BitCryptRansomware: A New Challenge in the Upcoming Era of Cashless Economy

Swaleha Zubair, PhD
Assistant professor
Computer Science Department Aligarh Muslim University
Aligarh, India

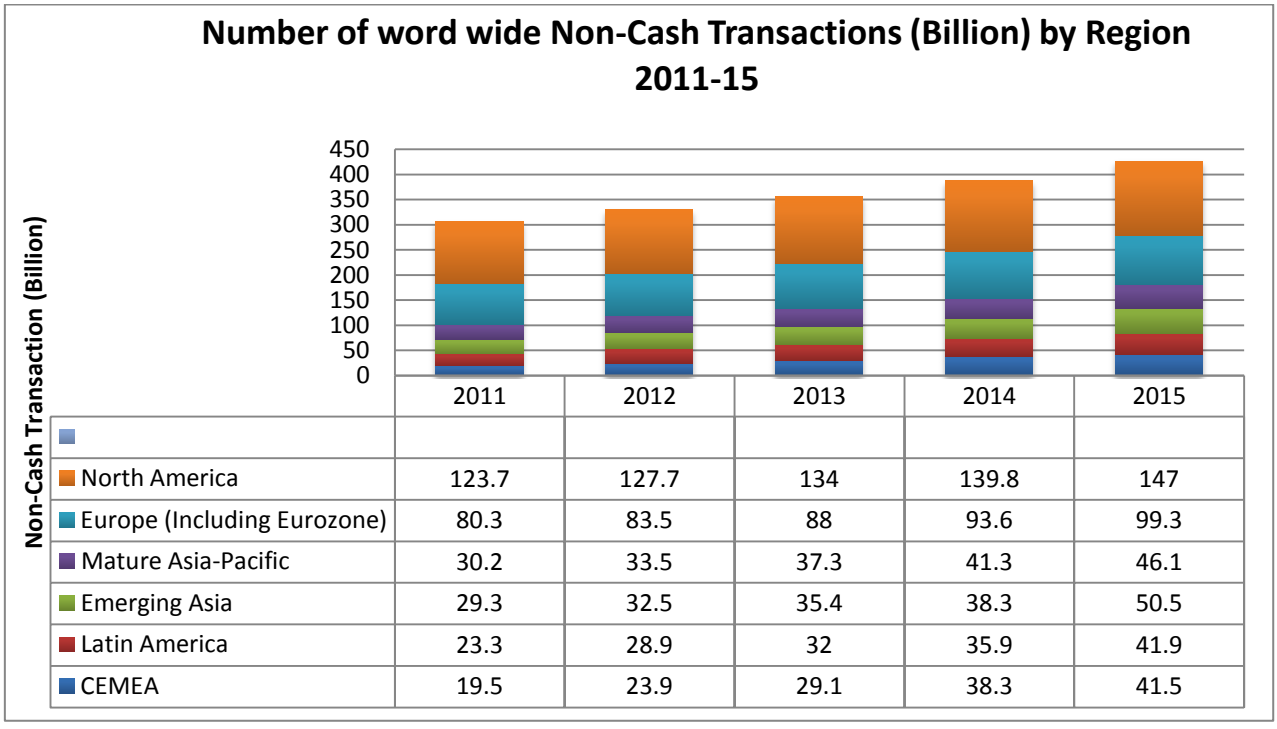
Mohd Saqib
Computer Science Department Aligarh Muslim University
Aligarh, India

ABSTRACT
The present study discusses impact of BitcryptRansomware in the upcoming era of cashless economy. The wide usage of Bitcoins and e-transactions makes it mandatory to have knowledge about anticipated online threats which one can come across upon wielding of proposed cashless economy. Bitcoin can influence upon both legal as well as illegal dark web based business. BitCryptRansomware can target lots of data and eventually economy. In fact cashless economy is prone to a range of malpractices that may pose a great deal of economy threats. Besides discussing various modes in effective hacking, the present paper also highlights measures and strategies to counter such attacks.

