1. INTRODUCTION
Cashless system means a system that uses Internet banking, credit card, debit card, online wallets and other means of methods to make payment for any purchase of good or service without needing to have physical cash money. In a cashless system there is a void of physical currency or cash. So a person doesn't have to carry physical wallet with him. He can make purchases using plastic money such as credit card, debit card or a similar card or by using his internet enabled Smartphone or a desktop. Mobile and tablets are becoming very popular these days and people often tend to use internet on these devices. Mobile devices are so much popular for internet browsing that they have just surpassed the no of internet users on desktop [7]. So people always carry their mobile with them and use them to make purchases but in a country like India complete Cashless system may not be possible because there are may
hurdles in this way. These hurdles may include poor network connectivity [8], poor power transmission system in India [9], natural disaster and many others. After the demonetization as the no of online transactions has increased massively there is also a increase in cyber attacks. In this paper, we would like to talk about some of Cyber security attacks and problems that can be a big threat to Cashless economy.

2. Cyber threats to Cashless system
A Cashless economy or Cashless system is a system where we don't use physical money for making purchases and instead use different type of electronic transactions such as using debit card, credit card, online transactions or using mobile applications and wallets. These all things are handy and are very useful but going completely towards cashless system may cause catastrophe in the society because there are many threats that can cause a major financial loss any end user without him even knowing who did this to him.

So there are many threats to the cashless system, here we will look at some of the cyber threats that may cause damage to a single or even a large no of population.

2.1. DDOS
It is Distributed Denial of Services attack, it is a type of attack in which a large no of host computers are hacked by a hacker and are made as slaves and this hacker at the same time access to some service such as some website at the same time. When these slaves visit any website at the same time then this website either becomes slow or it just goes down and the site is left inaccessible to its legitimate users. Recently a website was attacked by a large army of slave IoT devices and it is the biggest attack till now [11]. Now suppose this type of same attack is done on a bank website or any other wallet provider then millions of users will be left unable to use their money from their phones and also from internet banking. It may take a while for these types of attacks to stop but during this time normal public would have to face many difficulties for accessing their money. This
type of attack will collectively affect a large no of population.

2.2. Ransom ware
A ransom ware [14] is a special type of malware [13] that has come into light recently and it is a very annoying and dangerous malware. A ransom ware when activated on any mobile or desktop it just encrypts the files and take them as hostages and make them inaccessible to the user and ask for money in order to decrypt the files. These types of threats masquerade [15] as an important file such as downloaded with other application, with an update etc and make their entry into the system. They generally affects the person whose files are in the device. Suppose you use mobile or desktop for making purchases and all bank related details are stored in it and some ransom ware attacks on your device and encrypts all files and leaves them inaccessible and asks for money. So this type of situation may be very painful for the people, how will they make purchases and there is no guarantee that after making payment for decryption key to decrypt the files it will work and decrypt all files. The attackers may give the key for some files and may ask for more money. Another thing is that they take the money and doesn't give up the decryption key then the encrypted device is of no use for the person.

2.3. Man in the browser
Gangs are also using malware on PCs to infiltrate mobile phones in hybrid attacks on user's banking accounts, according to John Shier, security advisor at Sophos. A piece of malware dropped on the user's laptop can detect when the user is surfing his banking website. Dubbed a “man in the browser” attack[1] – the spying is all done in browser memory “so they can intercept your banking credentials before they get encrypted and sent across the wire,” he explains. Adding to the scam, thieves put up a warning message, such as “for increased security, download this app,” and they ask for the user's phone number and email address to send an SMS to their phone or to download a link. “You click on the SMS and download the app, and they basically own your desktop
and your phone,” he says.

2.4. Phishing Attacks
In this type of attack, attackers create a fake website that look similar to bank website and try users to visit these phishing sites and to login on these websites so that they may get the credentials for the original bank websites and later use it on original bank website to achieve their 'dark' goal.

2.5. Social Engineering
In these types of attack an attacker try to show as a real employee of bank and try to win the trust of a user and try to make him so that he give up his credential to them. It can be done on phone using a call or by email or by meeting personally. For example someone get a call and caller tells him that he is calling from his bank branch and ask him different questions to verify him and tell him that his account is going to close or debit card is going to be inactive and these talks looks like real to a normal user and in fear he might be in trouble if his card is inactivated he tells them all his card details when asked and by this way attacker tricks people in this way and try to win the trust and then making their ill plan successful. People may fall prey to these kinds of attacks because they are not aware how to handle these types of calls and protect himself from these preys. These types of attacks can be done using phone calls, emails, messages or by personally meeting the victim/

2.6. Online banking security risks for Android users
European and American banks and e-pay systems offer a variety of ways to protect users' transactions – including authentication using e-tokens, one-time passwords, confirmation of transactions through codes sent to the phone, and more.[3] Cybercriminals are developing programs that bypass these measures. For example, the Zitmo family[3] of programs is designed to attack a user's mobile phone and can bypass the two-factor authentication systems used by European banks. These mobile malicious programs work in tandem with Zbot (ZeuS):
 • First Zbot steals the username and password – to enter the
online banking system from the infected computer.
- Then, during a money transfer, Zitmo – Zbot's mobile counterpart – takes over and forwards the transaction authorization code (TAN) to the cybercriminals.

