Awareness About Cyber Security and Prevention Methods For Home User

Avinay Mehta , Sayan Chakraborty , Saurav Kapoor and Dr John Singh . K
School of Information Technology & Engineering
Vellore Institute of Technology, Vellore
Email: avinay1165@gmail.com

Abstract

Today we are in the era of digital world. In digital world everything works on internet and computers. Internet makes our life so easy that with the help of internet we can do many things. Shopping, social networking, business everything is going on internet. With the increase in the technology there is also parallel increase in cyber-threats. Cyber-threats causes many problems to Home Users and they mainly attack on them because either they don't know about the security system or they are not much familiar with the technology But due to lacking of knowledge about cyber threats, people become addicted to this kinds of threats. This kind of threats can be in form of malware or virus and they can hack the entire data of the computer. It is necessary to take some security measures to secure our system from these kinds of threats. This paper discuss on some technique that help user to secure their system from cyber attacks, it is necessary because information is very valuable and if it goes on wrong hand then it might creates major risks to users. E-mail, or any application that user uses in his day to day life.

Keywords: Cyber-Threats, Home users, CMA, Malware, Security, Risks, Hacking, Technology.

I. Introduction

It is the era of computers where we spend most of the time with computers. In other words we can say that we are in digital world. The digital world makes our life easy and simple. We can easily communicate face to face with the person who is very far from us, purchasing products from online markets, to pay some money to others, everything becomes easy. With the increase in digitization, users of internet also become more. With the increase of use of Internet, threats also get increased. Threats like hacking of account, tracing of somebody transaction etc. These threats are commonly known as **cyber threats.** The person who does this kind of activities are known as criminals and these activities are known as cyber-crime. Cyber- crimes has become a fast growing type of crime where more and more criminals exploit the speed, convenience of the Internet to do different types of criminal activities that may have no border. Now a day's cyber security is not restricted to a personal workstations but also used to suppress information of mobile phones as they have some less security issue. Every day, more and more home users connect to the Internet for business, social and networking purposes – or even simply to gather information. For this, they use all forms of computers and devices. Lately, though the trend has been increasingly towards mobile devices such as smart phones, tablets and the like. This leads to increase threads for home user security. To solve home user security issue all sectors, organizations comes together and they needs to understand the threats to the computing world.

Security Measures For Home Users Home network mainly contains two or more interconnected system by which internet service provider provides many services to its users(ISPs).Node connects two or more devices via wireless or wired medium they also connects devices such as PAD, mobile, etc.

There are three categories to get security for home users are as follows:

1. Thick Security
2. Intermediate Security
3. Thin Security

Thick Security Oriented Home User

As we know that malware is a powerful irrelevant program that effect computer system and it also affect those systems that are directly or indirectly connected by the corrupted system. It rapidly increases and affect as much as system in the network. Now a day's many users depend on their own domain knowledge to prevent their devices from multiple threats.

This is the level of thick security home user where users are only responsible for all of their security issues in thick security there is no involvement of any party in respect to prevent users from unwanted threats users can find their solution by their own to protect their connected devices from security issues.

There are many problems faces by thick security users:

- They forgot to download and updates
- They do not keep up to date with the security related technologies and risks
- They have inadequate and incorrect security protection
- They lack information security awareness.
- Their passwords tends to be weak
- They do not update their antivirus regularly

