Journal of Pharmacognosy and Phytochemistry
Available online at www.phytojournal.com

E-ISSN: 2278-4136
P-ISSN: 2349-8234
JPP 2019; SP3: 93-98

Saurabh
Research Scholar, Ph.D (CSE), Bhagwant University, Ajmer, Rajasthan, India.

Dr. Kalpana Sharma
Associate Professor & HOD(CSE), Bhagwant University, Ajmer, Rajasthan, India.

Correspondence
Saurabh
Research Scholar, Ph.D (CSE), Bhagwant University, Ajmer, Rajasthan, India.

(Special Issue- 3)
National Conference
"Sustainable Agriculture and Recent Trends in Science & Technology"
(February 22nd & 23rd, 2019)

A security framework of the future generation based trusted operating systems to overcome from the malicious and illegal threats

Saurabh and Dr. Kalpana Sharma

Abstract
The research paper presents robust means of the next generation-based information operating systems for building secure foundation to abolish unauthorized threats. There are various pitfalls in the existing and present operating systems. To keep the information safe in each respect from the wrong hands of the intruders is the major concern to eradicate from various kinds of unauthorized threats. Security deals with the avoidance and discovery of illegal conduct by the unauthorized users. There are still various flaws in gaining the complete security solutions of the operating systems. The overall aim is to secure data and information so that intruders can't gain malicious accessibility of the system. Unfortunately, due to the limits of various kinds of powerful and robust features in the existing generation of operating systems, many traditional security methods cannot be applied to build a hundred percent full proof security framework. This paper addresses this issue by introducing a secure framework to overcome from the malicious and illegal threats. This qualitative study focuses on describing a needed part of protection in the operating systems of the next generation. The research work deals the prevention and detection of unauthorized threats with an aim to produce the next generation based secure and powerful operating systems. The requirement of overall complete protection, reliability and enforcement of guarantee are main provisions of a trusted operating system. The most important qualities of trusted operating systems are represented to eliminate illegal threats.

Keywords: robust, operating systems, security, future generation, framework.

Introduction
The subsequent generation of operating systems ca dominate the subsequent twenty years of computing as comparison with the current generation of operating systems. It'll be all regarding remodelling the apps and therefore the interactions to influence the artificial intelligence capabilities of the device and therefore the information of the user to set up actions and perceive the purpose. There are various kinds of errors with existing backbones and it could be unsafe due to major unavoidable omissions of existing operating systems. The current backbones only work through computer architectures. Anyone can see a lot of omissions in WINDOWS and UNIX code [1]. Artificial Intelligence provides the advanced features utilizing its knowledge by a computer or a machine so as to determine advanced issues with no trouble. Strong AI could speak to human personalities in future though then again Weak AI can be made to go about as though they are insightful. Taking superior judgments at right time by handling complex issues is the outcome of intelligent systems. Intelligent System helps in picking the best application to open a record, reports, Audio, Image and Video. It will lessen the time and will pick the most ideal yields to be shown in an OS according to client's requirement. The expert systems will offer assistance in helping the client in numerous ways such as prompting and giving enlightening to the issues such as storage management, break downs in OS etc. Expert systems can be utilized to construct an improved Client Interface as well [2, 3].
Fuzzy logic systems receive imperfect and incorrect input. Its approach imitates the approach of higher cognitive process in humans. The components of Operating System

such as process management, file management, storage management, distributed system management, etc., are very useful while handling the fuzzy information. A fuzzy logic system makes the systems work expeditiously and economically [4, 5]. The natural neural network of human system has impressed artificial neural networks. It helps in speech recognition, speech classification, text to speech conversion, Pattern Recognition in biometric identification, optical character recognition, etc. The feature of ANN like Pattern Recognition in facial identification is often used for security of the OS. Natural Language Processing can facilitate in understanding the Artificial Intelligence OS. It can facilitate in analyzing them and providing the suitable output if inputs are not in an under stable format. Natural language processing works on the premise of Speech and text. This may facilitate the user to command the OS although the command isn't bound [6]. The powerful computerized technology should develop such kind of future generation operating systems that help as intelligent assistant, electronic adviser and supply engines. The artificial intelligence field can play its most important role in this direction. Its functions include observation, pattern learning and identification, forecasting, context priming, consideration, generalization, categorization, remembrance judgment and conduct [7].

