Bitcoin-Security Issues

Preeti Sharma[#1] Gulshan Kumar[*2]
[#] *Deptt of Computet Science,Punjab University*
Ferozepur City,India
preetishrm09@gmail.com

[*] *Deptt of Computet Science,Punjab Technical University*
Ferozepur, Punjab (India)
gulshanahuja@gmail.com

***Abstract*—Bitcoin is a free open source peer-to-peer electronic cash system. It is completely distributed, without any control of a central server or trusted parties. Bitcoin has the prospective to transform online payment systems in a way that welfare consumers and businesses. Instead of using an intermediary such as PayPal or submitting credit card information to a third party for verification-both of which often include transaction fees and other restrictions-Bitcoin allows individuals to pay each other directly for goods or services.**
The characteristics that make Bitcoin so ground-breaking have also made it a target for regulators, who dread that the cryptocurrency will aid money laundering, tax evasion and other crimes. But, unlike cash, Bitcoin transactions are logged in an online journal.
Bitcoin closely look like traditional cash than other forms of e-spending, and this ability to marry cash-like properties with prompt electronic payments is highly advertised by Bitcoin buffs as an advantage to various actors, traders involved. Bitcoin combines the best of both worlds from a feature viewpoint, from a security perspective this union of cash and computers could barely be inferior. A currency which is vulnerable to large-scale theft can never be widely accepted for everyday acquisitions, and thus it follows that if Bitcoin is to become a substitute to current payment systems, we must find some way to make it secure for the average user. This paper highlights various security issues and attacks on Bitcoin. Finally, it provides some research directions in the area of Bitcoin.

I. INTRODUCTION

Bitcoin is an open-source digital currency, is freely available and may be redistributed and modified [1]. Bitcoin network is free and we can use it to boost the transaction processing. A transaction frequently has either a single input from a previous larger transaction or multiple inputs from previous smaller transactions. Also, a transaction frequently has two outputs: one sending payment and one returning change [10]. A Bitcoin transaction drops between these two limits

- A full transaction record of every Bitcoin.
- Every Bitcoin user's encrypted identity is maintained on the communal register.

Traditional electronic payment systems have periodic security problems. A high incidence of security problems on a system trying to establish itself and advance customer confidence could be more harmful. Bitcoin exchanges and wallet services have fought with security [2]. Criminals are also attracted to the currency because it's almost impossible to trace to an individual. So it's easy to anonymously steal and spend Bitcoin. Thousands of Bitcoin investors found that out the hard way last month when millions of dollars disappeared in one fell leap after a virtual exchange missing [3]. The risk can be huge. But then again, with great risk comes countless prospects. There are people making great sums of money, and there are people with significant losses as well. And unfortunately, because the currency is not controlled by any country or central bank, consumers and businesses stand to lose a lot of money [3] [4].

All information concerning the Bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent and predictable.

Bitcoin's potential to disrupt the global financial sector, which profits by imposing high transaction fees in a banking system closed to outside innovation. ATMs charge several dollars to extract cash; credit cards, PayPal, and other payment processors assess vendors or users about 3 percent; and money transmitters such as Western Union collect nearly 10 percent - often from low-wage immigrants who have no other way of sending money to their home countries. By comparison, a typical Bitcoin transfer involves a fee of less than 1 percent.

II PROCEDURE

As we discussed what Bitcoin is a distributed peer to-peer payments network and a virtual currency that basically functions as online cash. Transactions are tested, and double-spending is prevented, through the adroit use of public-key cryptography [2]. Public-key cryptography entails that each user be given two keys, one public key that can be shared with the world and one private key that is kept secret like a password. When A decides to transfer Bitcoins to B, he creates a message, called a transaction, which contains B's public key, and he signs it with her private key. By looking at A's public key, anyone can confirm that the transaction was certainly signed with her private key, that it is an reliable exchange, and that B is the new proprietor of the assets [3]. The transaction and thus the transference of possession of the Bitcoins is recorded, time-stamped, and exhibited in one block of the block chain. Public-key cryptography guarantees

that all computers in the network have a continuously modernized and verified record of all transactions within the Bitcoin network, which averts double-spending and scam. As we have previously seen, because Bitcoin is a peer-to-peer network, there is no vital authority charged with either creating currency units or verifying transactions. This network rest on on users who provide their computing control to do the logging and reconciling of transactions. These users are called miners because they are pleased for their work with newly created Bitcoins.