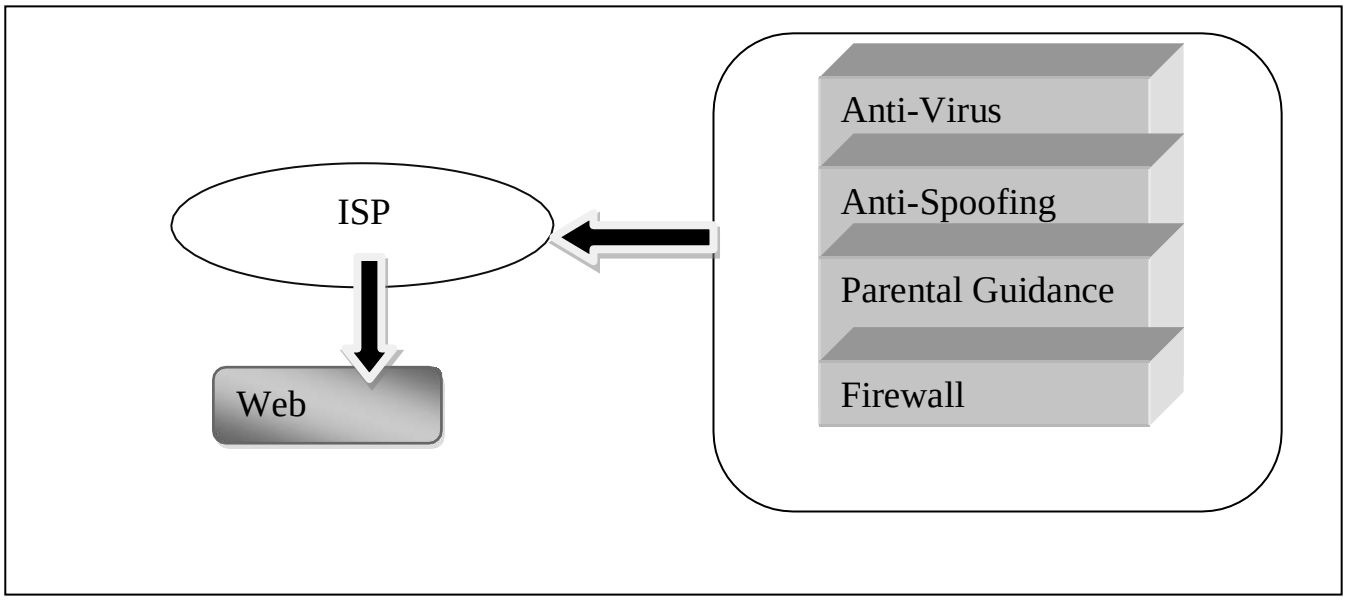

Fig.1: Thick Security-oriented home use

Intermediate Security Oriented Home user

At this level security issue is divided between user and a controlling entity (here controlling entity is regulating service-the ISP.) ISP provides users to connect to the internet. By the involvement of ISP. Some of the load of user were reduced because ISP will handled some aspects of security such as virus malware containment and alert users if any cyber threats have been detected.

This provides ISPs to make their users aware of cyber security problems and how they solve by their own. It is a very good start but intermediate approach is not fully solve the problems of users. Here we discussed other aspect of security prevention that make users free from all the responsibilities in concern with security.