Literature Review

Jain A. K. have assured that user authentication is extensively based on the use of passwords, but the security problems related to passwords are going to be more and more severe. Password sniffing and complexity to manage password are the main reasons because the users accessing resources are rising day by day. User requires security only with password-based security. This mechanism is very hard to implement. Biometrics has very significant role in this system. Users have added security as it depends on what users have rather than what others possess, since it is the combination of recognizing both fingerprint and password [8].

Ravi S. Sandhu and Samaratiy have narrated security services. The access matrix models have been reassessed and they described different approaches to implement the access matrix in practical systems. Finally, they have briefly described the administration of access control. Access controls provides various kinds of powerful control features. According to the system requirement, various norms and standards can be considered according to criteria specified by that system [9].

Robert and Watson have described that the operating system security depends primarily on the variety of applied access-control models. Operating-system developers must assure device vendors. Operating system vendors studied the trusted operating system and had observed that mandatory access-control experienced from bad features. Likewise, it was observed that many capable new security models are in research, each with some known feasibility [10].

Robert *et al*. have narrated discretionary access control. It was stated that access control could be used more powerfully when applied. The design was proposed of three tired mechanism. In the model, the object's creator, called as the owner, going to decide the properties for the object. The object it could be any file, any application, any hardware resource, etc. It was provided considerable flexibility for an object to the user who created that object. They proposed three layers as the first layer was general access control layer, second was parameterization and third was set of associated object and associated set of permissions respectively [11].

Tiwari *et al*. has suggested similar concept for cloud security. Cloud computing presents the platform for providing computing resources over the Internet. According to ones needs, user prefers to use a service of the Internet. It is possible for the user to store data or information on cloud or using its applications at another location. Doing so, may give rise to certain privacy implications [12].

Michel Gien *et al* concluded that the popular operating system UNIX can't satisfy the expectations of system developers if it keeps to grow in complexity, without a nicely-defined modular architecture based on simple principles. The complexity of Operating systems is increasing continuously. He pointed at UNIX evolution that various tendencies are pulling it far away from its origin. As extra functionality is usually demanded, it's far unavoidable that further variations should be more complicated. This growing complexity is diminishing the original benefits such as simplicity and portability. In place of evolving toward greater portability, new releases require excessive efforts to put in force on new structures [13].

Yanbing Li *et al* analyzed the possibilities and challenges posed with the aid of real-time operating systems. In real-time systems the right capability assumes each the correctness of the output as well as the appropriate timing behaviour of the system. A deadline is the time at which a task must end its execution after being initiated. Real-time operating systems have been used in many programs from vehicle, ship and aircraft electronics to wireless and optical communication system, clinical instrumentations, multimedia, internet and even home equipments, factory automation, economic transaction processing and video game machines [14].

Munsee and Lee worked on the safety and privacy of Linux operating system. A lot of recognition has been gained by this open source operating system. For a spread of tasks more and more human beings are using it. Linux has grown to emerge as one of the international's maximum popular running systems since its origin. Students love it for the price and the open source accessibility. Network supervisors love it due to the fact it can communicate with many different operating structures and run on honestly with any processor. Internet providers adore it due to the local internet help that it presents. Inspite of all of the strengths of Linux, many declare that Linux is not powerful due to its open source accessibility. Some experience that the open code makes it less complicated for attackers to discover and misuse flaws in the working device. They pointed out a few attacks such as malicious program attacks, worm applications, direct access or nearby hacking, buffer overflows and many others which are being used against Linux. They narrated that attackers can without difficulty search through the Linux code for vulnerabilities and looking to misuse them. Some other system structures that don't have open source are not as effortlessly probed for flaws that can be exploited. They advised that for you to preserve Linux running machine secured, we want to continue installing patches and also configure Linux absolutely [15].