General Terms
BitCryptRansomeware, Viruses, Bitcoin, Hacking,Indian Economy Cashless economy .

Keywords
BitcryptRansomware, Bitcoins, Dark Web, Hacking, Indian Economy, Cashless economy.

1. INTRODUCTION
November 8, 2016, the day will be remembered in the Indian economy as a unique and revolutionary demonetization scoop. The move was launched by Government of India in anticipatory consequence of certain observations that include the fact that 86% of the value of Indian's currency withdrawal and cashless payments increased by 22% in 2016 compared to 2015 [1]. Over all demonetization can be considered as progressive shift to a cashless economy with a greater focus on electronic transactions. Rising use of credit/debit cards, net banking and other online payment mechanisms will be another positive effect of demonetization, as these would not only lower transaction costs but some of these could help to earn a token fee income as well[1]. With the implementation of demonetization, 86% of India's currency was nullified that aimed to wash the stock of 'black market's cash supply' [2]. Money transfers using mobile banking and immediate payment system (IMPS) showed the highest increase in 2016. According to India Spend analysis of Reserve Bank of India (RBI) data, mobile banking transactions grew 175%, while money transacted using mobile banking grew 369%.[1]



	2011	2012	2013	2014	2015
North America	123.7	127.7	134	139.8	147
Europe (Including Eurozone)	80.3	83.5	88	93.6	99.3
Mature Asia-Pacific	30.2	33.5	37.3	41.3	46.1
Emerging Asia	29.3	32.5	35.4	38.3	50.5
Latin America	23.3	28.9	32	35.9	41.9
CEMEA	19.5	23.9	29.1	38.3	41.5

Figure 1 (Source: Capgemini Financial Service Analysis, 2016; ECB Statistics Data Warehouse, 2014 figures released Oct 2015; Country's Central Bank Annual Reports, 2014)

The top e-commercial companies (Flipkart, Snapdeal, Shopclues, CCAvenues, Ola and Oyo Rooms) are in favor of making maximum transactions through digital payments[2]. Payments companies Paytm, FreechargeMobiKwik, PayU *etc*; are dealing with gigantic demands which have increased upto many folds and still growing. Most of the service providing companies are trying to set up their own payment system or integrating it with existing global online wallets or payment gateways. According to market experts, the growth of digital payments and wallets is the first phase of the impact and will give big boost to lending and credit deals as the digital records of merchandize will expand and create more demand in the second phase [2].

Global non-cash transaction volumes are estimated to have grown at a rate of 10.1% during 2015 to reach a total of 426.3 billion. This growth will likely have been led by emerging Asia (31.9%), CEMEA(15.7%), and mature APAC (11.6%)[3]. (Figure 1)

The total share of non-cash transactions of developing economies increased by 2.0% in 2014, driven mainly by the growth in economic negotiations recorded by emerging Asian countries such as India. At the same time, the share of non-cash transaction volumes in North America and Europe declined by 1.6 percentage points 0.6 percentage points respectively. During the past 10 years, the percentage share of fully developed regions versus developing regions has dropped from 87% to 71% [3] (Figure 2).