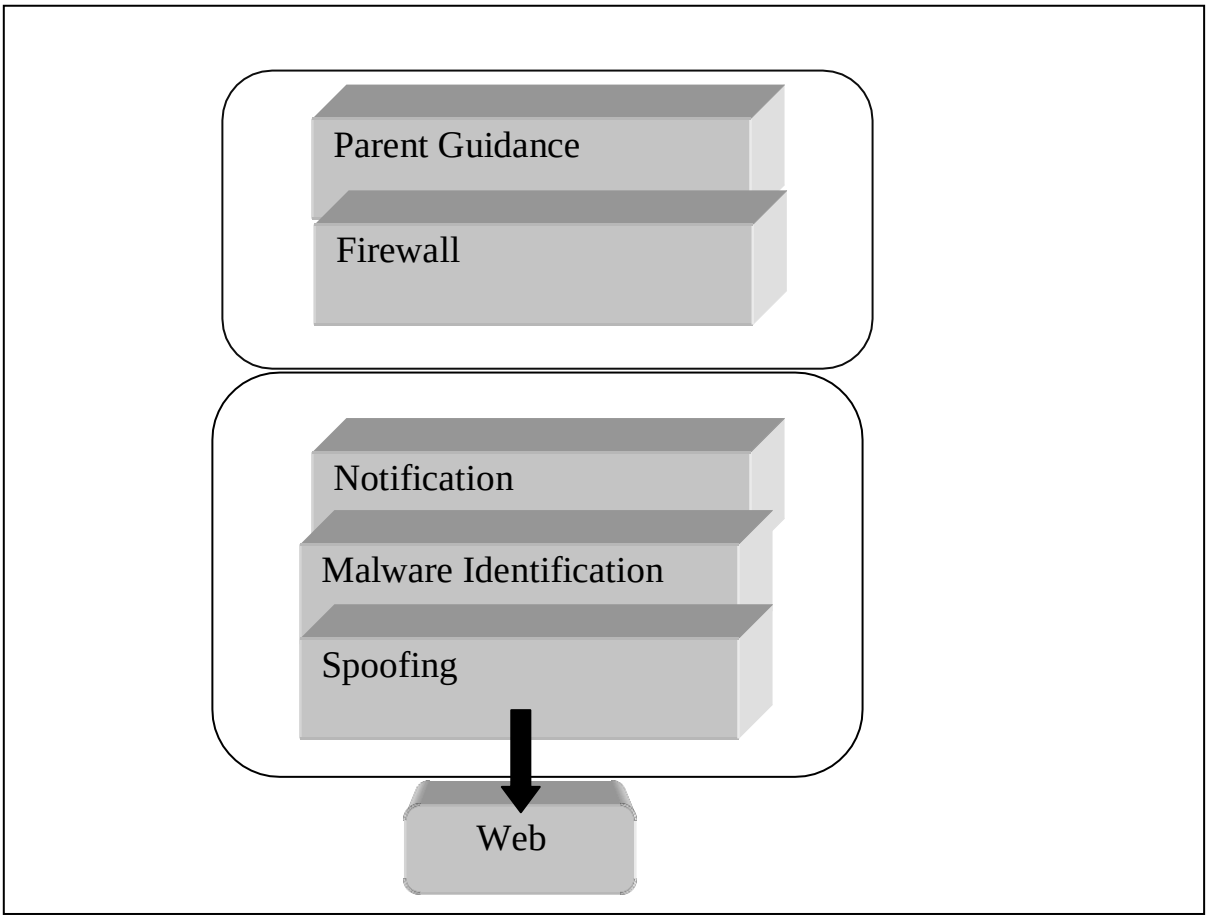

Fig.2 : Intermediate security-oriented Home User

Thin Security Oriented Home User

At this level, most of the responsibility for cyber safety is taken away from the home user and becomes the responsibility of the ISP. The home user will still have limited cyber safely issues (human related) to address but will be assisted by his or her ISP with the technical security aspects.

The ISP will provide the home user with a number of technical requirements needed to provide protection against cyber threats. In addition, each home user will be advised of all the technical services provided and enforced by the ISP.

Examples of such services are:

1. Continuously updating virus-protection.
2. Immediate patching of vulnerabilities when patches become available
3. Time to time scanning of the user computer to detect malware
4. Protection against spam.

