International Conference on Recent Innovations in Engineering and Management
Dhananjay Mahadik Group of Institutions (BIMAT) Kolhapur, Maharashtra (ICRIEM-16)
23rd March 2016, www.conferenceworld.in ISBN: 978-81-932074-5-1

RANSOMWARE ANALYSIS: INTERNET OF THINGS (IOT) SECURITY ISSUES, CHALLENGES AND OPEN PROBLEMS INTHE CONTEXT OF WORLDWIDE SCENARIO OF SECURITY OF SYSTEMS AND MALWARE ATTACKS

Ms. Prachi Sharma[1], Mr. Shubham Zawar[2], Dr. Suryakant B Patil[3]

[1, 2,3]*Computer Science & Engineering,Sanjay Ghodawat Group of Institutions, Atigre, Kolhapur, MH, (India)*

ABSTRACT

India is the third highest Asian country to receive Ransomware attacks, adding that with the growth in "Internet of Things" (IoT) industry, the threat towards infections and new malware threats will only increase in upcoming years of IoT and Digital India [12]. An objective of this paper is to investigate the types of information that can be deduced from analysis of Ransomware attacks, where data can be analyzed and whether the information obtained can be used to aid Ransomware attacks especially in the IoT era. In the todays Internet world when we are going to witness the Digital India, Make in India, Start Ups, IoT in next couple of years; huge number of Online applications and services will be offered during the same; Ransomware kind of threats will be harmful to the data as well as the devices attached through the interface in the IoT [4]. The Post Offices as well as other Govt Offices will be converting into the online service provider hubs to the various E-Applications and E-Services

[3, 8]. These initiatives need to have large numbers of applications and software's to be installed and used [6, 10]. Here, due to the huge growing use of internet cyber-attacks are common to happen and thus safety is to be maintained. Recently one of the attacks is been come into existence known as Ransomware attack which targets at any system files. It enters as an application or software then spreads itself inside the data files thus encrypting the system and finally locking the system. It asks for a huge amount of cash for unlocking the device in the form of bitcoins else loose the valuable data. A Ransomware attack campaign based in India has caused millions of dollars of damages after infecting three banks, a pharmaceutical company and large number of regular users. This paper ensures the awareness of Ransomware attack, its analysis during the course of time from its origination, geographical attacking analysis and operating system based attacks. The analysis and results end up with the major achievement as the awareness and counter measures. Thus it will play a key role in safe use of Digital India, E-Governance, E-Commerce, IoT and so on [7].

Keywords: ***bitcoins, cyber-attack, Digital India, Internet of Things (IoT), online threat, Ransomware.***

I. INTRODUCTION

In IoT, Internet Era and in Digital India, the use of web applications and services is tremendously increased [1]. In recent years, personal use of computers and the internet has exploded and, along with this massive growth, cybercriminals have emerged to feed off this burgeoning market, targeting innocent users with a wide range of malware. The vast majority of these threats are aimed at directly or indirectly making money from the victims [13].

Today, Ransomware has emerged as one of the most troublesome malware categories of our time. Ransomware is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of Ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key. Ransomware typically propagates as a Trojan, whose payload is disguised as a seemingly legitimate file. There are two basic types of Ransomware in circulation

-The most common type today is crypto Ransomware, which aims to encrypt personal data and files.

-The other, known as locker Ransomware, is designed to lock the computer, preventing victims from using it.

In this paper, we will take a look at where and when the Ransomware attacks worked, not just from a geographical point of view but also from operating system viewpoint. We will also look at how these threats evolved, what factors are at play to make Ransomware the major problem that it is today, and where Ransomware is likely to surface next.

II. PROPOSED METHODOLOGY - EXPERIMENTATION AND RESULTS

The Fig 1 shows the month-by-month mix of binary-file-based locker Ransomware versus crypto Ransomware in the past 12 months. Our findings reveal that over the past 12 months, 64 percent of binary-based Ransomware families observed have been crypto Ransomware while locker Ransomware made up the remaining 36%.

