The International Journal's
Research Journal of Science & IT Management
ISSN:2251-1563

Security Threats In Window 8

Syed Mustafa Ali , MadeehaMukhtar, NidaYasir.
Department Of Computer Science, University of Lahore (Sargodha campus) PAKISTAN.

ABSTRACT:
Security threats concerning to operating system was considered to be the core issue. From the past two decades with the proceeding of new technology many security procedures are invented to thwart those threats. Window 8 also suggest many procedures and take precautionary measures like new trusted boot system, App locker, Data isolation, Antivirus protection, extensive memory, Secure internet explorer 10 browser, secure boot, Anti-malware protection to thwart. The main focus of this research article is to discuss these security threats. Antivirus protection to take full advantage of Windows 8's new security features; your PC needs to run a new kind of boot system called Unified Extensible Firmware Interface (UEFI). This system, which replaces the archaic Basic Input/output System (BIOS), adds many new boot features and greatly speeds the startup process. Internet explorer 10 browsers are the first line of defense in keeping you safe on the Web. Extensive memory Windows 8 also includes extensive memory protection that works to reject invalid input. Due to the inclusion of UEFI, there is also a boot-level malware scanner which will prevent your computer from booting if a USB thumb drive is infected. Anti-malware protection, Windows 8.1 is provided the built-in encryption devices. At the end of the conducted research study we sum up with future improvements/suggestion in window 9 such as (Bio Matrix finger print authentication, eye authentication, voice authentications) Bio matrix, Active X controls, security of signals and active defiant bug for apps.

INTRODUCTION:
The compression between the latest three versions of Micro soft windows.
Here we describe the sum latest feature of Micro Soft windowsXp, window 7 and windows 8.[1]

Table 1

	Windows XP	Windows 7	Windows 8
License	Proprietary commercial software	Proprietary commercial software	Proprietary commercial software
Worldwide release	October 25, 2001	October 22, 2009	October 26, 2012
Stable release	April 21, 2008	February 22, 2011	August 1, 2012
Kernel type	Hybrid	Hybrid	Hybrid
Platform support	IA-32, x86-64 and Itanium	IA-32 and x86-64	IA-32, x64, and ARM
Preceded by	Windows 2000 Windows ME	Windows Vista	Windows 7
Succeeded by	Windows Vista	Windows 8	-
Physical Memory Limits	4 GB-128 GB depending on the version and the architecture.	2 – 192 GB depending on the version and architecture.	4 GB -2048 GB depending on architecture.
Processors	32 for 32-bit, 64 for 64-bit	32 for 32-bit, 256 for 64-bit	32 for 32-bit, 256 for 64-bit
New Features	GDI+ graphics subsystem	Touch and handwriting recognition	Support of ARM architecture
	DirectX 8.1 upgradeable	Support for virtual hard disks	new "Hybrid Boot" mode

	to DirectX 9.0c	Improved performance on	New lock screen
	Improved Taskbar	multi-core processors	New Start Menu
	New features (task panes, tiles, improved sorting and grouping, built-in CD player, Autoplay, Simple File Sharing, etc.)	Improved boot performance	Native USB 3.0 support
	Kernel enhancements	DirectAccess	Microsoft Account Integration
	Faster start-up	Kernel improvements Window borders and the taskbar do not turn opaque when a window is maximized	Windows Store
	Ability to discard a newer	Taskbar	Windows To Go
	device driver in favor of previous one.	New version of Windows Media Center	NFC support
	More user-friendly interface	XPS Essential Pack	Windows Explorer renamed to File Explorer
	Fast user switching	Jump Lists	File Explorer includes a ribbon in place of a command bar.
	ClearType Font rendering mechanism.	Show desktop button shifted to right-hand size	Additional Security Features (SmartScreen, Security Essentials, Parental Controls, etc)
	New networking features (Windows Firewall, Internet Connection Sharing integration with UPnP, NAT traversal APIs, Quality of Service features, IPv6 and Teredo tunneling, etc.)	Allows more customization	Internet Explorer 10 as a program and an app. Charms
	Remote Assistance and Remote Desktop features.	A new version of Microsoft Virtual PC, newly renamed as Windows Virtual PC	Direct synchronization to SkyDrive App.
	New security features	The Remote Desktop Protocol supports real-time multimedia application.	Heavier integration with online services
	Side-by-side assemblies	Improved backup and restore	Redesigned Task Manager
	Improved media features	New Extended Linguistic Services API	Supports UEFI specification known as 'Secure boot'.
	DLC and AppleTalk network protocols are removed.	Better support for solid-state drives, including the new	Changes in Backup and Restore

