MOBILE FILING OF TAXES - A SECURITY MODEL

Ginni Garg*

Dr. Meenal**

ABSTRACT

The Income Tax Department (ITD) of the Ministry of Finance, Government of India, is committed to provide world - class services to taxpayers in the country, making tax compliance easy and convenient. One of the initiatives of the Income Tax Department was the introduction of Electronic Filing (e - Filing) of income tax returns (ITRs), to make the filing process easier for taxpayers as well as to reduce the time required for data entry on receipt of returns. Now mobile filing is going to be introduced - a service where- in customers can e-file their income tax returns through their mobile phone. This paper deals with the importance and security of filing returns through mobile phones. Also a proposed security model is recommended to ensure safety to customers.

Keywords: *Encryption, ITR, mobile Filing, Security, SSL, Tax, Taxpayers, TLS.*

*Assistant Professor, D.A.V College Sec-10, Chandigarh.

**Assistant Professor, GJIMT, Ph-II, Mohali.

1. INTRODUCTION

The department desired a system that would make the process of filing of income tax returns (ITRs) easier for taxpayers as well as reduce the time required for data entry at their end on receipt of the ITRs. The next step in this direction is the introduction of software to enable e-filing of income tax returns on mobile phones. Enabling the filing of ITRs over the mobile phones was the most viable answer to the department's needs. While the facility would be beneficial to the taxpayers, the department had to create an environment wherein the user would feel secure about filing his ITRs through mobile. The online process did not require the taxpayers to be physically present for filing their ITRs.

e - Filing is a system for submitting tax documents to the Income tax department through the internet or direct connection, usually without the need to submit any paper documents. Various tax return preparation softwares with e-filing capabilities are available as standalone programs or through websites or tax professionals or from major software vendors for commercial use. "e - File is the term for electronic filing, or sending your ITR from tax software via the Internet to the tax authority" .(1)

E-filing of Income Tax Return Online refers to the process of filing Income Tax Return electronically either on computer or on mobile phone. We no longer have to stand in long queues to file income tax returns.

Now we can file returns through mobile phones at anytime and anywhere. TaxSpanner.com, India's largest and most trusted website for easy filing of taxes, announced the launch of its mobile version. This new facility offers taxpayers the freedom to file income tax returns (ITR) through their mobile phones from the first week of July, 2011.(2) However the same has not been actively adopted yet.

Known for providing secure and easy-to-use solutions for efiling tax returns for individuals and businesses, TaxSpanner has made the process simpler by introducing its website optimized for the mobile medium. Its most popularly used application to file income tax returns, "eFile by eMail", will be offered on mobile now. Also available on the website and on its Facebook page, this application is the simplest and fastest way to eFile returns. With accessibility on mobile, its simplicity can now be used on the move.

TaxSpanner has developed eFile by mobile solution using open source technologies namely Linux, apache, postgres, python, django which it has used for the service from its website(3).

In order to access this service, an individual will have to access the company's site from his mobile phone browser, from where he/she will automatically be directed to the e-file application page of the mobile site. A user also need not be register for this service, they only need to fill in a short form with some personal details and upload relevant form on the same page. Once this is done, the ITR will be filled and generated automatically(4)

The problem of how do we secure the delivery to mobile phones? By choosing a browser based platform allows security of SSL, encryption of content in transit, multiple firewalls to detect and prevent malicious access and Microsoft Active Directory to manager user accounts.(5)

2. SECURITY WHILE E-FILING RETURNS THROUGH MOBILE PHONES

SSL-The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.

SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

There are reasons to choose TLS over SSL, and the most significant relates to how it was developed. TLS is based on open community standards, which makes it far more extensible and more likely to be supported in the future. Perhaps the most unique advantage of TLS is that it is backward compatible, which basically means that it can be scaled to secure client side connections that only support SSL. Another distinct benefit is that TLS permits secure and insecure connections over a single port, while SSL designates one port for secure connections only. Even this factor does not make either any more or less secure than the other.

When it comes to SSL or TLS, what you need to know is that by not using either, the communications between you and another server can become the party line for eavesdroppers and cyber criminals. The data contained in your email, login screens and even financial transactions will be delivered across the net in plaintext for all to see. In addition, there will be no way to ensure that the server you connect with is valid and not just an interloper or middle

man setting you up for the fall. Therefore, it would be wise to adopt either of these protocols to keep your communications private.[8]

MOBILE SIGNATURES

Currently, GSM phones and WAP phones are mostly supporting this technology. Those mobile signature services on sim cards can be supported by almost all GSM phones, regardless of their capacity. In the near future, 3 G-phones and other portable devices will feature a similar mobile signature application.