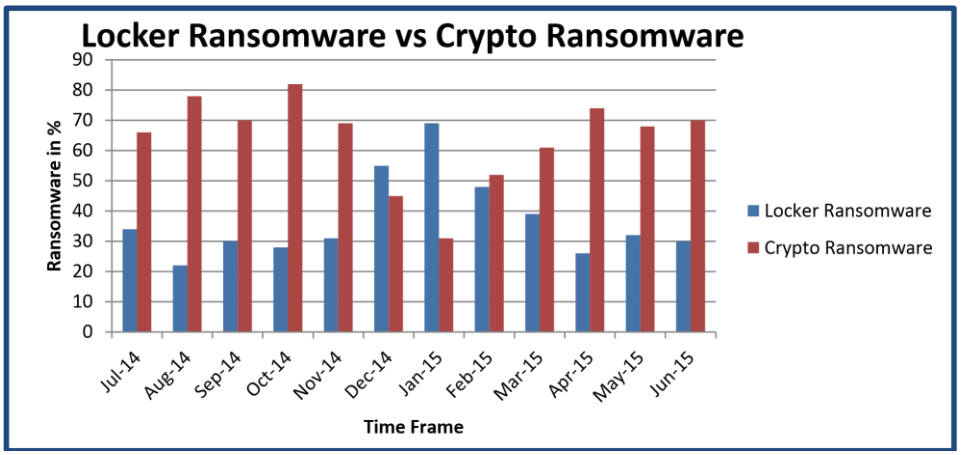

Figure 1: Analysis of Locker Ransomware Vs Crypto Ransomware 2014-2015.

Table 1 show quarter to quarter to analysis of the same; it reflects the dominance of binary based crypto Ransomware over binary-based locker Ransomware. This is in line with Symantec's findings that between 2013

and 2014 only as 2015 data yet not available, there was a 250 % rise in new crypto Ransomware considering the threat level.

CoinVault first came to the attention of Kaspersky Lab November 2014. The virus, which has targeted more than 20 countries, usually gains access to victims' machines via phishing emails or links to malicious websites and in an IoT such devices will get infected [5].

Table 1: Analysis of Locker Ransomware Vs Crypto Ransomware 2014-2015

Ransomware Type	Qtr1 Jul 14- Sep 14	Qtr2 Oct 14-Dec 14	Qtr3 Jan 15-Mar 15	Qtr4 Apr 15-Jun 15
Locker Ransomware	86	114	156	88
Crypto Ransomware	214	196	145	212

Fig 2 Cybercriminals behind Ransomware are targeting most populous OS in the hope of finding rich pickings. In spite IOS having less vulnerabilities for a loophole, is most secured System and Robust yet is been attacked the most and being exploited.

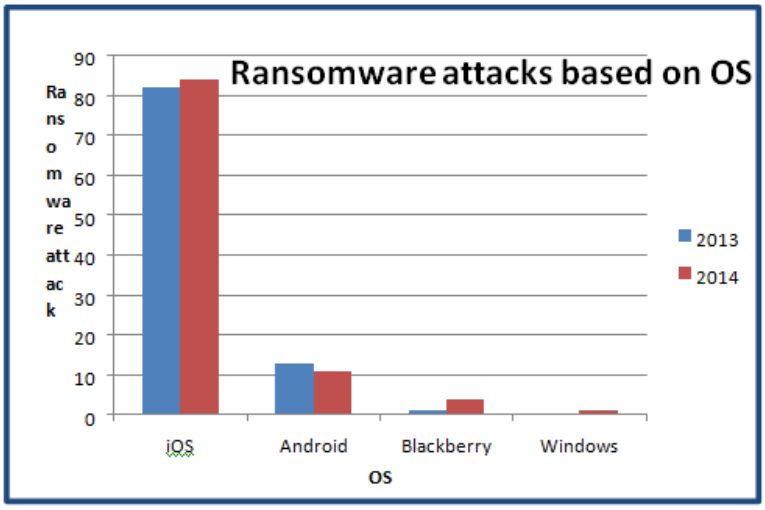

Figure 2: Yearly evolution of Ransomware Attacks based on OS

As shown in Fig 2 the summary indicates that 84% of mobile vulnerabilities related to Ransomware attacks to apple iOS in 2014, compared with 11% for android, 4% for BlackBerry and 1% for Nokia.