The Bitcoin protocol requires that each new equation is incrementally harder to solve than the preceding one, limiting the rate at which Bitcoins can be added. Currently, there are 12.66 million units in circulation. By the program's design, there can be no more than 21 million Bitcoins - a maximum that's projected to be reached in the year 2140.

Users can also acquire Bitcoins by accepting the virtual currency as payment, or by buying Bitcoins with fiat currency on an exchange. Once users open an account, the Bitcoin protocol generates a unique address and a public and private encryption key to verify transactions.

To exchange Bitcoins, users enter the recipient's coded address and the amount to transfer into an electronic message, and then authorize it with their private key. The Bitcoin protocol does the rest. Every transaction is recorded, time-stamped, and displayed in a public ledger. As Bitcoins move from account to account, the verified transactions form an identifiable chain on this ledger that anyone can view over the Web.

Bitcoins are created, or mined, as thousands of dispersed. Computers solve intricate math problems that prove the transactions in the block chain [6]. As one commentator has put it, the actual mining of Bitcoins is by a purely mathematical process. A useful similarity is with the search for prime numbers, it used to be equally easy to find the small on. But as they were found it got harder to find the larger ones. Today researchers use progressive high-performance computers to find them.

For Bitcoins the exploration is not really for prime numbers but to find a sequence of data that produces a specific pattern when the Bitcoin hash algorithm is applied to the data. When a match happens the miner gets an abundance of Bitcoin. The scope of the abundance reduces as Bitcoins around the world are mined. The trouble of the search is too enlarged so that it becomes computationally more difficult to find a match [2]. These two effects associate to lessen over time the rate at which Bitcoins are produced and impressionist the production rate of a commodity like gold. So, the protocol was designed so that each miner contributes a computer's processing power toward maintaining the infrastructure needed to sustenance and validate the currency network [5]. Miners are given newly created Bitcoins for subsidising their processing power toward upholding the network and verifying transactions in the block chain. And as more processing power is dedicated to mining, the protocol will increase the difficulty of the math problem, ensuring that Bitcoins are continuously mined at an expectable and inadequate rate. This process of mining Bitcoins will not continue forever. Bitcoin was designed to impressionist the removal of gold or other precious metals from the earth—only a limited, known number of Bitcoins can ever be mined. The arbitrary number chosen to be the cap is 21 million Bitcoins. Miners are projected to thoroughly yield the last Satoshi, or 0.00000001 of a Bitcoin, in the year 2140. If the total mining power scales to a high enough level, the difficulty in mining Bitcoins will have increased so much that procuring this last Satoshi will be quite a challenging digital undertaking. Once the last Satoshi has been mined, miners that contribute their processing power toward verifying transactions will be rewarded through transaction fees rather than mined Bitcoins. This ensures that miners still have an incentive to keep the network running after the last Bitcoin is mined.

III BITCOIN'S LAPSE AS A CURRENCY

This segment illustrate the scrutinization of ways in which Bitcoin judge to alter to the conventional properties of a currency. An effective currency typically functions as a mean of exchange, a unit of account, and a salt away of value [9]. While it is hard to level the size of the merchant network that take Bitcoin, many proof suggest that Bitcoin has complete important inroads as an average of exchange. Nevertheless, Bitcoin does not seem to have known itself as a division of explanation or a reserve up of value. Bitcoin levies great menaces on its proprietors, since it has needless variability and fails to show linking with the actions of other currencies. For decision purposes, most widely traded stocks have volatilities in the range of 20% to 30%, and even very hazardous stocks rarely show instability as high as 100% [2]. One have to close that investment Bitcoin yet for a short period is quite unsafe, which is not in pact with a currency the theatre as a store of value and which really undermines the aptitude of money to meaning as a unit of account. We learning the society of Bitcoin compared to the other currencies and to gold. In the London gold charge and each currency's swap rate against the U.S. dollar, by means of day after day data from July 2010 up to the present. As shown, the three European currencies are likely to display strong helpful connection, with the Euro having 0.60 connections with the Swiss Franc and 0.65 relationships with the British Pound, and the Pound and Franc having 0.42 correlations [3]. The Yen's swap over rate is also certainly linked with those of the other currencies, though at a rather summary level [9]. Bitcoin remains a target of doubt and scorn. Its enigmatic origins, mysterious protocol, anonymous users, and libertarian advocates have shocked governments around the world. And its ability to ease basically unnoticeable transactions in illicit goods means law enforcement views it as little more than a tool for criminals. The anonymity offered by these payment systems attracts criminals who now can easily change, hide, and launder illicit profits. Bitcoin may be useful
for certain types of transactions, especially illegal ones. But Bitcoin's defenders argue that the experiment has proved that a currency can come into existence and function without any government role, so designed as to make inflation impossible and bank transfer fees unnecessary. These features are supposed to make Bitcoins irresistible for consumers. In the face of such widespread suspicion,

