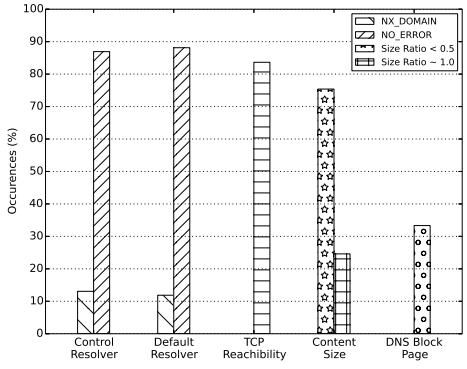

Fig. 7: DNS, TCP and HTTP results: Wateen.

reachability tests. But in case of content size the content size less than 0.5 has approximately 80 percent occurrences; in this way we infer that Wateen is blocking Internet content by HTTP tampering.

From these results, we conclude that in Pakistan - even if different ISPs use different techniques - censorship is mainly deployed by using two techniques i.e. DNS tampering and HTTP tampering.

TABLE II: Time analysis of results: Variations of relative frequency

		Control		Default				
ISP	Time	NXDomain	NOERROR	NXDomain	NOERROR	TCP reach.	SR<0.5	DNS Block Page
PCTL	Nov-Dec	+1	-1	-3	+3	+17	-6	-6
	Dec-Jan	-19	+19	-14	+14	-62	-19	-12
	Jan-Feb	0	0	0	0	0	-16	-16
	Feb-Mar	+20	-20	+20	-20	+29	+24	+14
Wateen	Nov-Dec	0	0	+1	-1	-1	+2	+6
	Dec-Jan	-8	+8	-8	+8	-29	-54	-18
	Jan-Feb	0	0	0	0	0	0	0
	Feb-Mar	+21	-21	+18	-18	+18	+22	-32
Qubee	Nov-Dec	-11	+1	-11	+1	+1	-5	-1
	Dec-Jan	-7	+7	-7	+7	-47	-25	-6
	Jan-Feb	0	0	0	0	0	-16	0
	Feb-Mar	+24	-24	+20	-20	+27	+28	-7
WiTribe	Oct-Nov	-1	+1	-1	+1	0	+1	+1
	Nov-Dec	0	0	0	0	0	-9	-9
	Dec-Jan	-4	+4	-4	+4	-52	-47	-43
	Jan-Feb	0	0	0	0	0	0	0
	Feb-Mar	+16	-16	+16	-16	+35	+39	+35
Nayatel	Oct-Nov	+8	-8	+8	-8	-9	0	0
	Nov-Dec	+1	-1	-1	+1	-2	+3	+3

A. *Time analysis of results*

Thanks to the automated deployment and management of the probes we have been able to collect data over a timespan of up to 6 months; a summary of such results is reported in Table II and discussed hereafter. The Table reports the difference between respective values in the two months indicated in the "Time" column; compared values are shown as percentage of occurrence over measurements, averaged on the considered month.

A pattern can be noticed considering variations between January and February, that are negligible for all the ISPs for the techniques regarding DNS tampering; for Wateen and Witribe this constance of results regards all tests, while on PTCL and Qubee an increase can be found of *Content Size* based tests resulting in no censorship, of these only PTCL ones are associated with an equivalent drop of known *DNS Block Page* cases. From this pattern we speculate that between January and February no significant changes have occurred in the mandated blocklist, possibly with a ban lift applied by PTCL and Qubee, in the first case the blocking technique formerly adopted being DNS redirection to a explicit blocking page.

Outside the interval January-February, we notice much more differences across different ISPs, but for all a variation of test results can be seen before and after the "stasis" period at the beginning of the year. Common traits are an ubiquitous drop of TCP-unreachability outcomes between December and January, and its raise (at levels lower than the pre-stasis) between February and March.

B. *The Survey on Circumvention Techniques*

While working on censorship detection mechanism and analysis of what censorship techniques are deployed in Pakistan, we deployed a university closed survey in order to find out that what circumvention techniques are used in the country, in order to bypass Internet censorship.

The main focus of this research/survey was to point out the most common and popular commercial applications used by clients for Internet censorship circumvention. The array of anti-censorship techniques that resulted from the survey is described in Table III and is based on the classification of circumvention methods analyzed in [14].

TABLE III: Circumvention methods resulting from the survey.

Method	Description
Web Proxy	A web proxy (named *CGI proxy* in [14]) presents the user a web form to request an URL. The web proxy server sends out an HTTP request for the URL to the destination, and returns the result to the web client.
Virtual Private Network	Virtual Private Networks (VPNs) are tools that tunnel the client traffic in an encrypted communication with a server (outside the censored network, when used for circumvention) and then continue in clear from the VPN host to the destination. They are included in *IP tunneling* techniques in [14].
Tor	Tor is an application functionally similar to a VPN, but including multiple encryption tunnels between several servers, of which the last one acts as a exit to the clear Internet. The aim is that intermediate circuit of servers knows at most either where the traffic came from, or where it is going to, but not both. Tor belongs to the *Re-routing* techniques considered in [14].
Content Distribution Networks	Content Distribution Networks (CDNs) are systems that perform mirroring of content to allow better access performance or high availability. Censoring all the mirrors in a CDN can be harder that censoring the original content, thus they can be used as a circumvention tool. CDNs are among *Distributed Hosting* techniques considered in [14].
Search Engine Caches	Search engines can provide cached versions of the content resulting from a search. These can be used to access content when the originating server is censored. They can be considered as a form of *Distributed Hosting* with limitations in freshness of results.
Web-based DNS lookup	Web-based DNS lookup services are offered as troubleshooting and network analysis tool, but can be used as a circumvention tool if the censoring technique is based on DNS tampering. By requesting DNS resolution through HTTP, the untampered reply can be obtained, and used to reach the server hosting the content that would be censored.