2.7. Public WiFi
Public wifi is coming to India [17] and will be available on different locations and people can use them to access internet on their laptop and mobile but these wifi hotspots are not secure and the data passed through these hotspots can be accessed so for any banking related browsing using these these public wifi may be dangerous and possesses the risk of exposure of personal data to hackers.

2.8. Card Cloning
Card cloning [19] is another threat to plastic money. In this attack the attacker places a card copying device called skimmer[19] in ATM or in any machine that accepts debit and credit cards, such as ticket machines at the train station. A tiny camera is also placed that can record the password entered by the user. Now the attacker has copied your card and have your password he can make purchases using these details.

2.9. Credit card fraud
Credit card fraud is divided into two types: credit-card (offline) fraud and card-not-present (online) fraud. Offline fraud is committed by using a stolen physical card at storefront or call center. Online fraud is committed via web, phone shopping or cardholder-not-present. In online fraud only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase.

2.10. Lost or stolen cards
This is a method use by criminals to validate stolen credit card numbers. The criminals submit the credit card number and the cardholder's personal data on a website that has real time transaction processing. Typically, small monetary purchases are made in order to not attract the attention of a merchant and top reserve the credit limit on the card. Once validated, the card number
and related details will be sold to or exchanged with other criminals who will use the information to make larger purchases.

2.11. Shoulder Surfing
Shoulder Surfing is the act of direct observation, watching what number that person taps onto the keypad. The criminal usually positions himself in close but not direct proximity to the ATM to covertly watch as the ATM user enters their PIN or in the process of using public internet cafe. Sometimes miniature video cameras that are easily obtained might be installed discreetly on the fascia or somewhere close to the PIN Pad, and keyboard to record the PIN entry information.

2.12. Outdated softwares and insecure devices
Most of the ATMs are using outdated software system that are vulnerable to many attacks. Attackers can attack these devices and data of millions of customers can be stolen by these atms[21]. Other thing to be noted is some of these softwares that are outdated can not be provided patch as the company has ended the support for these softwares, so it means they are open to attacks and attackers are aware that all the vulnerabilities in these systems will be available and will not be patched so they can attack them whenever they want without worrying because they will not get updated.

Recently a massive attack on Hitachi Payment Services platform — which is used to power country's ATM, point-of-sale (PoS) machines and other financial transactions — and stole details of 3.2 Million debit cards [25]. Due to this attack millions of atm cards were disabled if the same thing happen in a cashless society then it will lead to a big trouble for millions of people.

2.13. Jailbreaking and rooting
Jailbreak and rooting is a method to remove the restrictions from devices. In Iphone this is known as Jailbreak and in Android it is called Rooting. Phone manufacturers doesn’t provide root access to devices as it can damage the device and it is not suitable for a normal user but there are many modifications and applications that requires root access. These
applications can be of many types and they can access phone completely without restrictions. So if any faulty or malicious application is installed then it can completely take the control of your device and also it can give the access of your device to the attacker that can access any of your data stored in your phone and also he can destroy all this data. So if your financial details are stored in your phone then it may be risky if phone has root access or jailbreak.

3. Cashless system of Nigeria and Cyber crime
The Central Bank of Nigeria (CBN) has introduced cashless system in Nigeria on January 1, 2012 in Lagos as pilot [28]. It started with the following visions

• To increase convenience/access to payment (more payment options)
• To enable more transparency in payment systems, and
• allow for more effective monetary policy
• To reduce risk of robbery
• To reduce huge cost associated with cash handling (printing, storing, processing, distributing, etc)
• To enable the achievement of the nation's vision 2020 objective

CBN states that its cashless system is aimed at reducing (NOT ELIMINATING) the amount of physical cash (coins and notes) circulating in the economy, and encouraging more electronic-based transactions (payments for goods, services, transfers, etc.) [27]. So Nigeria has not completely shifted to cashless economy but still it has cash based system too. Since then online transactions are increased in Nigeria for making payment transactions. With the increase in no of online transactions, the no of cyber attacks also increased in Nigeria. The government lamented the loss of over $450 million dollars to cyber attacks in 2015 alone.

The Minister of Communications, Adebayo Shittu, said a total of 3,500 attacks last year led "to a loss of about $450 million," the local Vanguard news portal reports.[26]

4. Conclusion
India is getting more and more digital each day and it is hoping for
going cashless. Many incentives and discounts are being provided to those who are going cashless. There are many pros in using cashless system to make purchases for buying goods and services but going fully cashless may not be a good idea as we have seen there are many security vulnerabilities that can be exploited by hackers that can steal our hard earned money from banks and our digital wallets that will lead to complete loss of money to many users. It is very easy to launch a cyber attack as the attacker doesn't have to face anybody and can launch the attack from a place which could be very hard to track due to the techniques used by him. So the conclusion is going completely cashless may not be a good idea and it might cause an increase in no of attacks as we have seen with Nigeria and can cause million of people to lose their money. But applying cashless system with cash system as a backup is a good idea as the Nigeria is working because if anything wrong happen such as massive atm card left disabled than people can use the cash instead of plastic money.

5. References