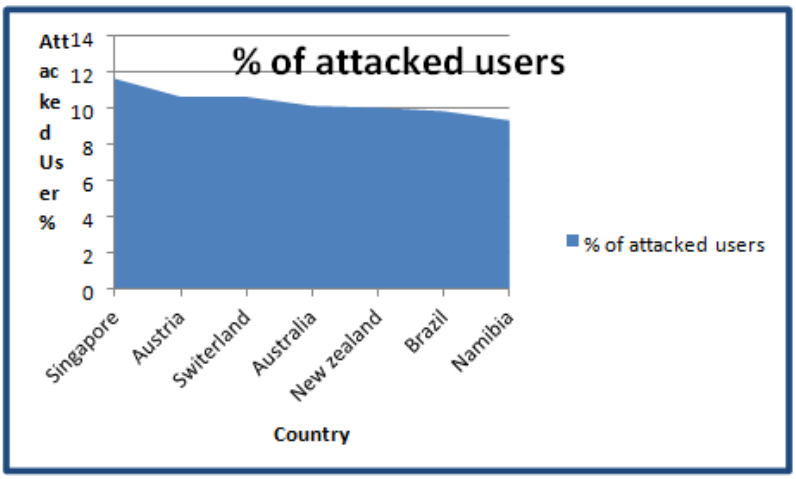

Figure 3: Percentage of attacked user's over the countries.

Fig 3 show that the cybercriminals behind Ransomware are for the most part targeting more developed countries in the hope of finding rich Ransomware. As a result, most of the top 7 countries impacted by Ransomware are members of the G20 organization, representing industrialized and developing economies that make up roughly 85 percent of the world's global domestic product (GDP).

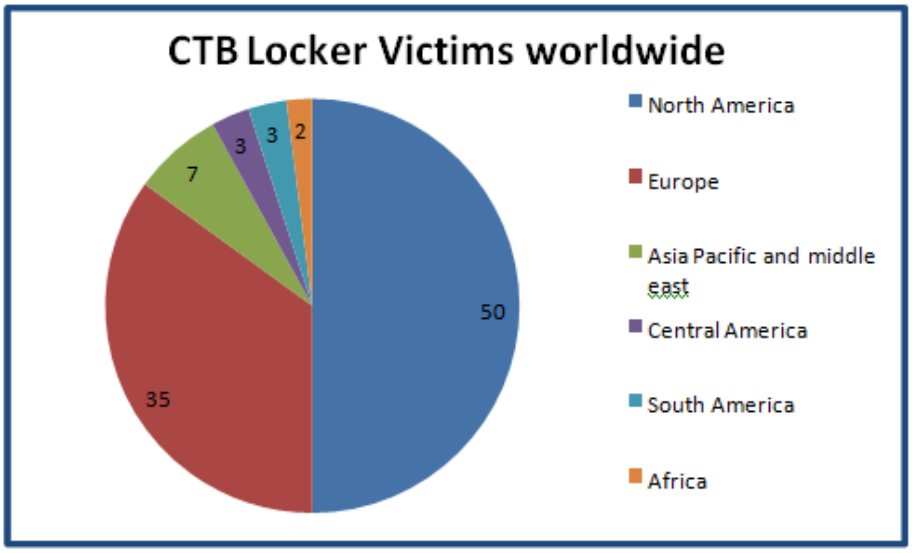

Figure 4: CTB Locker Victims worldwide

Campaigns using CTB-Locker started early in December 2014, but mass campaigns took off in January 2015. CTB-Locker has been found in English, Dutch, German, French, and Italian as shown in Fig 4. Language options extend to the attachments, making the phishing emails more authentic. Even the filenames have been localized. In spite of the malware's multilingualism, most CTB-Locker victims detected by McAfee Labs are located in North America.