Bitcoin's backers have struggled to gain the government's trust. Without that sanction, transactions using virtual currency may be relegated to technology enthusiasts operating at the margins of the economy.

But gaining legitimacy involves more than simply convincing regulators of Bitcoin's benefits. On one side were entrepreneurs and venture capitalists eager to embrace innovative technologies. On the other were government agencies prone to deliberation and caution, institutions leery, for the most part, of rapid technological change.

IV. OBSTACLES FOR BITCOIN

The digital currency stands alone from any central bank, administration or other type of business to guarantee its value [5]. Bitcoin exchanges take place directly between the buyer and seller - meaning no banks are involved to facilitate Bitcoin payments. Though, confidence in Bitcoin has also been tested. The lack of regulation around it, and the statistic that transactions using Bitcoin are essentially unidentified [6] [7]. It has made governments and retailers alike worried about the use of the currency - especially for black market activities. The bank keeps saying "Bitcoin is an electronic money, we saw it on internet. The internet is never wrong." (or something like that) while we have been citing parts of the laws regarding electronic money and how they have a fixed value against a fiat currency, and are issued by a central authority and can be exchanged back for fiat at anytime (that's what the law says).

This time, the court was not able to find a solution for this, so it declared the issue shall be reviewed by a regular court (we were using the court for emergency matters, as not having a bank account is having an enormous negative impact on our business in Europe) starting September 13th .

For Bitcoin to turn out to be extra than a inquisitive and found itself as a bona fide money, it's on a daily basis worth will need to become added even so that it can constantly supply as a stock up of value and as a unit of version in profitable markets. The life-threatening variability is more consistent with the enactment of an irregular investment than a currency. Also, Bitcoin's authority as a currency should also reel on its addition into the network of global payments and risk management dealings [9].

Data endorse that no efficient method exists to be cautious Bitcoin beside the value of added currencies, and the lack of any change, onward, or extra copied markets for Bitcoin worsens this anxiety. Bitcoin appears to accept by being cut off from the banking and expense systems of the U.S. and further countries. The mainstream exchanges are detained and transferred from side to side bank accounts, which in twist are limited by covers of instruction, put down insurance and global treaties. With no right of entry to this transportation, Bitcoin would appear weak to stealing, deceit and duplicity by expert computer hackers [9]. On the other hand, enthusiasts of Bitcoin might argue that Bitcoin evades the well-known defects in standard financial security systems, which have generate outbreak of identity theft and related problems for ordinary customers of mainstream 10 businesses.

Finally, Bitcoin face a structural monetary trouble related to the total border of 21 Million units that can still be issued, with no growth feasible of the Bitcoin bring possible after the year 2140. If Bitcoin becomes madly doing well and displaces ruler fiat currencies, it would narrate a deflationary power on the market since the money deliver would not rise in performance with economic increase. These circumstances would require the majority employees to believe pay cuts every time, for example, likely most important to political protests against the currency comparable to those qualified in the U.S. during the Populist pressure group at the end of the 19th century. One can visualize a recovery of William Jennings Bryan's 1896 Cross of Gold words in the after that century, modernized with innovative rhetoric about the monetary autocracy of an uber-currency with a hard send. For Bitcoin to become inquisitiveness and establish itself as a legal currency, its periodic value will have to become more firm so that it can certainly serve as a cache value [9].