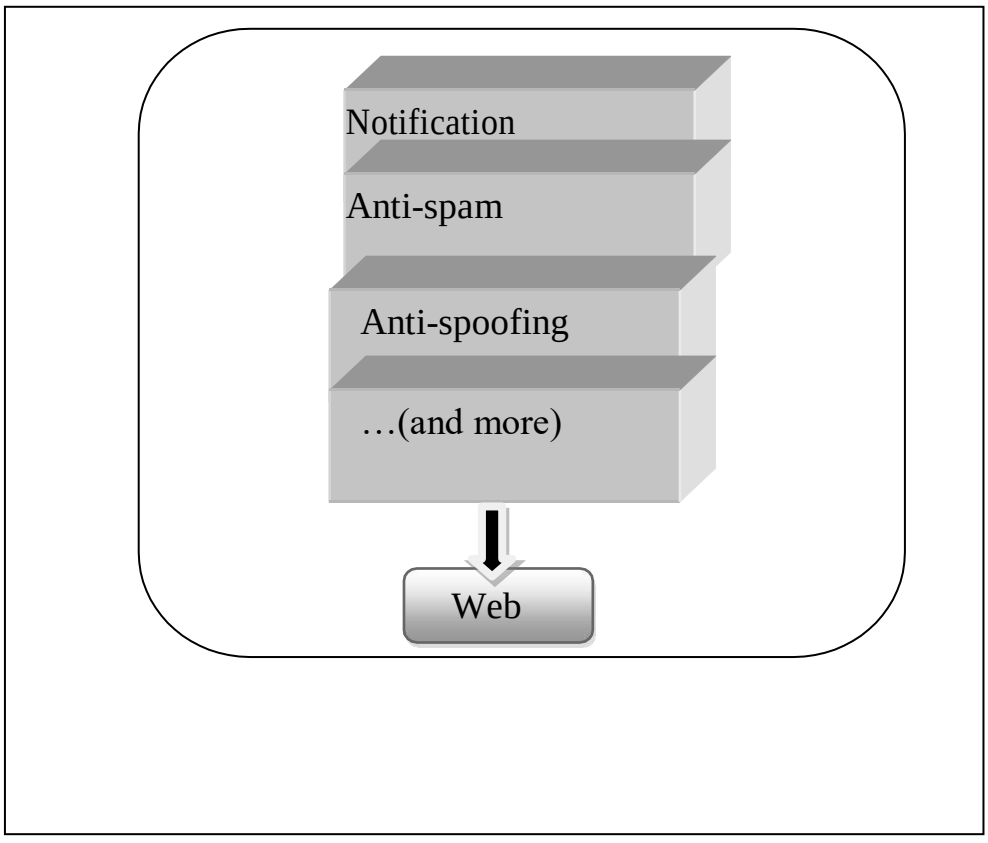

Fig.3: The Thin security-oriented home user

II. Related Work

As now a days there is sudden rising in the E-business and E-marketing and also in today's world our life is more dependent on internet **[1]** and beside that we also getting more susceptible to get caught in any mishap through cyber connectivity. The government and private companies are still finding out the ways to resolve both cyber crime in cyberspace and accounting responsibility. As there is a big rise in need of cyberspace, its exploitation is increasing on a very rapid pace. Now-a-days, cyber security is becoming very important and crucial area for lager number of terrorist attack on important and critical information centre. International cooperation is the need of hour to crack down an efficient law to handle cyber crime which is not confined to boundaries of states and thus an universal collaboration of states is required to plan together in order to reduce the rapidly increasing cyber crime & cyber risk to the least level.

In **[2]** is focused on providing the cyber security to home users as in India the many people excess internet from their home but many of them doesn't belongs to technical fields and do not have any idea about cyber threats to their data or information and they don't know how to protect their important data and information from these threats while connected to internet. It is therefore vital that home users be assisted to ensure that they are "cyber secure". So in this paper the author has proposed three ways to address cyber security among home user. The first step involves home users taking full responsibility for their own cyber security. Currently this is the adhoc situation in most cases and it is the cause of most of the cyber security incidents, breaches and cases of fraud that occur. The reason for this is that most home users do not understand and/or do not implement proper cyber awareness principles."Thick security-oriented home user" is refer as a first step . In the second step of cyber security that will assist home user to manage their cyber actions. The main focus of this step is to move some of the responsibility to regulating bodies for e.g.: ISP(Internet Service Provider). At last in the third step the all the responsibility of cyber security will be given to their Internet Service Providers.

As in today's world the internet has become vital part of ever field and emerging at an increasing rate. **[3]** examines the problem of cyber crime and the difficulties that it presents due to the way that it is being placed in England and Wales. In this the author focused on the area of hacking. Keywords— computer misuse act; cyber crime; hacking; regulation of investigatory powers, IT law, internet technology. CMA that is mainly computer misuse act established in 1990 to deal with the cases of cyber crimes but in nowadays it seems to be failed because of new technology arrived in this emerging era. Today is the generation of smart phones which made one's life easier but it creates problems also, like hacking some personal data of an individual or hack the account and many more. There is some provision in the legislation like CMA 1990, RIPA 2000, DATA PROTECTION ACT 1998. One of the provisions in RIPA is that under section 1 of RIPA act if someone commits any illegal activity in relation to computer or network either public or private intentionally then he or she gets a life imprisonment of 2 years.

In **[4]** assumed star-topology home network model. Home server is center at the star- topology. It can supply that devices with various communication methods (wireless/wired LAN, LNCP, HNCP, Bluetooth, ZigBee, UWB, etc.) can communicate each other through home server, and home manager (father or mother, or both) can be control of home network service access. Also, author suggests a user authentication mechanism using biometric information. It is proper for our home network model. And it is applicable to user authentication mechanism for ID/PW, certificate, etc. At Our home network model, home server is very important and must be secure from attacker. And it works all days like refrigerator.

In **[5]** this proposed an effective Home Automation System along with the security using low cost Wi-Fi modules. The user gets notified by the security system on his mobile if any threat occurs. A camera module is connected to the Micro controller which captures the image of the intruder. The prototype of our proposed system.