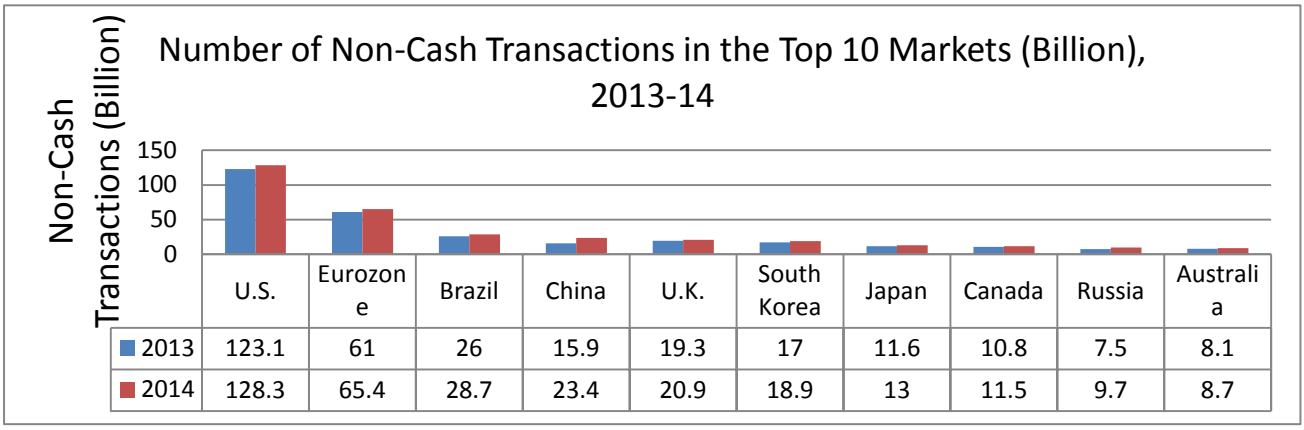


Figure 2 (Source: Capgemini Financial Services Analysis, 2016; European Central Bank (ECB) Statistical Data Warehouse, 2014 figures released Oct 2015; Bank of International Settlement RedBook, 2014 figure Dec 2015; Country's Central Bank Annual Reports, 2014)

The above mentioned statistics explicitly suggests that new coming era is all about cashless transactions. Money has shaped the modern economy across the world. In the primitive days transactions was executed through usage of grain and cattle and even salt as currency to using metal tokens (coins) or paper bills. However, paper bill note based economy prevailed world over since the Chinese introduced it during the Tang dynasty. The modern man has grown with contented usage of paper currency and no one can deny that it has had boasted its usefulness. While entering to next age era in which Bits-Currency (Bitcoin, Monero, Ethereumetc) is going to replace paper note bill], Bitcoin, will be the new form of the currency [4, 5].The cashless economy can boast of complete anonymity and do not require storage issues associated with physical object like gold and all. Transactions are cheap to execute, and, are quickly and easily transferred around the world. Currently, it's the only currency accessible on the darkweb. Due to its anonymity, some people have been using Bitcoin on the darkweb to execute illegal transactions like drug markets, paedophiles and sex traffickers [5-7]. The recent "Wannacry" computer ask for ransom payment in Bitcoin[5].

Another form of Ransomware, BitCryptRansomware works on the Wannacry mode. However, dupe double make it more dangerous as first it make zero e-wallet of a person followed by demand for ransom[8][9]. However, one can escape from such kind of dangerous virus using preventive techniques [10–12]. Post demonetization there is a rapid increase in digital transfer of funds, online transactions, storing money in form of virtual currency, thereby rising concern for both customers and bank. The technology is still evolving and prone to too many undiscovered attacks. Further, the expanding industry of digital payment and wallet is attracting the interest of cybercriminals, who are ready to take advantage of the technology. Attackers can exploit technical or developmental issues, buggy software, un-patched applications, zero-day vulnerabilities *etc*.

BitCryptRansomware shares some working module with Cryptorbit virus, PoshCoder virus and many other threats. It performs same task as Cryptolockerand encrypt all files [13–15]. It is more fatal as compared to Cryptolocker or any other virus from Ransomware family because it first implies

BitCoin wallet followed by demand for ransom [16]. It extorts extension of the files and look like [file].jpg.bitcrypt, [file].xls.bitcrypt, etc[16].