Andrew Baumann *et al* observed that dynamic update is a mechanism that lets in software updates and patches to be applied to a living machine without lack of provider or down-time. Operating systems might advantage from dynamic update, however require particular needs on any implementation of such features. These needs stem from the event-pushed nature of operating systems, from their constrained run-time execution surroundings, and from their

function in concurrently servicing a couple of clients. Dynamically updatable systems produce other characteristics. Such systems offer an excellent prototyping environment. In addition, a few user constraints save you the machine from ever being shut down. In this way, customers can get new capability into the machine most effectively via performing a dynamic update. Therefore, a dynamic update mechanism that allows patches and updates to be carried out to a running system without lack of service [16].

Habib and Zubair evaluated the safety of windows mobile working device. The researchers proved that the hassle with clever phone running system is that a recognised vulnerability has a tendency to exist for a longer time due to unavailability of patches. As a consequence they can be an clean target to take advantage of. To reveal the vulnerabilities on the network level, they accomplished penetration testing on Windows cellular 6.1 running system. In addition they pointed out that Windows cellular does offer a security infrastructure that uses safety regulations with code signing, but it isn't not possible to bypass the safety regulations. The researchers concluded that these cellular running structures nevertheless have an extended way to be able to prove themselves [17].

Fang *et al* stated that Google Chrome running device is evolved by Google that runs on specialized hardware. He talked about that this is a elementary flaw of Chrome and doubtlessly all cloud based working structures. The Chrome is based totally at the open source chromium structure. This running system differs from traditional running structures due to its layout nature. This running device is designed to work specifically with internet-based applications. The circulation in the direction of cloud computing has been evolving. This means that all of your information are stored online inside the cloud to allow you to retrieve it from anywhere. This model will help to broaden a better overall experience and recognition on growing an os with advanced velocity, protection and ease. However, due to the fact this is open and connected, one may additionally argue this is less secure than physical computer systems. Now a days, the numbers of attacks at the net have grown unexpectedly. Stealing password via phishing attacks is presently less difficult than stealing it physically or breaking the cryptography. If attackers succeed in getting access to the user's password, the attacker can easily access all of the facts without even desiring to have the physical machine. He pointed out that this is an essential flaw of Chrome os and potentially all cloud-based systems. He defined that Chrome os does not deal with phishing, therefore, it does not provide any stronger assurance [18].

Qurat-ul-Ain Malik *et al* offered a comprehensive survey report for the requirements and evolutions of rising operating systems for the next generation. OS researches traditionally encompass including new functions to the running system. Operating systems are the maximum complex piece of software in a pc device, which contains millions of lines of code. These days's running device research is directed at finding new ways to shape the operating device to be able to increase its flexibility, allowing it to adapt to modifications as per requirements [19].

Ritika Pandhi delivered protection icons which perform effectively with graphical user interface based working systems in determining patterns, accuracy, privacy and reducing security problems. A robust GUI based system has to offer a trusted path and it must allow integrity, validation, and secrecy of the transmitted records. The safety sample provided how to manage the retrieval to input/output devices consisting of keyboard, mouse, and display. Diverse factors of protected graphical user interface-based systems were analyzed as security styles [20].

Joshua Harry Berlin concluded that as per the latest estimates, Windows at greater than 50 million lines of code and the Linux kernel now exceeds 15 million lines of code. With codebases of this length, it's nearly assured that bugs and security defects will exist and OS developers frequently launch patches to repair errors as they are determined. Due to such unavoidable threats, regardless of how well applications are designed, a single flaw or compromise in a running machine can bring in the compromise of each application. The quantity of cash and attempt spent on the prevention of such kind of malwares and viruses across popular computing structures today is a proof of such vulnerabilities [21].