		TRIM command	
	Plug-and-play–incompatible communication devices are not supported	New networking API with support for building SOAP-based web services in native code.	Traditional Start Menu
	Service Pack 2 and Service Pack 3 also remove features from Windows XP.	Classic Start Menu user interface	Windows Media Center as a purchasable option

In Sep, 2011 BILD Developer firstly Launched Window 8 in Conference 1,2 at BULID developer. It was just a prototype of window 8 which grabs a great attention in blogs, research articles. Officially it is released on 6th OCTOBER 2013 and gets attention from Microsoft users by its dual mode interface. It operates efficiently in both environments i.e, one for the touch screen and other for the traditional PCs. Formally this interface change is known as Metro user interface. Window 8 focused on cosmetic changes, but considerable advancement has made into its security procedures.

Today world should have become a global village and people are connected to each other all over the world by using the services provided by Operating system. So it is needed to introduce new foolproof security procedures for secure execution and communication. For this purpose Window 8 also suggests many procedures and take precautionary measures like new trusted boot system, App locker, Data isolation, Antivirus protection, extensive memory, Secure internet explorer 10 browser, secure boot, Anti-malware protection to thwart. The main focus of this research article is to discuss these security threats App locker Specify exactly what is allowed to run on desktops with the AppLocker feature in Windows 7. It provides the flexibility to allow users to run the applications, installation programs, and scripts which need to be productive. Learn how you can realize the security, operational, and compliance benefits of application standardization by using AppLocker [2].Antivirus protection. In order take full advantage of Windows 8's new security features, your PC needs to run a new kind of boot system called Unified Extensible Firmware Interface (UEFI). This system, which replaces the archaic Basic Input/output System (BIOS), adds many new boot features and greatly speeds the startup process [2,3].Internet explorer 10 browser is the first line of defense in keeping you safe on the Web. Internet Explorer 10 was designed with keeping security in mind, and third-party reports [3,4] Extensive memory Windows 8 also includes extensive memory protection that works to reject invalid input. Browser's Tracking Protection privacy controls give users with more control over online privacy. Anti-malware protection, Windows 8.1 is provided the built-in encryption devices, and also provided 16 other new security methods to these precautionary measures, because Attacker priorities are changed with the technology advancements. Attackers now attack application programs to web browsers to web plug-in instead of operating system. In this paper as the name suggests we discuss security threats in window 8.The purpose of this paper is to review all security threats. In operating system security threat is the main issue. From the beginning to till now, It is harder to find and understand how to protect our system from different threats; they are harmful and damage our system in different ways. Windows 8 do effort for securing PCs/hand handled devices than ever before e.g. By UEFI secure boot, By ELAM boot process and at the end it is fully loaded by the window defender. Its working is enhanced with network monitoring behavior for stopping the malware protection. Now it is working not only as anti-virus but it also checks the bad behavior in memory, the registry, or the file system. All this security system works when the window is up-to-date. If this software is outdated the attackers will attack very easily.

Many layers of the antivirus are used for protection. Because of two interfaces there is possibility for the user to confuse and ignore the alert messages of window which are generated for malware, unauthorized access, leg mate or user attack/social engineering Cyber Criminals used to change their modes operands of attack as soon as the security procedures change and increase new tricking computing. After ELAM and digital certificate usage in window 8 it is large possibility that cyber criminals attack on these digital certificates and damage/harm the digital signed code for the boot