The survey was conducted inside University (National University of Science and Technology, Pakistan) main campus and total of 64 users participated in this survey. Figure 8 shows the dominant techniques used in order to evade censorship. About 51 percent users used virtual private networks (VPNs), in which the most prominent one was Hotspot shield. About 25% uses web proxies, 17% uses onion routing, about 7.2% uses content distribution networks, mirror and archive sites, search engine caches, and web based DNS lookup.

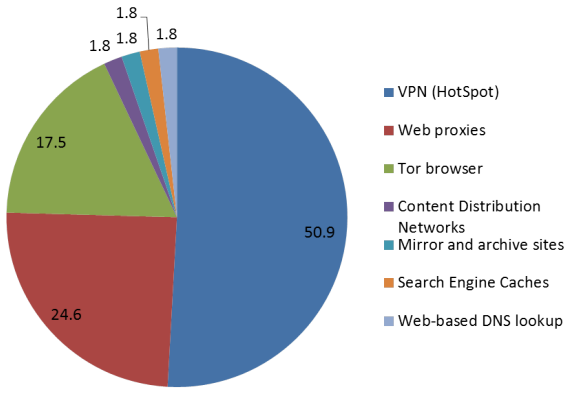

Fig. 8: Circumvention Techniques: results of the survey.

VI. Discussion and Conclusion

This study has cast more light on the degree of Internet censorship in Pakistan. Pakistan, like many countries, applies filtering and censoring only if it considers that the website is not in realm with their religious (the most censored aspect), cultural, economic and political norms. Our analysis shows how different ISPs deploy Internet censorship in Pakistan. The main findings and take home messages can be summarised as follows: (i) **Pakistan applies selective filtering**; (ii) **Different ISPs apply different techniques for filtering**; (iii) **Two main approaches are used. More precisely: WiTribe, PTCL and Nayatel blocks content by using DNS tampering while Wateen and Qubee apply filtering, using content tampering (HTTP tampering)**.

Acknowledgment

The work of Antonio Pescapé and Giuseppe Aceto has been carried out thanks to a Google Faculty Research Award for the project UBICA (User-Based Internet Censorship Analysis); the work of Alessio Botta has been partially funded by NM2 Srl.

References

[1] G. Aceto and A. Pescapé, "Internet censorship detection: a survey," *Computer Networks*, 2015, in press. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615000948

[2] "Open net initiative report," https://opennet.net/research/profiles/pakistan.

[3] P. Gill, M. Crete-Nishihata, J. Dalek, S. Goldberg, A. Senft, and G. Wiseman, "Characterizing web censorship worldwide: Another look at the opennet initiative data," *ACM Transactions on the Web (TWEB)*, vol. 9, no. 1, p. 4, 2015.

[4] "IMCEW," http://dbtb.org/2006/09/03/committee-formed-to-block-websites/.

[5] "Herdict Project," http://www.herdict.org.

[6] A. Sfakianakis, E. Athanasopoulos, and S. Ioannidis, "Censmon: A web censorship monitor," in *USENIX Workshop on Free and Open Communication on the Internet (FOCI)*, 2011.

[7] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman, "Planetlab: an overlay testbed for broad-coverage services," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 3, pp. 3–12, 2003.

[8] A. Filastò and J. Appelbaum, "Ooni: Open observatory of network interference," in *USENIX FOCI*, 2012.

[9] "Tor Project: OONI," https://ooni.torproject.org.

[10] "Tor Project," https://www.torproject.org.

[11] "The Open Net Initiative," https://opennet.net.

[12] S. Khattak, M. Javed, S. A. Khayam, Z. A. Uzmi, and V. Paxson, "A look at the consequences of internet censorship through an isp lens," in *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014, pp. 271–284.

[13] Z. Nabi, "The anatomy of web censorship in pakistan," in *USENIX FOCI 2013*.

[14] J. Palfrey, H. Roberts, and E. Zuckerman, "2007 circumvention landscape report: Methods, uses, and tools," 2009.

[15] G. Aceto, A. Botta, A. Pescapé, N. Feamster, T. Ahmad, and S. Qaisar, "Monitoring Internet Censorship with UBICA," in *Seventh International Workshop on Traffic Monitoring and Analysis (TMA) Barcelona, ES*, April 2015.

[16] S. Sundaresan, W. De Donato, N. Feamster, R. Teixeira, S. Crawford, and A. Pescapè, "Broadband internet performance: a view from the gateway," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, 2011, pp. 134–145.

[17] F. N. Council, "U.S. Government Internet Domain Names," RFC 1811 (Informational), Internet Engineering Task Force, Jun. 1995. [Online]. Available: http://www.ietf.org/rfc/rfc1811.txt