In **[6]** highlights the security threats faced by home users and their inability to understand the problems due to a lack of awareness. The increase in internet home users is ever rising in a developing country like India due to the benefits of easy access to information. It also encompasses security threats due to lack of security awareness. From the results of this study, it is shown that peoples' perception of information security can be improved through awareness and user friendly security controls (interface).Both sets of event samples recorded during the study period includes significant proportions in which the users were unclear on what they had to do and were prevented from completing the the task that they were attempting to undertake. Even from the relatively small sample involved it is clear that the security features within applications can demand knowledge that the end-users do not possess. This leads to an unfortunate segregation among users, where one group is capable of protecting themselves while another group cannot even recognize a security threat. In addition, it is worth remembering that the results were obtained from a group that largely classed themselves as non-IT users. Some of the features in internet browsers such as cookies, activeX controls, blocking popup (window), are too complex to be comprehended by the common end user. While downloading free software from internet, the user, by clicking yes to all these controls, can become a victim of an attack, without his or her knowledge. To have an effective and secured end user protection, intelligent software can be developed which would track the user behavior, user internet behavior, and the software installed on the system and accordingly tune the system to protect without much user intervention. This software should have the ability to respond to complex features such as enabling or disabling cookies, activeX controls, toolbars, etc and the end user should not be prompted to respond to activate such controls.

In proposes user authentication **[7]** mechanism for user convenience in home network i.e. user can be authenticated by user' s favorite authentication method, and then access to contents servers. If our user authentication mechanism is applied, user don't have to remember all user oneself authentication information which is user enrolled to various contents servers. And user' s important personal information such as biometric information can be protected from home network enterprises or internet service providers. And user doesn't have to carry certificate to log in to the certificate required contents servers.

In the home network **[8]** is to provide various home services inconvenient way considering user's characteristics with home devices familiar to users. However, without security tremendous confusion can be occur. So, in this paper, author focused an access control model based-on home gateway. It provides not only secure protection of home network system from inner/outer illegal accesses, but blocking of unnecessary accesses to services.

III. Modified Work

ISP is not in the position to handle all the problems of user because ISP has limited functionality due to

- Client is not in a position to pay money for their Security.
- Due to some legal problem

ISP provides many awareness to protect their data they cannot ensure that users really understand and sufficient for implementing safeguard for them.

As we discuss above the three categories as THICK, THIN, INTERMEDIATE here the functionality of ISPs and users are different that in one case we see that all the security measures of user are only dependent on user itself he only need to select the appropriate choice to reduce its cyber threats, in other case we see that the function is divided between ISPs and user here both can access the security and provide better solution to a problem, similarly in other case the all security responsibility went to ISPs hand from the user here in this case there is no intervention of user only ISPs is responsible for every single threats.

The following diagram is given below:

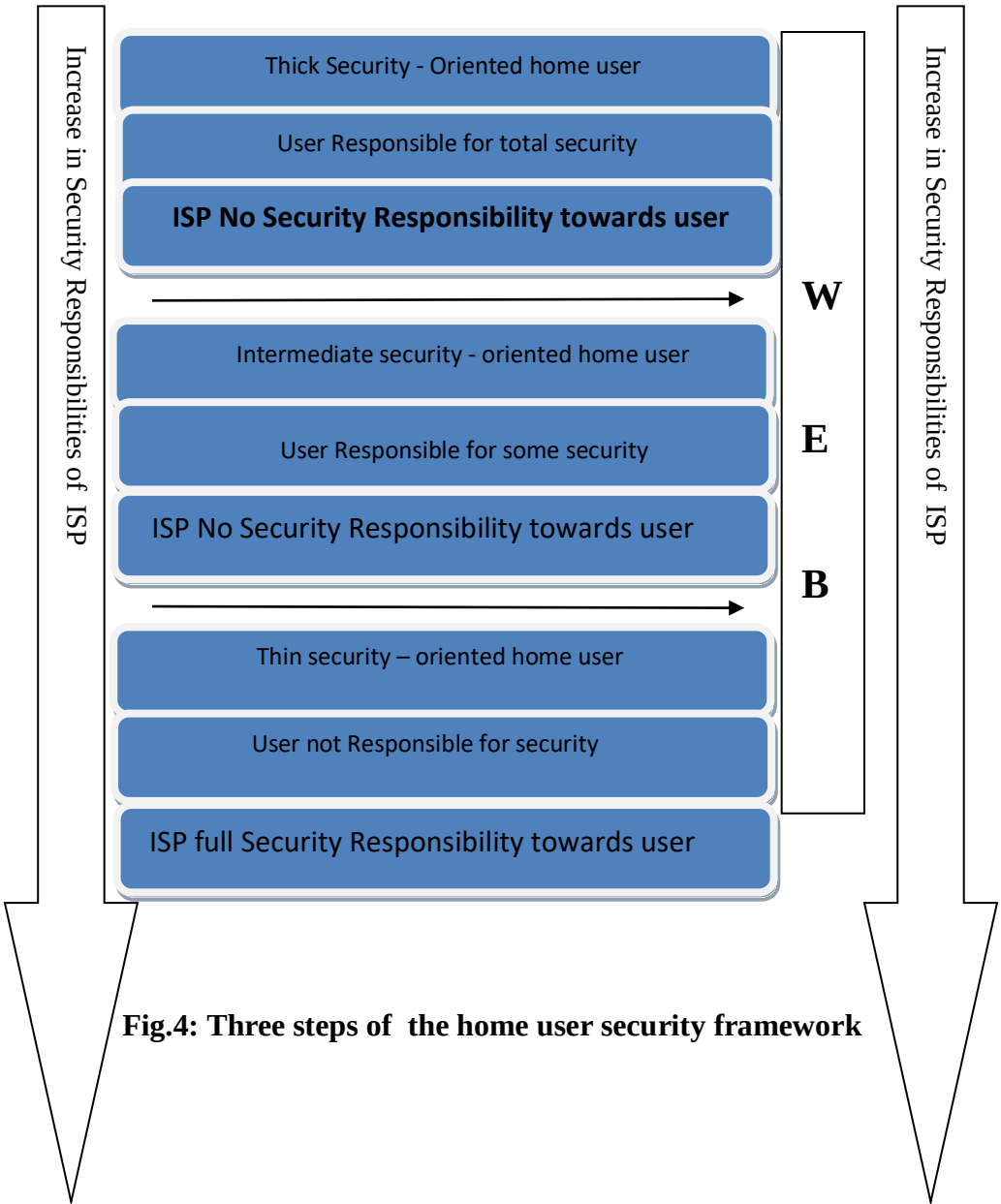

Fig.4: Three steps of the home user security framework

In above three technique we see that there is some security issue still exist because there is no equal access to both ISPs and user. In the above cases either ISPs or user will handle security or they access some limited security at intermediate level. So in worst case if one of them is not able to provide security then it causes many troubles for user like some outsiders can get access to your confidential data and files. For example if someone is using THIN ORIENTED SECURITY he handover all the security responsibilities to ISPs (Internet Service Provider). But in some point if ISPs is unable to provide security to the user then user is not able to secure himself because he do not have any security access to protect him by himself.

So we come up with the another new technique to solve this problem face by the users the diagram is shown below:-