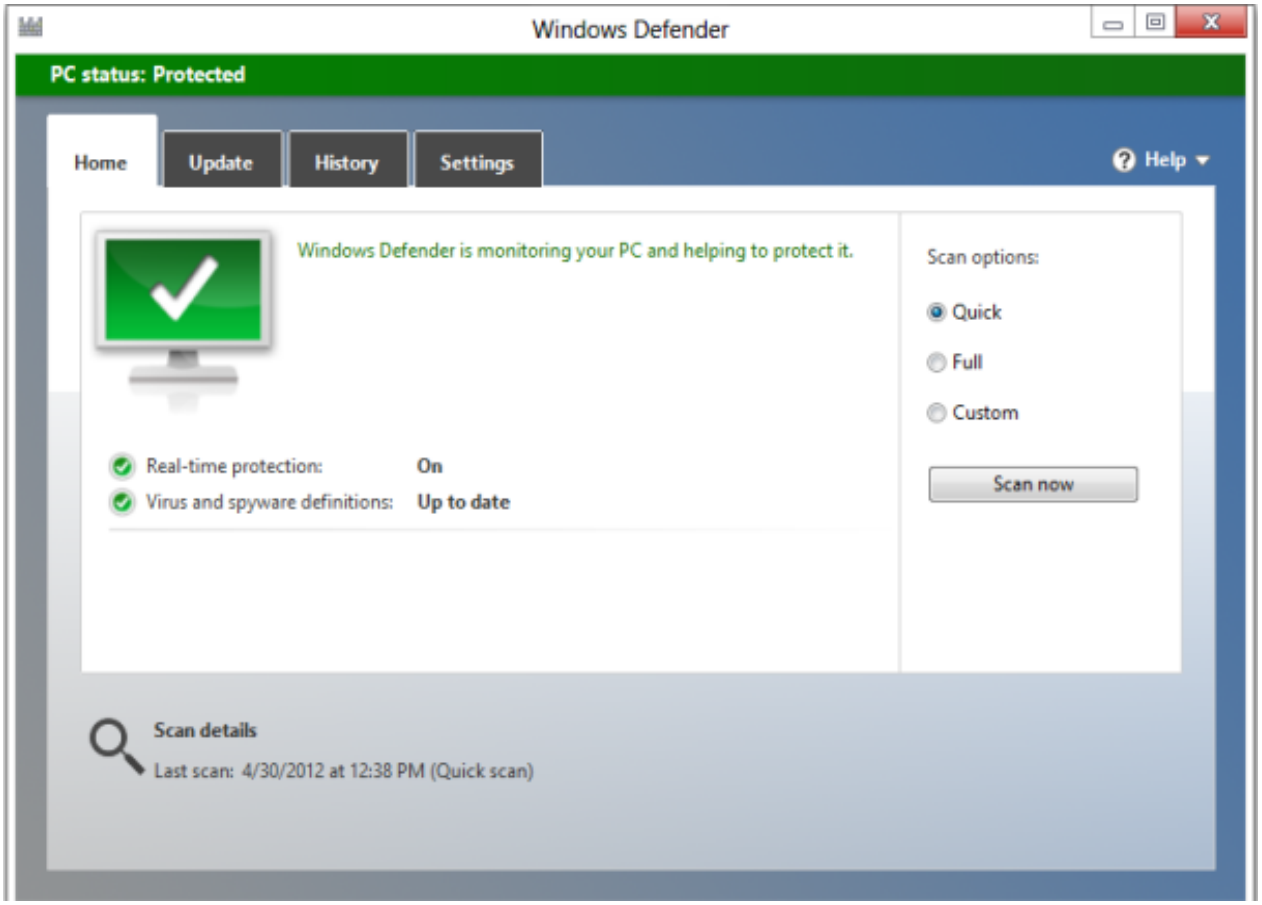
loader. If these codes are theft it will cause a great harm to millions of computers. For this reason it is necessary to update security procedures. Especially security authorities update it by defining new rules/procedures for assigning digital codes. For all these features it is reported that window Bio Matrix feature for picture password in not enough for secure login. Microsoft said that it would be far more secure than PIN numbers or passwords because users would have a potential of 1,155,509,083 different ways to touch an image via taps, circles and lines. It sounds like an ideal security system, but a recent research paper now claims many picture passwords in Windows 8 can be cracked. As with character-based passwords, it is easy to figure out a picture and gesture code because many people create patterns that are easy to discover. The study found that many Windows 8 users upload their own photo for use in the picture password system and then come up with touch screen gestures that center on objects in the image that stand out, such as a nose, mouth or eye if a person is in the picture. The researchers polled 685 Windows 8 users and asked them to create gesture combinations for passwords with two different pictures. 60.3 percent of the participants said they used "special objects" in the images to map out their gestures. Only 9.8 percent of those polled indicated they created gestures that had nothing to do with what was seen in their images. Bio matrices can be designed for interface logging because with the advancement of the technology PIN and Picture password are not enough for logging in security.

LITERATURE REVIEW:

In this section, we discuss work on new windows 8 security system. In Window 8 ground- breaking challengers are made for competing new technology world demands. It merges comfort and convenience of use of touch screens operating systems with the aptitudes of window PC operating system. Window 8 is not only for traditional PC,it is also functional for tablet (touch screens).