The technological ingenuity of the scheme, of course. And people have misinterpreted the run-up in price as a sign of success rather than failure. But more fundamentally, Bitcoin unites futuristic left-wing Internet anarchism—the fantasy that the Web can provide the conditions for a government less society—with the cave-dwelling right-wing libertarianism of gold bugs who think a stable money supply can be established without government involvement. It is proof for both that government is not needed for much, or at all.

In addition to Bitcoin legitimacy as a currency should also joint on its integration into the network of risk management transactions and international payments. However it is not allotted by an autonomous government, Bitcoin tells jeopardy to any business that accepts it for transactions, just like any other currency. All major companies that deal in more than one currency, such as Corporations, attempt to verge themselves against risks related to changes in those currencies' values. Most currencies are held and moved through bank accounts, which in turn are protected by sheets of guideline and global pacts, deposit insurance [9].

Deprived of this admittance to this substructure, Bitcoin would seem susceptible to scam, stealing, and sedition by expert computer hackers.

Some major barriers for Bitcoin are as follows:

- No guard or assurances on transactions.
- Unalterable transactions, even on incorrect ones.
- Vague guideline.
- Perils of government obstruction
- Numerous governments issuing Bitcoin cautions.
- Originally currency that doesn't have an independent entity behind it

V. SECURITY CHALLENGES TO BITCOIN

Bitcoin is divided into two camps. People who comprehend the currency well tend to be keen promoters. Those who are perilous of Bitcoin tend not to understand the currency very well and, as a consequence, their

disapprovals tend to be mistaken, artificial, or pure wrong. Bitcoin does have some real weaknesses [7].

Bitcoins are also not earned solely through the efforts of another. Bitcoins are mined using computing power, often times within pools, but not solely through the efforts of others. Each miner that donates computer power to a pool is reward only in proportion to the amount computer power contributed to the pool [12].The absence of well-informed detractors has shaped resonance chamber effect that we concern may produce a fizz. Outdated financial products have strong consumer protections [8]. If someone makes a fraudulent transaction with your credit card then there are laws in place to limit consumer losses. Bitcoin has no such safety. If your Bitcoins are lost or stolen, there's no intermediary with the power to make you whole. There are two basic ways to hold Bitcoins.

• You can participate in the Bitcoin network yourself, storing the keys to your Bitcoins in a wallet stored on your hard drive.

• You can delegate this function to a third-party wallet service such as Coinbase.

The first option makes you susceptible to hard drive failures, malware, and user error. To safely hold Bitcoins, you need a reliable backup system and a good encryption scheme. A single misstep or security breach could cancel out your Bitcoin holdings instantly [8].

The online wallet option isn't much good. Wallet services are possibly disposed to the same security and reliability drawbacks as individuals. Customers also want to worry about scams or uselessness of those who operate the wallet service. There have been a number of cases where the operators of Bitcoin financial institutions have lost client funds because of alleged security breaches. Bitcoins are great for digital transactions because they're virtual, fast, but their worth as a true currency is still up in the air. The Bitcoin exchange is quiet, extremely instable, which weakens the very purpose of currency as a reliable source of adequately steady value [6]. So while Bitcoin as a credible currency is yet to be determined its vitality in subversive business and cybercrime is undisputable.

A. Bitcoin stealing

All the largest thefts of coins have taken place in these banks of sorts, where people keep their Bitcoins until they're ready to spend them. There's nobody to certify that safety procedures are sound for the storage and management of coins and financial records. Once a Bitcoin transaction has been accepted by both sides, it is irreversible without the permission of the recipient. So when hackers contrive the transaction, the cash is gone always [8].As all Bitcoin are open knowledge, what permits a user to expend a coin is ownership of the linked private key. Stealing of private keys or signature counterfeits, thus liken to loss of money in this world [9].

B. Malicious assail

Malicious assail on Bitcoin are on the upswing, resulting in the theft of private keys. The online wallet service mybitcoin.com recently lost $1:3 million worth of users' coins due to malicious activity [9].

C. Bitcoin interactions

Many people do not escalate the purpose of an exchange, which is by definition is to exchange financial tools - not to use the exchange as a bank for assumption. For those who wish to trade Bitcoin, some forex exchanges are now offering Bitcoin trading on sideline, where Bitcoin can be traded for profit or loss without ever having to actually take possession of Bitcoin [6]. The centralized Bitcoin exchange is almost certainly a temporary phenomenon, to be replaced with decentralized, distributed peer to peer exchanges as further issues arise and centralized exchanges are regulated to oblivion.