Paul Krzyzanowski *et al* analyzed that older operating systems were in huge size. Every system-related characteristic was done by using one block of code that turned into part of the running machine. As the functionality of the system grew, the operating system software became increasingly hard to maintain and understand, so operating system software began to get modular. A modular design allows some of the modules of the operating system to be replaced or mounted as per the requirements. The modules of Linux are an instance of it. The later trend was to keep the kernel of the running system small and flow as much as possible into separate programs that have the accurate security privileges. The kernel will invoke separate threads to address things. This technique is called a microkernel [22].

Gage Eads *et al* determined at the capability to satisfy the quality of service requirements. Today's users prefer touchy operation from super multimedia and interactive packages, which offer responsive user interfaces and meet stringent real-time surety. Moreover, the want for records security and accessibility leads to a number of compute-intensive packages, inclusive of anti-virus scanners or report indexers, executing behind the scenes and likely interfering with interactive and multimedia packages. Thus, a research challenge is familiar with how an operating system ought to best assist this dynamically changing and complicated mix of packages. Addressing this challenge means being capable of fulfilling the quality of service requirements while making green use of computing assets [23].

Literature Summary - From literature, it is observed that users carry out many important, private and sensitive operations on the system. Users work with their sensitive data on the operating system. So it is the responsibility of the operating system to ensure the security level, it is providing to users for their operations and data. As windows operating system is not designed primarily by considering security as the main issue. Microsoft invested much more in this design and it is not possible now to redesign from starch. Different approaches are proposed for securing windows operating system. Security relies on different elements as authentication, auditing, confidentiality, integrity. At the first level, for secure authentication, user generally relies on password-based security. It is in wide use. There is a need to work on these aspects to achieve more efficient security by keeping user, user applications and users' data as main perspective. There are various forms of benefits for users provided by the Windows OS like games, drivers, integrated

environments, one product for all, technical support for its users, diverse networking capabilities, better graphical user interface, report sharing, convenient to use, and powerful anti-viruses etc. Apart from a lot of these large variety of benefits, it has a few cons additionally. For example, greater hardware necessities because of installation of anti-viruses and malware, lacking security device, costly system and much less portability. Due to its closed-source nature, one cannot adjust or add any functions to the working system. Therefore, the robustness features are also lacking someplace. Windows is extra vulnerable to cyber assaults and hacking also. Thus, anti-viruses need to be installed and update once in a while.

Goals of future generation based operating systems

The present day running operating systems begin with their machine device, after which connect it to the consumer. Their aim is to package the processor, memory, disk and other peripherals with the intention to manipulate them remotely. The essential function of knowledge navigation is that you will have the interaction with the machine by talking and the computer will act as an sensible navigator via deciphering the voice and looking for to the person requirements. These working systems will be multi-touch, self-automatic and self-healing. It permits a person to have interaction with a device with a couple of finger at a time. The self-automatic operating systems are that merely a consumer feed the data to the system and rest of the work is achieved with the aid of operating systems. Thus, user is now not wanted in these days running machines. The major possessions of self-healing devices is that it self-diagnosis itself [24, 25, 26, 27, 28].

Critical aspects of next generation operating systems

A number of the important aspects of recent era working operating system structures to support such traits of real-time distribution, multiprocessing systems and availability of open system architectures include: efficient real-time foundations, optimised interprocess and interprocessor communications, user-transparent allotment of possessions, portability throughout hardware architectures from single processor to multiprocessors in open environments, interoperability of a huge variety of running environments from real time to fault-tolerant in a single transparent and comfortable allotted environment, scalability and versatility in design and in run-time useful resource utilization. A framework for working operating system modernization, improvement, debugging, continuation, extension, integration and absolute conformance to enterprise requirements is also needed [29, 30, 33, 34, 35].