In seems in near future all transactions and banking will be executed through e-currency especially via BitCoin. There are so many advantages associated with BitCoin like User Anonymity, No Third-party Interruptions, No Tax, *etc*.[17]

Apart from such advantages, BitCoin has some disadvantages as well such as:

i. Low awareness-In spite of the fact that world is moving toward cashless economy, Crypto Currency is not much in practical use when compared to paper currency [3, 18]. The dark web totally depends on crypto currencies just because of its anonymity but a large part of legal business affairs are still covered by paper currencies due to low awareness.

ii. Semi-Developed Environment-Bitcoin software is still in beta with many incomplete features in its active development.

Most Bitcoin businesses are new and donot offer insurance [19].

iii. In Secured transaction mode-BitCryptRansomware was quite active in Aug, 2014 and victimized many organizations. If the Hacker Knows a Specific Bitcoin Miner or a Company involved in Mining, he could just infect involved systems with a Malware that would search for Private keys Stored on the system drive or hack their pool account and change the payout addresses as well [20].

Besides above mentioned disadvantages associated with Bitcoins, the hackers can use following techniques to access others computer systems:

i. Exploit Kits- Exploit kits, is a collection of files, which exploits (Open) file manager of the victimized system. If victim visits insecure websites some of them start downloading a malicious kit which executes and infect the system and hold files for ransom[15, 21].

ii. Malicious Email Attachments- Such kind of e-mail attaches a malicious files which looking as it is receive from trustable resource like social media or IT. The recipient opens the attachment. Once the file is opened, the Ransomware payload is unintentionally downloaded, the system is infected [15].

iii. Malicious Email Links- Similar to malicious email attachments, malicious email links are URLs in the body of the email. When victim clicked, these URLs download malicious files over the web, the system is infected and system open the door for Ransomware[15][21].

2. METHODOLOGY

The study is based on secondary sources of data/ information. Different books, journals, newspapers and relevant websites have been consulted in order to make it effective. The study attempts to examine various prevention techniques against hacking the computer system. It is very critical both for users and digital payment solution providers to maintain a high level security posture to safeguard themselves from the menace of cyber criminals.

3. PREVENTION TECHNIQUES

Users are always the at the receiving end and weakest link in the security architecture. In general, hacking is not merely a technical skill; however it is an art of tricking human beings. Security is a shared responsibility of users of digital platforms and not a sole responsibility of the creators and protectors of the platform. Therefore, it is essential for users of the technology to watch their online behavior and rigorously follow certain Do's and Don'ts to protect themselves from hackers and cyber criminals.

In spite of tremendous advancement in hacking techniques, the active users can protect themselves from Ransomware by adopting some preventive regular practices.

Use of good antivirus software and firewalls is the foremost step towards defending oneself against cyber criminals. Second in line, yet a very significant move would be to befriend people online very carefully. Third is taking back up files regularly is the best prevention we have. If we have back up files, one can simple format the system after getting infected by such viruses. It is also desirable to be careful about exchanging and opening emails and should never click on links or download attachments that are not expected and should avoid browsing suspicious websites. If one receives a Ransomware notice, simply disconnect the machine from Internet.

Furthermore, creating separate email accounts for different purposes could prove to be helpful. Lastly, referring to the online payment, it is important to note that, storing card details on websites could be dangerous. Therefore, taking a few extra seconds to feed in card details, when paying online, is a small price to pay for the entire security process.

The government should lay down basic security standards for operative devices, non-compliant businesses should not be allowed to operate. Many companies in India do not report breaches. This practice is to be done away with timely reporting and should be made mandatory. As the government initiates the creation of digital highway and smart platforms, hackers will also take advantage of the same to break the walls. Online marketplaces will continue to be the prime target of cyber criminals. Hence, embedding security measures at every step is the need of the hour.