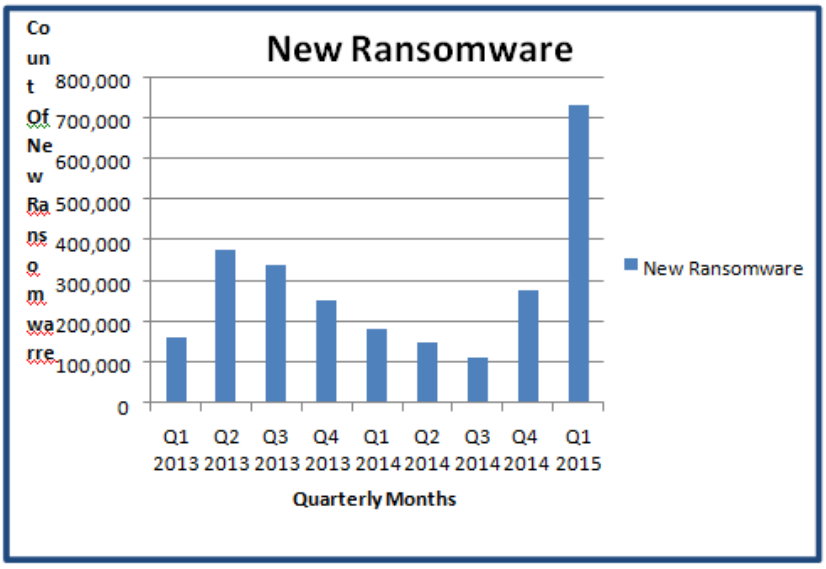

Figure 5: New Ransomware Discovered Quarterly

In the McAfee Labs Threats Report [5]: November 2014 it predicted nine major threats that would occur in 2015 as shown in Fig 5. Regarding Ransomware, it said this: "Ransomware will evolve its methods of propagation, encryption, and the targets it seeks." McAfee Labs has seen a 165% rise in Ransomware in Q1, especially with the family CTB-Locker, along with new versions of CryptoWall, TorrentLocker, and spikes of BandarChor. It is also seen that the new family Teslacrypt surface in the first quarter.

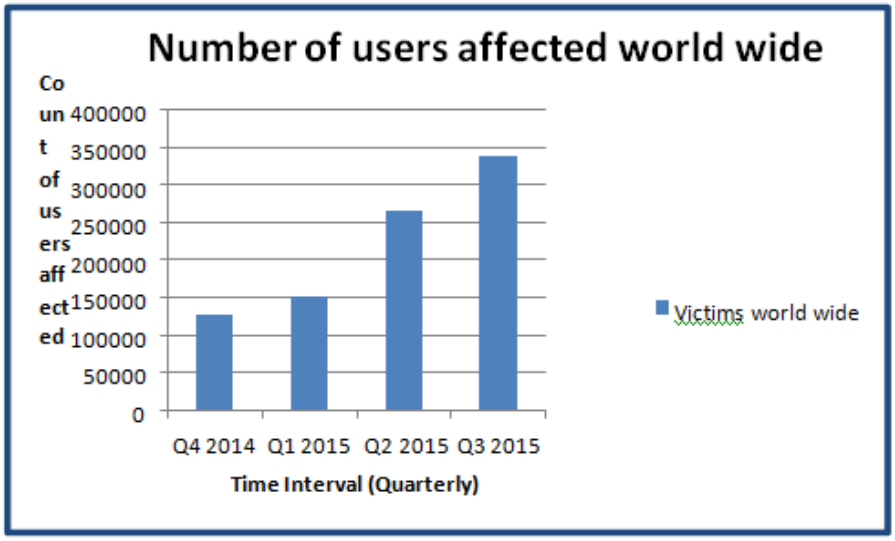

Figure 6: Number of users affected worldwide quarterly due to Ransomware.

The Fig 6 shows the rise in users with detected Trojan-Ransom within the last year. Overall in 2015, Trojan-Ransom was detected on 753,684computers. Ransomware is thus becoming more and more of a problem

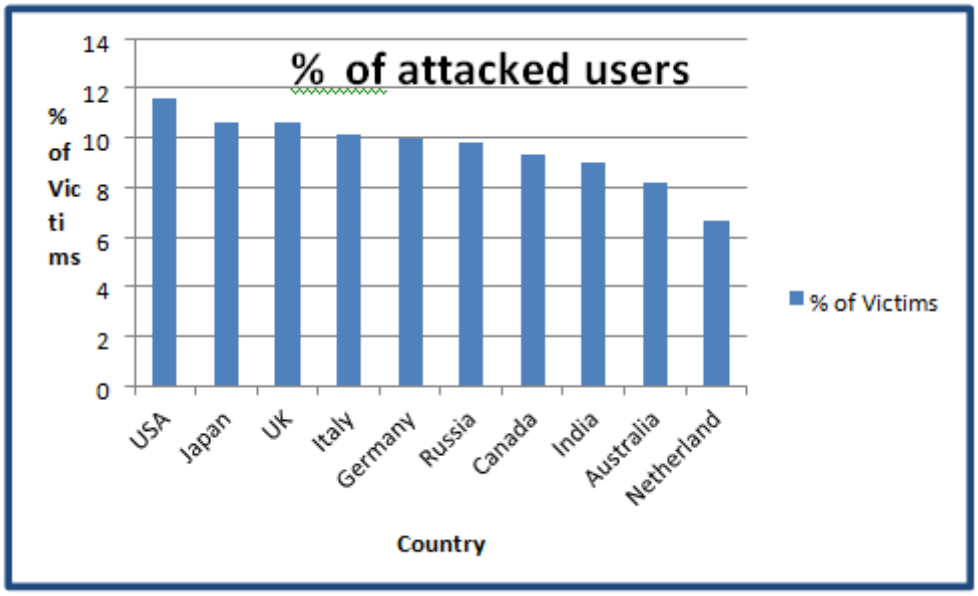

Figure 7: TOP 10 countries by percentage of attacked users

In Fig 7 the % victims in Top 10 countries are listed based on the Ransomware attacks in last one year. It reflects the way it spreading all over the world in short duration.