Objectives of the research work

1. To investigate the various security features of the most widespread and successful operating systems.
2. To investigate the all types of security imperfections in operating systems.
3. To protect the city's financial investment in computer systems and to ensure stable computer operations.
4. To evaluate broadband and WiFi opportunities including fiber optic connections throughout the city's wide-area network.
5. To investigate all those strategies which are based on the principle of Quality of Service.
6. To make use of the best services and features of Cloud Computing.
7. To evaluate those strategies that enhances security and robustness.
8. To provide public access to GIS maps and drawings.
9. To evaluate opportunities for E-government, e.g. online business licenses, online permitting.
10. To maintain suitable and important public amenities in an economical manner.
11. To assist in updating the emergency operations and disaster recovery plan.
12. To find out the best possible outcomes of recently established operating system.
13. To build a trusted operating system for the convenience of humans at large.
14. To attain the outcomes by making the use of Artificial Intelligence based Operating Systems.
15. To verify the security at all levels.
16. Need of additional simplification, multiprocessing, similar hardware architectures and extra flexibility at all levels.
17. Explore the feasibility of a new framework and design an architecture for generic web-based distributed control systems.
18. Provision of obligatory protection, reliable path and enforcement of guarantee are primary necessities of a robust and trusted OS.
19. Techniques for caching the results of dynamically generated Web content, and a wide-area security system that provides high performance and availability despite network limitations.
20. Portability of numerous applications and retaining backup for all programs.

Diversity among cloud operating systems and general operating systems

The existing operating systems do not perform nicely in a huge-region due to implicit assumptions which include indirect supposition like homogeneous hosts and fairly excessive overall performance networks. The coming generation based operating systems should offer comfy behaviour with fault tolerance abilities and warranted absolute conformance to enterprise requirements. Not like conventional operating systems, running structures cloud working system is primarily a browser based operating device. The difference among cloud operating systems and general operating systems is that the general operating running structures manages hardware and works as a platform in order that the underlying hardware may be used successfully by using the application software. A device executing on cloud operating system has no operating systems established on it in actual. The cloud operating system is a simplified working machine that permits the user to carry out many simple duties without booting a machine. The Cloud structures can be used as a standalone operating system in addition to collectively with different operating systems [36, 37].

Assessment of existing kernels with future generation operating systems

The present kernel architectures cannot accomplish the wishes of this current modernized digital era due to complex structures and irregular modular structure. Despite with all of the strengths of Linux, many researchers claim that Linux isn't comfortable because of its open source nature. Some experience that the open source code makes it less complicated for attackers to discover and take advantage of flaws inside the running system. They mentioned a few assaults which are getting used against Linux along with

computer virus assaults, worm programs, direct physical retrieval or local hacking, buffer overflows and many others. Other operating systems do not have default administrator access or root access, whereas Windows provide access rights to all of the applications. That's why, Windows is more hazardous or susceptible to viruses, worms etc. The next generation operating systems need to provide secure behaviour with fault tolerance competencies and guaranteed absolute conformance to industry requirements. The requirement of future generation running operating system structures are scalability and versatility in layout, run-time useful resources usage and obvious distribution of operating device offerings [38].

Illegal vulnerabilities of existing operating systems

A trusted and secure operating system must not permit spiteful programs to run as most of the viruses include. exe extension. In Windows operating system, users have administrator entrance rights by default. That is why the viruses spread in Windows OS eventually. But Windows assert that Linux is full of safety problems, insufficient technical assist, inconsistent interfaces and lots of illegal vulnerability. Linux developers however, accuse Windows of being extra susceptible to assault, volatile, rigid, and of low first-class standards. An assailant could take complete control of an entire system. An assailant can observe the daily traffic to learn user's endorsement and consent credentials. Spoofing is an assault by which an assailant gains admittance to the certificate used by the end user for verification. Risk is recognized by detecting the hazard and susceptibility. Therefore, trusted operating systems should handle many obligations and trustworthy set of characteristics together with an appropriate degree of assurance that the features have been assembled and implemented appropriately [39].