Pic.1

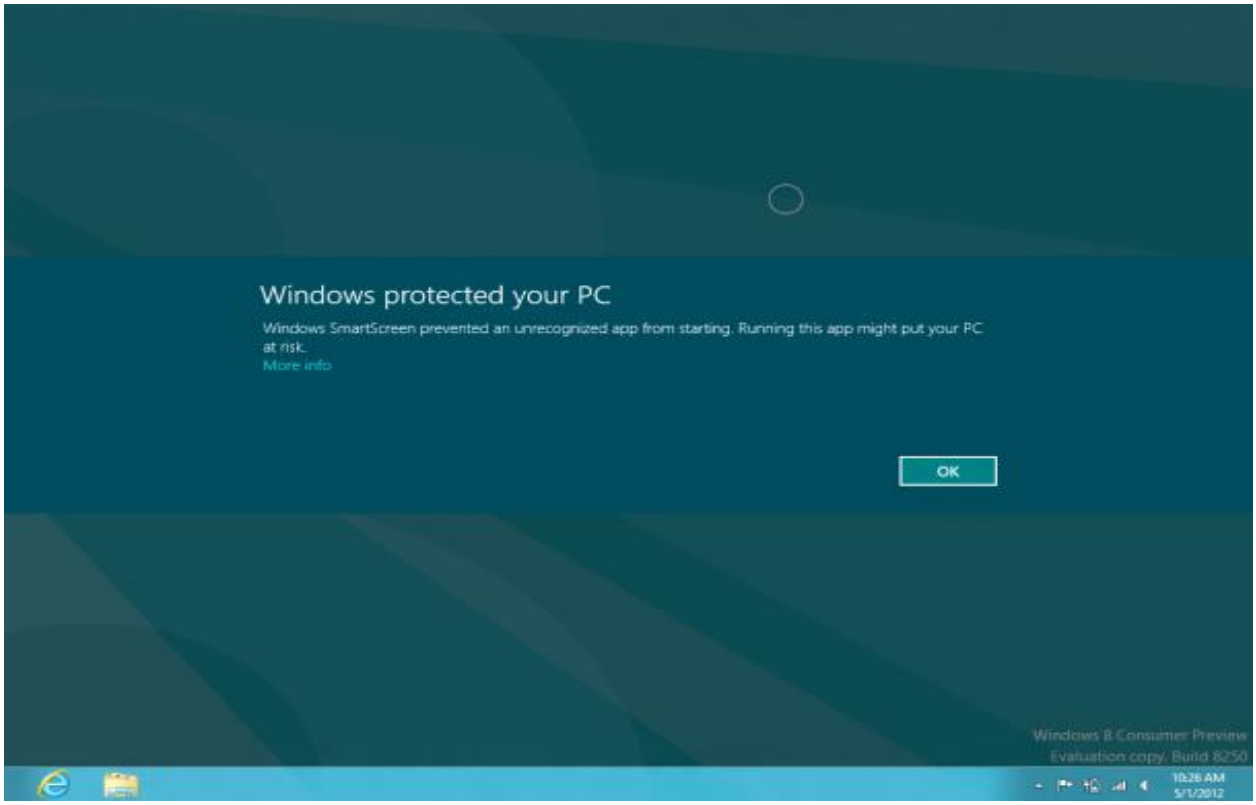
[6,5]Microsoft provides two interface modes the new modern (UI) for touch screens and the classic Desktop user interface(UI).Due to its dual functionality on single device the primary benefit is no issue for data transport, data compatibility. Day by day technology is progressing and use of tablets, smart phone and pcs are growing. Microsoft integrates various fool proof security updates in windows 8 such as new trusted boot system, App locker, Data isolation, Antivirus protection, extensive memory, Secure internet explorer 10 browser, secure boot, Anti-malware protection etc.[2,3] Window defender is comprised in window 8 which is a next version of Microsoft Security Essentials. It works as anti-virus and anti-spy-ware application.