The mobile signature is the legal equivalent of your own wet signature. The mobile signature is created by typing a secret code (i.e. your signing PIN) into the signing device (for example: your mobile phone). This secret code in combination with your key storage token (for example: SIM card) and a chosen text triggers a cryptographic algorithm to generate the (digital) signature.

Each of your mobile/digital signatures can be linked to a digital certificate (an electronic record) that vouches for your real-world identity.Thus, the mobile signature is a unique feature for:

1) Proving your real-world identity to third parties without face-to-face communications

2) Making a legally-binding commitment by sending a confirmed message to another party

3) Solve security problems of the online world with identity confirmation.

Authentication may still be vulnerable to man in the middle attacks and trojan horses, depending on the scheme employed.[6] Schemes like one-time-password-generators and two-factor authentication does not completely solve man in the middle attacks on an open network like the Internet. However, supporting the authentication on the Internet with a parallel closed network like mobile/GSM and a digital signature enabled SIM card is the most secure method today against the man in the middle attack. If application provider provides a detailed explanation of the transaction to be signed both on its Internet site and signing request to mobile operator, the attack can easily be recognized by the individual by comparing both screens. Since operators do not let anonymous third parties to send signing request, normally the cost and technicality of intrusion between the application provider and the mobile operator, makes it an improbable attack target.

SecMsg-

eMudhra SecMsg is mobile application designed to secure the SMS channel(7). It allows users to send SMS's that are encrypted and signed using PKI technology and ensures that it is decrypted only by the intended user.(9)

The algorithms used for crypto processes like Signing, Encryption, Decryption are RSA/ECC, AES and SHA.

Features-

1) This application supports multiple X.509 certificates from any certification authority(CA).
2) These digital signatures can also be used for digital signing and encryption/decryption.
3) Logging the history of transactions an d messages,access to which requires PIN.
4) Remote data wiping for clearing the contents of the application if the mobile is lost.
5) Uses simplest and ubiquitous communication mode-SMS channel.
6) Low operating cost.
7) Extensive device support.
8) Password Protection Software for mobile phones—

With more and more sensitive information being transferred to mobile smartphones, the implications of having your phone lost or stolen have grown more serious. Fortunately, many apps are available for smartphones that help safeguard your application passwords and make them easier to retrieve if you happen to forget them.

Password Safe Pro

This Android app stores web logins, credit card pin numbers and other sensitive data in a database protected by 128-bit AES encryption. It allows you to define your own data fields for each secure record and can back up data to DropBox and other cloud storage sites.

Splash ID

This application offers a typical range of password protection features, including single-password protection of sensitive data and 256-bit AES encryption. What makes SplashID unusual is that it is available for nearly every kind of smartphone, including iPhone, BlackBerry, Android and Windows Mobile.