D. Bitcoin wallets

To the new Bitcoin users, a wallet is a folder. But it is different from a general wallet with local computer based wallets such as web based on-blockchain wallets such as Blockchain.info [3]. Users will need to comprehend the important alterations among these options as well as the relative threats and how to use them efficiently. Although web based solutions are the most convenient they are also the least protected. And will come under increased manipulation by hackers because, unlike an email service there will be billions of dollars to be gained which will make hackers highly driven and no web based wallet will ever be totally secure. The most secure is the wallet by Blockchain.info which is on- blockchain and therefore at least cannot be inhibited with by administrations and other entities. Because of this anyone can send all of the Bitcoins from their Wallet onto a Wallet stored on a different machine and make a claim their Coins got stolen. In order to try to prove them wrong one would need to go through the effort of tracking the movement of those Bitcoins onwards until they reach a service that can link the data of a real person to their Address and check whether that identity is linked with the alleged victim of theft [11]. Anyone can insert arbitrary data into a Transaction that later can become a part of a Block. As Bitcoin relies on exchanging of all Transactions between Nodes and indefinite storage of Block Chain data, once a Transaction is included in a Block it will be received and stored on every computer running the Standard Client. Because of this, if illegal content was to become a part of the Block Chain, anyone using Bitcoin could in theory face legal problems.

Detection of illegal content in a Transaction varies depending on how it is stored. It can be simply inserted and dropped as a part of a script describing where to send the Bitcoins to [11]. In this case the Transaction can be easily picked up as non-standard and analysed in greater detail for possible malicious activity.

If the data is encoded as a Coinbase Transaction, input of which is regularly ignored, detection of whether its content is malicious is harder. However, since there is only one Coinbase Transaction per Block, and in turn Blocks don't appear nearly as often as standard Transactions, it can be checked more

thoroughly. Local computer based wallets including smartphone are the most secure because they can be used to cold store Bitcoin. But considerable user education is required even for this due to the fact most users are non-technical, with configuring and organizing wallets far beyond their computer ability.

E. Computer Trojans

This is the single biggest threat to Bitcoin security and the toughest to deal with. The personal computer of the average person is absolutely damaged with trojans. Not only does this deliberate the computer and use Internet bandwidth, these trojans are always being used for malicious purposes whether it is to steal data, delete data or harm the operation of the system in some way [6]. Numerous computers are infected by at least some malware. Most of the users have no idea how their computer becomes infected, that is has been infected and what to do if they do realize. If you want to profit from Bitcoins, you would not want to work against it. A 51% attack would not bring you profit, rather it would make everyone involved in the project loose, as Bitcoin's reputation would be damaged.The other thing is getting enough hashing power. Unless you target mining-specific machines, chances of getting higher-end mining-compatible graphics cards isn't too high. So the trojan would have to rely on getting a lot of moderately powered PCs, and in order to launch a 51% attack, the botnet would have to be quite big. The biggest botnets, consisting of over 100'000 computers could potentially accomplish this, but so far Bitcoin isn't a prime target for botnet activity. There is now a new wave of malware that specifically targets Bitcoin in various ways, including hacking the wallet and private keys and key loggers that record passwords, key phrases etc [2].

F. Packet sniffing

Someone who can get all of your Internet traffic can easily see when you send a transaction that you didn't receive. A hacker that has physical access to your network and computers can always find a way to abuse that access.

G. Denial of Service (DoS) attacks

Sending lots of data to a node may make it so hectic it cannot process normal Bitcoin transactions. The Denial of Service attacks are pleasing the practice of malformed transactions, which are similar enough to real transactions so that they can fool the exchanges. If Bitcoin exchanges get fooled by too many fake transactions, they fall out of synchronization with the blockchain, which holds the database for all transactions. And those exchanges subsequently need to recalculate their funds. This causes the Bitcoin exchange to slow down to an extent that it can no longer process users' transactions [4]. Instead we can use namecoin, Namecoin is a distribuited DNS system where information held about a web address (MX, A, etc) are held within the coin itself. Advantages of this are no other company holds the address, unique ownership will always be had due to the way the bitcoin works [11].