Pic.2

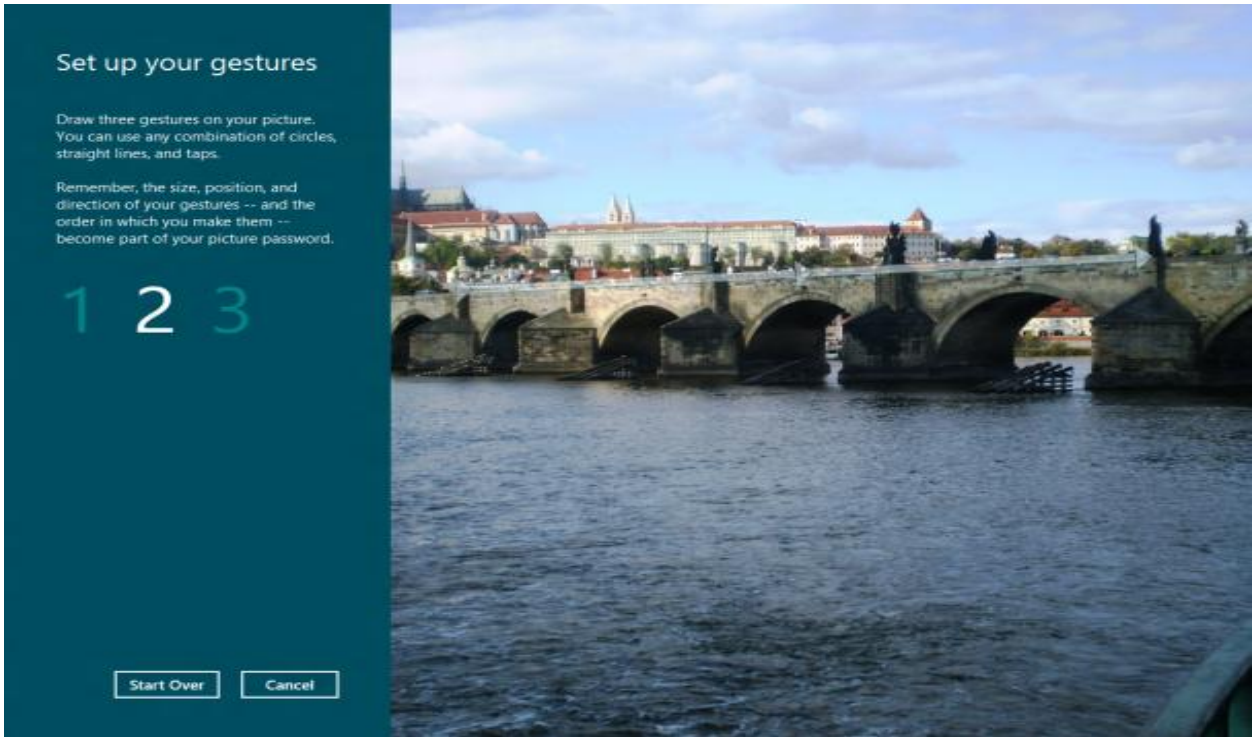
Due to this inclusion, the death of antivirus software's is predicted. However Microsoft made it easy for the users as well as for the manufacturers to restrict window defender services and use other anti-malware/ antivirus software. In past it is difficult to restrict defender. In some cases it affects the other performance of the user but window 8 solves this problem for business and customers. New boot system process is introduced called Trustworthy computing (TWC) in which Microsoft takes defensive measures by hardening the codes of operating system against rootkits and malicious codes. It works for 64-bit edition of Microsoft windows due to support issues. Microsoft practice a new kind of firmware called UEFI (Unified Extensible Firmware Interface) .It is a light weight operating system that loads windows. It replaces BIOS firmware (software embedded mother boards). IN security view point BIOS has some limitations. UEFI firmware verifies the boot loader code and allows the CPU to execute. Secure boot is another feature that prevents a computer from booting without verifying the key stored in UEFI firmware. IT only works when the boot loader code digitally signed with the certificate derived from the key stored in the UEFI firmware. Microsoft not only limit it security to boot self or boot loader. IT also adds many new features in it like ELAM (EARLY LAUNCH ANTI MALWARE).It is non-Microsoft software which runs while the operating system is loading. With ELAM combination a component which is called TPM (trusted platform module) is included. TPM records all the measurements during boot process and sent the result to the trusted external entity. The trusted external entity verifies the code and only wanted code was executed. It is necessary because through rootkits/boot kits 3 parties use mechanisms and loads itself without detection before the boot process. In window 8 special ELAM device driver soft wares are installed for anti-malware software. After that when OP fully finishes booting, the Elam handover all the control pass to desktop anti-malware program and additional scans can be done at that point. [3,4] As the technology improves the priority of attackers change. Attackers' goal is to steal user information and trash system instead of destruction. They moved up to attack business applications to web browsers to web plug-in. For this purpose window 8 introduced new utilities called smart screen filters which work with INTERNET

EXPLORER 10.Its basic purpose is to block the known malware, phishing and malicious sites for being downloaded and executed.