Trusted and protected operating systems require secure identification of individuals and each individual ought to be uniquely recognized. The robust operating system should control the resource allocation of multiple processes concurrently. Thus, reusable resource objects must be cautiously guarded. Highly trusted operating systems must check process retrieval carefully in order to provide meaningful results. One way for a malicious user to achieve advantage of illegal access is to "spoof" users, making them think they are exchanging a few words with a genuine defensive enforcement system when in fact their keystrokes and commands are being seized and observed. The audit log must clearly be recorded and protected from outsiders. The trusted operating systems should include all these design considerations to guarantee complete secrecy, truthfulness, and accessibility of the system [40].

Qualities of a trusted operating system

The qualities that can build a secure framework of a trusted operating system are as under:

a. Identification and Authentication - Identification means that you should be able to tell who requests access to an object. In other words, establishing an identity and then verify or authenticate it.
b. Obligatory and discretionary control of access - Individual judgments are observed by the possessor of an object. In other words, which information is available to whom and the user cannot change the rights of access.
c. Object Reuse Protection - The reuse of objects is one way a computer system maintains its efficiency. OS controls the allocation of resources and the operating system allows the next user or program to access the resource as a resource is freed for use by other users.
d. Complete Mediation - All access must be monitored. Access to files only if the attack acquires access via memory or an external port or network or a covert channel is not sufficient to control access. In this way, complete mediation is carried out.
e. Trusted Path - Trusted Path One way for a malicious user to gain inappropriate access is to "spoof "users, who believe they communicate with a legitimate security enforcement system when observations are actually intercepted and analyzed.
f. Accountability and Audit - Accountability usually involves keeping a record of security-related events, listing each event and the one who was adding, deleting or changing the event. It must be protected against outsiders and any security-related event must be recorded.
g. Intrusion Detection -Intrusion detection software builds normal system use patterns, triggering an alarm whenever the use appears abnormal. There is a primitive degree of intrusion detection software in some trusted operating systems [31, 32].

Conclusion

In this paper, the research work represents a qualitative study of various generations of operating systems, their applications used in the wide area and performance of one generation over other. This study outlines a comparative qualitative study of various generations of operating systems and their applications used in the broad area. The most important objectives of the research work are represented to eliminate illegal threats. The research work deals the prevention and detection of unauthorized threats with an aim to produce the next generation based secure and powerful operating systems. The Operating System that doesn't have AI will certainly be of no use. That is, it lacks a brain that is artificially intelligent. The humans would desire a system that may act as our personal assistant. The goal of computing is to form systems whose intelligence equals or surpasses humans. If this goal is achieved then we'll have AI primarily based OS additionally. Therefore, development of the forthcoming artificial intelligence-based OS is an important concept. Constructing a trusted operating system that can often defend towards assaults and provide safe and comfortable computing surroundings is the need of this century. Various security mechanisms and solutions are needed to provide secure next generation based operating systems. For this reason, a reliable safety framework and a multilevel safe computing environment can be obtained only by developing next generation based efficient and protected operating systems.

References

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Concepts, Wiley India Edition, 2012, ISBN:978-81-265-2051-0
2. Andrew S. Tanenbaum, Modern Operating System, 2008.
3. Dhamdhere DM. "Operating Systems: Concept based Approach", 2nd Edition, Tata McGraw Hill, India, 2003.
4. Cloud as an evolutionary operating system, Omesh Kumar, ICNICT 2012.
5. http://www.csi-india.org/Communications/CSIC_feb_2017.pdf