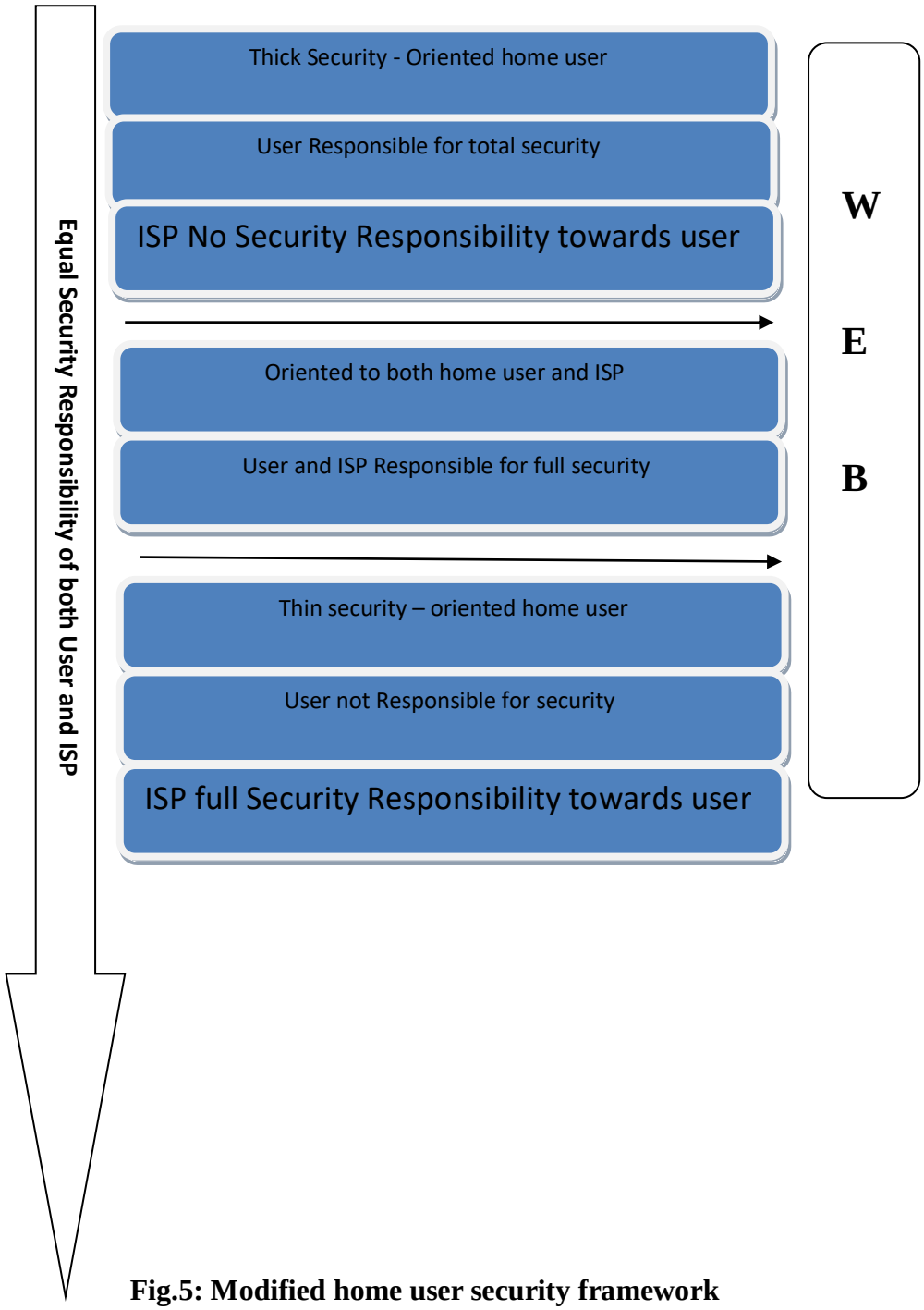

Fig.5: Modified home user security framework

IV. CONCLUSION

Here this paper proposed a new technique that both the user and ISPs has equal amount of access to the data so that in worst case if any of them are unable to resolve the threat then other can resolve it. In this technique we do not want to worry about security threats that we face in thick and intermediate there either we are only responsible or both we and ISPs are responsible there we have not full access to security that's why in worst case if (ISPs) loose to handle the security then user can't do anything to help himself that's why equal access to both user and ISPs are necessary to protect the device from unwanted threats and provide better security to user.

REFRENCES

[1] E Kritzinger "Providing the cyber security to home user as in India", In proceeding of IEEE International Conference on Science and Information, PP 340-345 ,2013.

[2] SH von Solms :"Home User Security-from Thick Security-oriented Home Users" In proceedings of IEEE International Conference on Science and Information 2013 London UK, PP 340-345,2013.

[3] Reza Montasari Pekka Peltola, Victoria Carpenter "Gauging the Effectiveness of Computer Misuse Act in Dealing with Cybercrimes" In proceeding of IEEE International Conference on Science and Information 2015.

[4] Yun-kyungLee , Hong-il Ju , Dowoo Kim and Jong-wook Han "Home Network Modeling and Home Network User Authentication Mechanism Using Biometric Information" ,In proceedings of IEEE International Symposium Conference on Consumer Electronics, PP 1-5,2006.

[5] S.M. Brundha, P. Lakshmi and S. Santhalakshmi; "Home Automation in Client-Server Approach with User Notification along with Efficient Security Alerting system" ,In proceeding of IEEE International Conference on Smart Technologies For Smart Nation,PP-596-601,2017.

[6] Umesh Hodeghatta Rao Xavier and Bishwa Praksh Pati,"Study of Internet Security Threats Among Home Users", In proceeding of IEEE Conference on Computational Aspects of Social Networks, PP 217-221,2014.

[7] Yun-kyung, jee-hye Par,"User Authentication Mechanism Using Authentication Server in Home Network", In Proceedings of IEEE Conference on Advanced Communication Technology, PP 500-506,206.

[8] Geon-Woo Kim, Do-Woo Kim, Jun-Ho Lee, Jin-Beon Hwang, Jong-Wook Han."Consideration on Security Model of Home Network", In proceedings of IEEE Conference on Advanced Communication Technology,Volume-1 Issue 4,PP-112,2006.