H. No Physical Form

Since Bitcoins do not have a physical form, it cannot be used in physical stores. It would always have to be converted to other currencies. Cards with Bitcoin wallet information stored in them have been proposed, but there is no consensus on a particular system. Since there would be multiple competing systems, merchants would find it unfeasible to support all Bitcoin cards, and therefore users would be forced to convert Bitcoins anyway, unless a universal system is proposed and implemented.

I. No Valuation Guarantee

Since there is no central authority governing Bitcoins, no one can guarantee its minimum valuation. If a large group of merchants decide to "dump" Bitcoins and leave the system, its valuation will decrease greatly which will immensely hurt users who have a large amount of wealth invested in Bitcoins. The decentralized nature of Bitcoin is both a curse and blessing.

VI. Conclusion

Bitcoin is an exhilarating invention that has the prospective to greatly improve human welfare and sta rtup helpful and theoretically radical developments in infrastructures, and payments. Bitcoin can also be used for money laundering and illegal jobs. Prohibiting Bitcoin is not the answer to ending money laundering and illegal jobs, just as prohibiting cash is not a solution to these same problems and business. No matter where your wallet is kept, it still counts as data at rest, which makes it an easier goal. Using strong encryption, as this will prevent unauthorized access and theft of your Bitcoins. But, remember it is not good practice to keep large amounts of Bitcoins in an easily accessible manner such as a mobile wallet. Instead, keep small amounts on a computer, mobile or online for everyday use and the remaining part on physical media, encrypted and locked away safely. In addition to encrypting your wallet, create redundant backups of it in order to avoid data loss. Eventually, we are not encouraging Bitcoin, but for modernization. It is important tha offcicials allow this experimentation to continue. Representatives should work to clarify how Bitcoin is regulated and to normalize its directive so that we have the opportunity to learn just ho pioneering Bitcoin can be.

References

[1] E. Jacobs, "Bitcoin: A bit too far?" Journal of Internet Banking and Commerce, vol. 16, no. 2, pp. 1–4, 2011.

[2] W. Dai, "b-money," 1998. [Online]. Available: http://www.weidai.com/bmoney.txt

[3] P. M. J. G. L. K. M. D. V. G. S. S. Meiklejohn, S., "A fistful of bitcoins: Characterizing payments among men with no names," in Internet Measurement Conference, 2013.

[4] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better how to make bitcoin a better currency," in Financial Cryptography and Data Security. Springer, 2012, pp. 399–414.

[5] G. Ateniese, A. Faonio, B. Magri, and B. de Medeiros, "Certified bitcoins," in Applied Cryptography and Network Security. Springer,2014, pp. 80–96.

[6] S. W. Haber, S., "How to time-stamp a digital document," Journal of Cryptology, vol. 3-2, pp. 99–111, 1991.

[7] F. Brezo and P. G Bringas, "Issues and risks associated with cryptocur- rencies such as bitcoin," in SOTICS 2012, The Second International Conference on Social Eco-Informatics, 2012, pp. 20–26.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: Bitcoin.org/bitcoin.pdf

[9] Preeti Sharma,Shweta Nanda,Sonamdeep kaur Is Bitcoin a Bona Fide Legal Tender? Journal of information and technology,vol II,summer 2014 page 101

[10] Fergal Reid, Martin Harrigan (2011), "An Analysis of Anonymity in the Bitcoin System", http://arxiv.org/abs/1107.4524 , accessed 2012-05-28

[11] MaxSan, "What are Namecoins?", http://bitcoin.stackexchange.com/a/1489/323 , accessed 2012-05-2

[12] Bitcoin Titan, "Are Bitcoins Securities Under U.S. Law?", http://blog.bitcointitan.com/post/16995504313/are-bitcoins-securities-under-u-s-law , accessed 2012-05-28

[13] MagicalTux , "Bitcoin in France: first legal decision directly related to Bitcoin?", https://bitcointalk.org/index.php?topic=41317.0 , accessed 2012-05-28

[14] Singh and Bansal. "A Survey on Intrusion Detection System in Data Mining." *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET,). Vol. 2, no. 6, June 2013*