4. CONCLUSION

The proposed study presents an analytical report on how Bit Crypt ransom ware could be a challenge for upcoming era of cashless economy. It is fact that not only India, however other countries too are moving very fast toward cashless economy. e-Commerce prefers e-money in all transactions. Not only e-commerce, illegal tasks on the dark web have only one option for the money transaction, a Crypto Currencies i.e. Bit Coin. Nevertheless, cashless economy has to come across with so many challenges like Bit Crypt Ransom ware. Just a mistake on the web end and one will lose whole e-money balance. After hacking money from e-wallet, hacker can demand for ransom too. There are some preventive measures for every hacking technique. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration both at individuals and government level. There is so much scope where one can ensure a safe, secure and trustworthy computing environment.

5. FUTURE SCOPE

While cashless economy is the way ahead and the country is already moving towards it, security continues to be a major concern in the digital payment ecosystem. An exponential growth in online transactions post demonetization has attracted interest of cyber criminals, who can potentially target online payment platforms. Given the fact that more people will now inevitably opt for online payment, it is very critical both for users and digital payment solution providers to maintain a high level security posture to safeguard themselves from the menace of cyber criminals.

6. REFERENCES

[1] "2016_ The year cashless payments trended upwards Business Standard News."http://www.business-standard.com/article/economy-policy/post-demonetisation-digital-payments-are-down-15-116122700098_1.html .

[2] "Demonetization and its impact on Indian Economy."http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=2253:demonetization-and-its-impact-on-indian-economy&Itemid=137.

[3] W. Payments, "World Payments Report," 2016.

[4] "Bitcoin & Other Cryptocurrencies Shaping Future Economy, Capitalism Morphing."

https://cointelegraph.com/news/bitcoin-other-cryptocurrencies-shaping-future-economy-capitalism-morphing .

[5] "Bitcoin ."https://bitcoin.org/en/how-it-works .

[6] "3 ways to get busted on the Dark Web – Naked Security."https://nakedsecurity.sophos.com/2015/09/04/3-ways-to-get-busted-on-the-dark-web/ .

[7] K. Finklea, "Dark Web," 2017.

[8] "New BitCrypt ransomware variant distributed by bitcoin stealing malware Network World." http://www.networkworld.com/article/2175508/byod/new-bitcrypt-ransomware-variant-distributed-by-bitcoin-stealing-malware.html .

[9] "Web-hosting firm agrees to pay over $1 million to ransomware extortionists." https://www.welivesecurity.com/2017/06/20/web-hosting-firm-agrees-pay-1-million-ransomware-extortionists/ .

[10] "How to Remove BitCrypt Rasomware, Cleanup Virus Completely." https://malwarefixes.com/remove-bitcrypt-decrypt-infected-files/ .

[11] "BitCrypt Ransomware Removal Report."https://www.enigmasoftware.com/bitcryptransomware-removal/ .

[12] "Removal of Bitcrypt virus and recovery of encrypted files - Help, my PC is infected! - Emsisoft Support Forums."https://support.emsisoft.com/topic/17529-removal-of-bitcrypt-virus-and-recovery-of-encrypted-files/?do=email&comment=132887

[13] H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," 2016.

[14] P. B. Pathak, "A Dangerous Trend of Cybercrime : Ransomware Growing Challenge," vol. 5, no. 2, 2016.

[15] "RANSOMWARE," p. 2016, 2016.

[16] "Remove BitCrypt virus." https://malwarefixes.com/remove-bitcrypt-decrypt-infected-files/.

[17] "What are the advantages of paying with Bitcoin_ _ Investopedia." http://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp.

[18] "Demonetisation :Impacton the Economy Demonetisation : Impact on the Economy," no. 182, 2016.

[19] R. A. Glantz, "WHAT IS BITCOIN ? HOW DOES BITCOIN WORK ?," pp. 1–16, 2014.

[20] "How to hack bitcoin_ - wallet hacking, private key hack &exploits". https://www.hacker9.com/how-to-hack-bitcoin-system-wallet-password.html.

[21] R. Sushmitha, D. Venkatasubramanian, and R. S. Sundar, "HACKING METHODS , TECHNIQUES AND THEIR PREVENTION," vol. 2, no. 2, pp. 183–189, 2014.