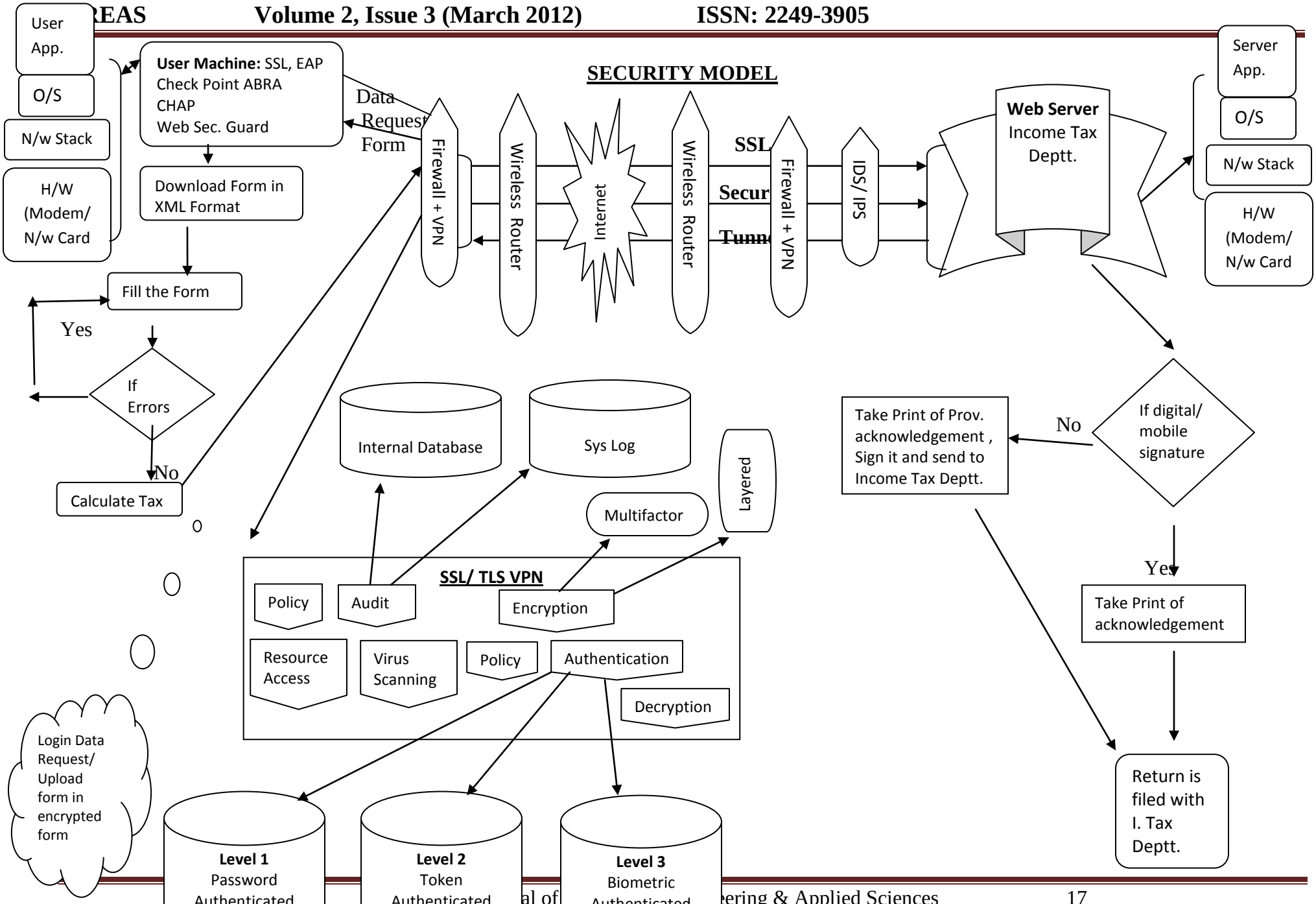
Wallet

Another Android program that stores your sensitive data in an encrypted database is Wallet. Special aspects of this program include that it auto-locks the phone and completely wipes the clipboard after a set timeout period, so that data that has been copied, cut or pasted can't be seen by others.

1Password

1Password is available for iPhones and Android phones. It locks usernames and passwords behind both a password and a four-digit lock code. Once inside the app, you see a list of log-in combinations you've saved; tapping one of them takes you to the relevant site and immediately logs you in.

3. PROPOSED SECURITY MODEL WHICH CAN BE FOLLOWED BY INCOME TAX DEPT IN E-FILING OF RETURNS VIA COMPUTER/MOBILE


SECURITY MODEL
User App.
O/S
N/w Stack
H/W (Modem/ N/w Card
User Machine: SSL, EAP
Check Point ABRA
CHAP
Web Sec. Guard
Data Request Form
Download Form in XML Format
Fill the Form
Yes
If Errors
No
Calculate Tax
Firewall + VPN
Wireless Router
Internet
Wireless Router
SSL
Secur
Tunn
Firewall + VPN
IDS/ IPS
Web Server
Income Tax Deptt.
Server App.
O/S
N/w Stack
H/W (Modem/ N/w Card
Internal Database
Sys Log
Layered
Multifactor
SSL/ TLS VPN
Policy
Audit
Encryption
Resource Access
Virus Scanning
Policy
Authentication
Decryption
Login Data Request/ Upload form in encrypted form
Level 1 Password Authenticated Database
Level 2 Token Authenticated Database
Level 3 Biometric Authenticated Database
If digital/ mobile signature
No
Take Print of Prov. acknowledgement , Sign it and send to Income Tax Deptt.
Yes
Take Print of acknowledgement
Return is filed with I. Tax Deptt.