Pic.3

The program monitoring portion of smart screen filter is built in window itself. It works with IE, Firefox, and Chrome etc. Window 8 only stimulate user and warn it when they execute the malicious/unknown application to smart screen. For securing two modes interface touch screens and PC window 8 introduces two new account authentication methods. 1. PIN passwords. 2. Picture passwords.



Pic.4

Basically Picture passwords are made for touch screens/hand handled devices and PIN password is made for PCs. A PIN password is 4-digit code and the picture password is the series of movements and clicks also gestures captured over a user selected picture. With these entire features window 8 includes a new feature which is app locker. Now a day's organizations are facing many challenges in executing and controlling applications, to meet these challenges App locker provides the ability to specify the user who can run the specific application. It defines the privileges for executable files, scripts, window installer files and DLL files. IT helps in reducing management computing resources etc. Window 8 toughening up security at a very deepest level-memory allocation, data isolation. Our work is focused to review of window security threats for future improvements in window 8.

SUGGESTIONS:

Most work has been done for window PCs but it is necessary to remember that cyber-criminal/hackers/attacker diverting their attraction to mobile devices/tablets. Many security changes in window 8 will be discussed in this paper and many of them are still out of scope. But we will try our best to discuss all. Microsoft did well and made much effort to increase security but there are many changers still required not because of any complaints but because the scope and nature of changes to the look and the feel of operation system such as

1. Bio matrices can be designed for interface logging because with the advancement of the technology PIN and Picture password are not enough for logging in security.
2. Such Actives X controls are introduces which detect all the malware and block them automatically instead of generating messages and alerting user. If these are automatically blocked then in reaction with the passage of time development of these malware will ended.
3. It is necessary to keep in mind that now attackers attack on touch screen, on sensor though signal. So in window 9 Microsoft should work on it and must keep provide security for harmful signals, because through detection singles one must detected and attacked through malware.
4. Attackers must try to comes through the malware signals and damage the apps and web data of the user who is running in win8 touch screen devices. For this in cloud computing it is necessary to introduced one defiant bug that always connects through web and Apps that look after every harmful attack on web and Apps on run time with the propagation of signals.

CONCLUSION:

The main focus of this research article is to discuss these security threats. Antivirus protection. Window 8 also suggest many procedures and take precautionary measures like new trusted boot system, App locker, Data isolation, Antivirus protection, extensive memory, Secure internet explorer 10 browser, secure boot, Anti-malware protection to thwart. It has many enchanting features which differs window 8 from other OS. This Research help to suggest improvement in those areas which are not active in window 8 till now such as signal detection security, defiant bugs for cloud computing apps ,active X controls for malware detection, sensors security.

REFRENCES:

[1] .“Article neme”. “**Difference between Windows XP, Windows 7 and Windows 8**”.
URL:http://www.differencebetween.info/difference-between-windows-xp-windows-7-and-windows-8
Access time: 01.00AM ,
Access date:19-03-2014
[2]. “Article name”.“AppLocker”.

URL:http://technet.microsoft.com/en-us/windows/dd320283.aspx

Access time:12.00 AM

Access date:19-03-2014

[3].**"**ErsiGeier**"**,Windows 8: Put its hidden security features to work!

URL:http://www.pcworld.com/article/2027593/windows-8-put-its-hidden-security-features-to-work-.html ,
Access time: 12.25AM
Access date:19-03-2014

[4]." Fred Pullen**"**, "**Internet Explorer 10 Provides Safer Browsing**".

URL: http://blogs.windows.com/ie/b/ie/archive/2013/06/21/internet-explorer-10-provides-safer-browsing.aspx ,

Access time:12.30AM
Access date:19-03-2014

[5]. " Eric Geier", "**Windows 8 Security: What's New**".

URL: http://www.pcworld.com/article/255776/windows_8_security_whats_new.html
Access time: 5:00
Access date: 23-02-2014

[6]. "**NEIL J. RUBENKING**", "**Windows 8: Secure at the Deepest Level**".

URL:http://www.pcmag.com/article2/0,2817,2408016,00.asp ,
Access time:4:30,
Access date: 23-02-2014

[7]. G. KALPANA, K.BARKHA, "**A COMPARATIVE STUDY OF TWO OPERATING SYSTEMS:WINDOWS 7 AND WINDOWS 8**",Journal of contemporary research, EISSN: 2320, ISSN: 2319-5789, Jaipur institute india, octobr 2013.

[8]. TECHNOLOGY BUSINEESSRESEARCH","**" Windows 8 is Changing the Game**" , Windows 8 Game Changer White Paper | January 2013