6. Tanenbaum AS. Modem Operating Systerns, Prentice HaH, 2001.
7. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne. Operating System Concepts, Wiley India Edition, 2012, ISBN:978-81-265-2051-0
8. Jain AK *et al*. A Comprehensive Study on Risk, Threat & vulnerability in an Operating System and Online Application Software, Department of CSE, Stamford University.
9. Ravi S, Sandhu Samaratiy *et al*. A Comparison of Window 8 and Linux Operating System (Android) Security for Mobile Computing, Department of Information Technology, Hazara University.
10. Robert Watson *et al*. An Introduction to Information System Risk Management. SANS Institute InfoSec Reading Room, 2006.
11. Robert *et al*. A Preliminary Review on Trusted Operating System, H.V.P. M's College Of Engineering And Technology, Amravati.
12. Tiwari *et al*, Security considerations in a multihomed operating systems, Silesian University of Technology, 2016.
13. Next Generation Operating Systems Architecture, Michel Gien, Chorus syste`mes, 1991.
14. Real-time operating systems for embedded computing, Yanbing Li, *et al*, 1997.
15. Munsee CL, Lee C. Security Evaluation of the Linux Operating System. Oregon: Oregon State University, Corvallis, 2002.
16. Providing dynamic update in an Operating System, Andrew Baumann, Gernot Heiser, University of New South Wales & National ICT Australia, 2005.
17. Habib SM, Zubair S. Security Evaluation of the Windows Mobile Operating System. Goteborg, Sweden: Chalmers University of Technology, 2009.
18. Fang K, Hanus D, Zheng Y. Security of Google Chromebook. Massachuset Institute of Technology Cambridge, 2010.
19. Modern Trends used in Operating Systems for high speed computing applications, Qurat-ul-Ain Malik *et al*., (IJCSE) International Journal on Computer Science and Engineering, 2010.
20. Framework for security and integration for GUI-based Operating System, Ritika Pandhi, International Journal of Information and Communication Technology Research, 2012.
21. Secure User I/O for Applications on an untrusted Operating System, Joshua Harry Berlin, 2014.
22. Paul Krzyzanowski, Operating System Concepts, Rutgers University, 2014.
23. Building an adaptive operating system for predictability and efficiency, Gage Eads *et al*., 2014.
24. W Stallings, Operating Systems, Fourth Edition, Prentice Hall, 2000.
25. Tanenbaum A. Modern Operating Systems, 3rd Edition, Prentice Hall, 2007.
26. William Stallings, Operating Systems: Internals and Design Principles, 7th ed, Prentice Hall, 2011.
27. Deital HM. An Introduction to Operating Systems, Rev. 1st ed. Reading, MA: Addition-Wesley, 1984.
28. Dhamdhere DM. Operating Systems: Concept based Approach, 2nd Edition, Tata McGraw Hill, India, 2003.
29. Stallings William. Operating Systems: Internals and Design Principles, 4th Edition, Prentice Hall, India, 2004.
30. Stallings W. Cryptography and Network Security: Principles and Practice, Third Edition, Prentice Hall, 2003.
31. Tanenbaum AS, Modem Operating Systerns, Prentice HaH, 2001.
32. Rani Shriram Joshi *et al*. A Preliminary Review on Trusted Operating System, 2015.
33. Saxena Ashutosh. Reliable and Secure Operating Systems. CSI Communications, 2017.
34. Wang W, Li Z, Owens R, Bhargava B. Secure and efficient access to Outsourced data, ACM workshop on Cloud computing security. Chicago Illinois. USA; November, 2009.
35. Mohammed Faez Al-Jaberi, Anazida Zainal. Data integrity and privacy model in cloud computing. ISBAST, 2014.
36. Chowdhury Afreen *et al*. A Comprehensive Study on Risk, Threat & vulnerability in an Operating System and Online Application Software. IJARCSSE, 2012.
37. Nazeer Sumat *et al*. A Comparison of Window 8 and Linux Operating System (Android) Security for Mobile Computing. IJC, 2015.
38. Dhamdhere DM *et al*. Operating Systems: Concept based Approach, 2nd ed. Tata McGraw Hill: India, 2003.
39. Stallings William *et al*. Operating Systems: Internals and Design Principles, 7th ed. Prentice Hall: India, 2011.
40. Stallings William *et al*. Cryptography and Network Security: Principles and Practice, 3rd ed. Prentice Hall: India, 2003.