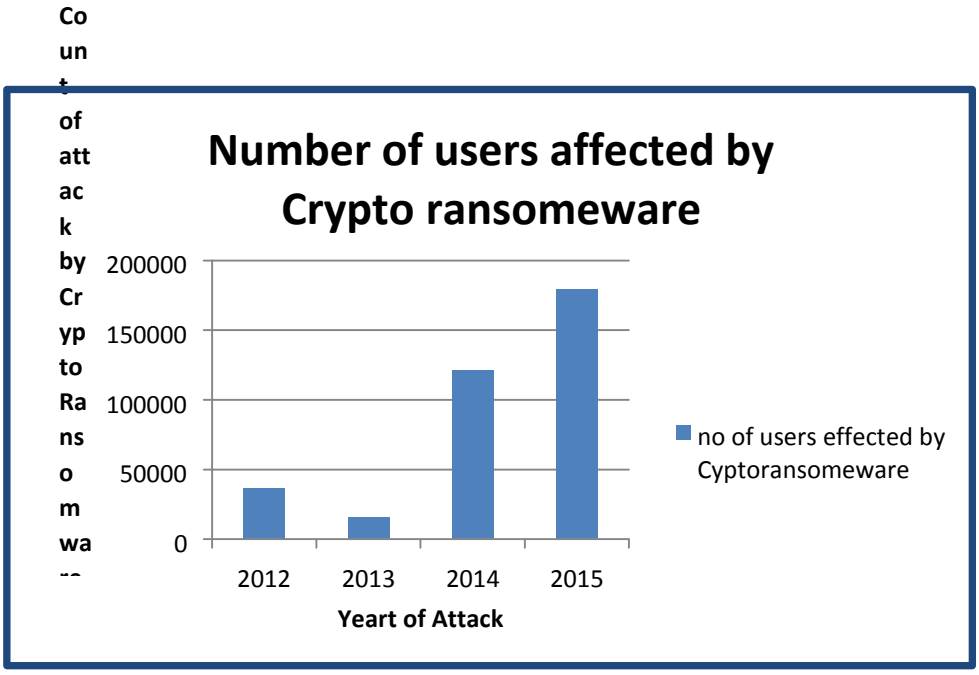

Figure 8: Number of Users affected by Crypto Ransomware

The statistics in the Fig 8 witnessing the rise in the Ransomware attacks in the last couple of years; the drastic hike in the count indicates the severances of the issue.

III. CONCLUSION

As per the analysis done in this paper, in 2015, there were 1,966,324 registered notifications about attempted malware infections that aimed to steal money via online access to bank accounts. Ransomware programs were detected on 753,684 computers of unique users; 179,209 computers were targeted by encryption Ransomware. In order to evaluate the popularity of financial malware among cybercriminals and the risk of user computers around the world being infected by banking Trojans, the preventive measures need to be taken immediately. In Singapore only 11.6% were targeted at least once by banking Trojans throughout the year. This reflects the popularity of financial threats in relation to all threats in the country. 5.4% of users attacked in Spain encountered a banking Trojan at least once in 2015. The figure for Italy was 5%; 5.1% in Britain; 3.8% in Germany; 2.9% in France; 3.2% in the US; and 2.5% in Japan. 2% of users attacked in Russia were targeted by banking Trojans.Sharing its security prediction in 2016, the US software security firm Symantec Corporation that produces software for security, storage, backup and availability said India receives Ransomware attacks with over 60,000 attacks per year or 170 malware attacks per day. The overall number of encryptor modifications in our Virus Collection to date is at least 11,000. Ten new encryptor families were created in 2015. In 2015, 179,209 unique users were attacked by encryptors. About 20% of those attacked were in the corporate sector. It is important to keep in mind that the real number of incidents is several times higher.