In the above process of filing returns through computer or mobile phones.There are various security measures which are added to existing security architecture.

User machines-Various softwares are to be installed on user machine to ensure safety.

CheckpointAbra-Check Point GO uses hardware and software encryption to protect user credentials, documents, and other sensitive data, so that data cannot be compromised in transit or in the event the device is lost. The system uses an authentication process that enforces minimum levels of password strength, as well as certificates and security tokens for multifactor authentication for remote connectivity.

TSL- Transport Layer Security (TLS) is a protocol that ensures privacy between communicatingapplications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

CHAP- CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network.

WEB Security Guard- Web Security Guard warns you before you access a dangerous website, so you can prevent infection of your computer and invasion of your privacy.

Then user machine sends the request to income tax department web server for opening the site and downloads the form for filing return online.

After filing the form and calculating the tax user login to income tax dept website and the form is uploaded.the request passes through firewall and VPN then through wireless router through a secure SSL tunnel.

Installed in a matter of minutes, the Barracuda SSL VPN[(10)] enables complete control over the resources designated for external access, such as internal Web applications, file systems and other applications. From any Web browser, users can take advantage of a reverse proxy to access internal Web applications or access network files shares. Richer support for SSL tunneling is enabled through the Barracuda SSL VPN Agent, a lightweight Java client that supports common remote applications, including Remote Desktop Services, Citrix XenApp, VNC, NX, SSH and Telnet.

For complete network layer access, the Barracuda SSL VPN includes the Barracuda Network Connector, an installable VPN client for TCP or UDP connectivity. With the Barracuda Network Connector, users gain SSL access to legacy client/server application during a VPN session.

With robust security and auditing features, administrators define custom policies to govern resource access to particular users or groups while tracking user activity. For added security, files uploaded during a VPN session to network file shares or internal Web sites are scanned for viruses and other malware to prevent infections of critical network resources.

Remote access by nature can be risky exposing network resources across the Internet. However the Barracuda SSL VPN mitigates these risks by tightly controlling user access through a full suite of authentication mechanisms and support for third-party authentication, such as Active Directory or LDAP. Administrators have the option of layering security by enforcing the use of PIN numbers, hardware tokens, client certificates and other forms of secure authentication on top of AD or LDAP.

By restricting usage to internal resources upon presenting the correct credentials and token code, an organization securely manages external access to network resources

At the receiving end Income tax dept receives the return then check for digital signatures and send the acknowledgement of return filed.

4. BENEFITS OF FILING RETURNS THROUGH MOBILE PHONES

Tracing of culprit- for filing returns through mobile phones.mobile phones must be registered with income tax department.If anyone does fraud with the information then culprit can be traced bi income tax dept.

Voice recognition system for filing e-form-For blind persons voice recognition software can be very beneficial.They can fill the e-form by voice only which will be recognized by software .

5. CONCLUSIONS AND RECOMMENDATIONS

We have concluded that there are many benefits of e-filing. Various researchers have different opinion regarding the security architecture adopted by income tax dept for secure e-filing . Many companies have made software for mobile phones for filing returns like TaxSpanner.com .According to some researchers many challenges are there regarding adoption of e-filing by mass population .Main challenge is risk of security. In this regard we have proposed the security model which can be followed in mobile phones as well as computers to ensure more safety to customers. The three main aspects of security include: confidentiality, integrity and availability.

Hence main importance should be given to security of private data of customers, so that more and more people e-file their ITRs.

6. REFERENCES

1. http://en.wikipedia.org/wiki/IRS_e-file
2. http://taxguru.in/income-tax/file-returns-mobile-phone.html
3. http://www.themobileindian.com/news/2197_File-Income-tax-return-via-mobile
4. http://taxworry.com/e-file-tax-return-through-mobile/
5. http://www.judicialsupport.com/blog/?page_id=648
6. http://www.schneier.com/essay-083.html
7. PC's Telecom Blog
8. http://webhostinggeeks.com/blog/2009/11/30/ssl-vs-tls-which-provides-the-best-protection/
9. http://en.wikipedia.org/wiki/SecMsg
10. http://www.barracudanetworks.com/ns/products/sslvpn_overview.php