Considering the past as well future growth of the Internet based applications and ventures in India, especially the major scope for the same in the Digital India. In IoT the additional threat will be to the devices along with the

software and data as IoT has direct interface with several devices. Safe practices to protect against Ransomware by tightly monitoring intelligence feeds, to detect and stop most

Ransomware before it can execute. It also means that no Bitcoins will flow into criminals' pockets. Good policies and procedures includes Back up data, Perform ongoing user-awareness education, Block unwanted or unneeded programs and traffic, Keep system patches up to date, Employ antispam, Protect endpoints.

IV. ACKNOWLEDGEMENT

We express our gratitude towards the Hon. Director Dr. V. A. Raikar, Sanjay Ghodawat Group of Institutions (www.sginstitute.in) for his valuable guidance and support by providing the required infrastructure as well as the setup for the real time experimentation of this work.

REFERENCES

[1] M. M. Ahmadian; H. R. Shahriari; S. M. Ghaffarian; "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable Ransomware, Information Security and Cryptology (ISCISC), 2015 12th International Conference on Iranian Society of Cryptology Year: 2015, Pages: 79 - 84, DOI: 10.1109/ ISCISC.2015

[2] A. Sanatinia; G. Noubir, "OnionBots: Subverting Privacy Infrastructure for Cyber Attacks", 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2015, Pages: 69 - 80, DOI:
10.1109/DSN.2015.40

[3] S B Patil, Dr. D B Kulkarni, "Improving web performance through Hierarchical caching & content aliasing", The 7th International Conference on "Information Integration and Web-based Applications & Services", IIWAS2005, Volume 196, 19-21 September 2005, Austrian Computer Society, KUALA LUMPUR, MALAYSIA, SBN: 3-85403-196-3,
Pages: 987-998

[4] O. Flauzac;C. González;A. Hachani;F. Nolot;"SDN Based Architecture forIoTand Improvement of the Security"
Published in: Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference onDate of Conference:24-27 March 2015

[5] K. Fischer; J. Geßner;" Security architecture elements for IoT enabled automation networks" Normally-off computing for IoT systems Published in: 2015 International SoC Design Conference (ISOCC)

[6] S B Patil, PreetiPatil, "Improvement in the efficiency of web based search engines by increasing the page rank based on referring factors". In international Journal of Information Technology & Management Information System (IJITMIS), volume 5, Issue 1, January - April (2014), pp. 53-59. Journal Impact Factor (2014): 6.2217 Calculated by GISI

[7] Han, B.J., Choi, Y.H. and Bae, B.C. (2013) Generating Malware DNA to Classify the Similar Malwares. Journal of the Korea Institute of Information Security & Cryptology, 23, 679-694. http://dx.doi.org/10.13089/JKIISC.2013.23.4.679 .

[8] S B Patil, PreetiPatil, "Network Traffic Optimization for Performance Improvement in the Web Service Infrastructures
By Categorization Of The Web Contents With Size Reduction Approach". In International Journal of Advanced
Research in Engineering & Technology (IJARET), Volume 5, Issue 4, April (2014), pp. 198-204 Journal Impact Factor (2014): 7.8273 Calculated by GISI

[9] Tianda Yang; Yu Yang; Kai Qian; D. C. T. Lo; Ying Qian; Lixin Tao; "Automated Detection and Analysis for Android
Ransomware" IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015, Pages: 1338 - 1343, DOI: 10.1109/HPCC-CSS-ICESS.2015.39

[10] S B Patil, PreetiPatil, "Network architecture and design for optimized web page clustering with customized local proxy server to reduce user-perceived latency and network resource requirements in the world wide web". In International Journal of Computer Engineering & Technology (IJCET), Volume 5, Issue 4, April (2014), pp. 210-217. Journal Impact Factor (2014): 8.5328

[11] S B Patil, PreetiPatil, "Architecture for vigorous GSM handovers in Mobile cellular networks by Jettisoning Hidden Terminal Problem", International Journal of Computer Engineering & Applications, ISSN 23221-3469, Volume VI, Issue III, June 2014, Pages 121-131. (Journal Impact Factor: 2.849)

[12] Kevin Savage, Peter Coogan, Hon Lau, " The evolution of Ransomware", http://www.symantec.com

[13] S B Patil, Sachin Chavan, PreetiPatil; "High Quality Design To Enhance and Improve Performance Of Large Scale Web Applications", International Journal of Computer Engineering &Technology (IJCET), ISSN 0976 – 6375, Volume 3, Issue 1, January-June 2012, Pages: 266-272.(Journal Impact Factor: 1.0425)