Emerging Issues in Cyberspace and Virtual Reality

Peter Joseph Moven
Email: peter.moven@iaue.edu.ng
https://doi.org/10.56201/rjmcit.vol.12.no8.2026.pg44.54

Abstract
The paper examines emerging issues in cyberspace and virtual reality, focusing on the opportunities, challenges and implications of these technologies for contemporary society. It discusses the growing influence of digital technologies, including mobile connectivity, cloud computing, artificial intelligence, robotics, virtual reality and augmented reality, on communication, education, commerce and organisational activities. The paper adopts a conceptual approach, drawing on existing literature and the theory of technological determinism to explain how technological developments influence human behaviour, social interaction and institutional practices. The discussion reveals that emerging technologies facilitate information access, improve communication, support service delivery and create new opportunities for learning and innovation. However, their increasing adoption also presents significant challenges, including cybercrime, online fraud, privacy violations, cybersecurity threats and digital exclusion. The paper further highlights the importance of responsible technology adoption, effective governance, digital literacy and institutional accountability in addressing these challenges. It recommends that government agencies, educational institutions and technology providers strengthen cybersecurity measures, protect users' personal information, promote digital-literacy programmes and establish clear policies for the ethical and responsible use of emerging technologies. The paper concludes that cyberspace and virtual reality offer considerable benefits for social and economic development, but their long-term value depends on accessible infrastructure, appropriate regulation and sustained efforts to ensure safe, inclusive and accountable digital practices.

Keywords: *Cyberspace, virtual reality, augmented reality, emerging technologies, cybersecurity, technological determinism.*

Introduction

It is axiomatic that the present age of humankind is a computer technology age where virtually all aspect of human activities are computerized or computer-based and basic tasks in most spheres of human endeavor are enhanced or better executed via the instrumentality of modern or state of the art computer technology (Adnan, 2010). It is also crystal clear that the whole wide world is presently in a state of constant transformation courtesy of the advent of advanced computer technology breakthroughs that are systematically revolutionizing the human society (Adnan, 2010). The interesting thing about today's computer technology advancement orchestrated by competitive wizards, working rigorously, independently or collaboratively, all over the globe but driven by the positive goal of making the world a better place, is the quick succession of contemporary computer-based innovations.

Cyber systems provide flexibility leading to its illicit use with the government framed internet

policy (Pfaffenberger, 2000). Internet is making life easy with economy activities like buying, selling, online transactions and social networking brings along many threats. The internet has simplified business processes such as sorting, summarizing, coding, editing. Cyberspace refers to a "global and dynamic domain" (subject to constant change) characterized by the combined use of electronics and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate, inform and disrupt physical resources (Pfaffenberger, 2000).

The Cyberspace can also be seen as a "notional environment in which communication over computer networks occurs" (Vakharia, Mishra & Kumar, 2013). The word became popular in the 1990s when the uses of the Internet, networking and digital communication were all growing drastically and the term was able to represent the many new ideas and phenomena that is emerging (Vakharia, Mishra & Kumar, 2013). However, it is through the same cyber networks which intrude and attack our privacy, economic, social life in a way which is harmful. It has also brought unintended consequences such as criminal activities, spamming, credit card frauds, phishing, and ATM fraud. Some scholars have interestingly argued that "In the internet nobody knows you are a dog" (Vakharia, Mishra & Kumar, 2013). This raises some legal issues and concerns. IT revolution has brought about a wide array of aides and conveniences that have indelibly influenced modern communication travel, security and commerce. The massive gains brought by the information age are not perfect, with the pervasive correlation of human activity with electronic resources and infrastructure there is a crucial vulnerability, which is the ever-present risk of abuse, insidious manipulation and sabotage of computer and computer networks.

Virtual reality (VR) and augmented reality (AR) represent important developments in the ways people experience and interact with digital information. VR creates computer-generated environments in which users can experience simulated spaces, while AR introduces digital information into a view of the physical environment. These technologies have applications in education, professional training, entertainment, simulation and the visualisation of complex processes. Their significance extends beyond recreation because immersive technologies can provide opportunities for practical learning and the exploration of situations that may be difficult, expensive or unsafe to reproduce physically. However, their adoption also raises questions about equipment costs, accessibility, user safety, data collection and the suitability of immersive experiences for particular purposes. Artificial intelligence, robotics and data analytics further complicate this environment by enabling automated processes, predictive analysis and increasingly personalised digital experiences. Such developments require critical examination of the relationship between technological capability, human judgement and social responsibility.

Despite the benefits of emerging technologies, their expansion has intensified concerns about cybersecurity, misinformation, digital inequality, privacy and accountability. Anah (2002), whose cited work addresses cybercrime in Nigeria, provides a relevant starting point for considering the implications of digital criminal activity, although the complete bibliographic details of that publication require verification before academic submission. The increasing dependence on connected systems means that technological failures and security breaches can affect individuals, businesses and public institutions. Furthermore, unequal access to connectivity, devices and digital skills may prevent some populations from benefiting fully from technological innovation. These concerns establish the need for a balanced examination of the major developments in cyberspace and virtual reality, the opportunities they create, the challenges they introduce and the measures required to promote their responsible use. Accordingly, this paper examines emerging technological trends, discusses their benefits and risks, and identifies practical measures for strengthening digital security, inclusion and accountability.

Conceptual Framework

Cyberspace

Cyberspace can be conceptualised as the interconnected digital environment in which computer networks, internet-based services, connected devices and digital information support communication and other forms of human activity. It includes websites, social networking platforms, cloud services, electronic payment systems and digital infrastructures that enable information to be created, transmitted, stored and processed. Pfaffenberger (2000) provides a computing terminology reference that helps situate the technical language associated with computer networks and digital systems. In contemporary society, cyberspace functions as an environment for interpersonal communication, commercial transactions, education, public information and organisational coordination. Its influence is therefore not restricted to the technical operation of computers but extends to the social and institutional relationships established through digital interaction.

The development of cyberspace has increased the speed, reach and flexibility of communication. Individuals can maintain relationships across geographical boundaries, organisations can coordinate activities remotely, and businesses can reach customers through online platforms. Cloud-based services and mobile connectivity have further reduced the need for users to depend exclusively on physical locations or locally installed computing resources. These capabilities can improve access to information and support new forms of collaboration. However, the interconnected nature of cyberspace also creates opportunities for cybercriminals to exploit weak passwords, insecure networks, software vulnerabilities and inadequate data-protection practices. Anah (2002) addresses cybercrime in the Nigerian context in the cited reference, making the subject relevant to discussions of digital safety, although specific claims should be checked against the original publication.

Trends in Cyberspace and Virtual Reality

1. Mobility

As broadband mobile connectivity to the internet spreads and the scope and availability of IT resources such as software expands, smartphones and tablets are morphing into seamlessly integrated devices that are indispensable in the workplace (Korchmaros *et al*, 2013). Businesses and their workforces have fingertip access to communication and information whenever and wherever they need it. People are increasingly interconnected in their personal and professional lives and recent tablet and smartphone incarnations, fonepads and phablets, have the potential to enhance communications and connectivity further and to blur barriers across the work and personal spheres, not to mention geographic boundaries (Korchmaros *et al*, 2013).

Reliable broadband networks are essential to the exploitation of the ever-expanding mobile ecosystem. For countries, investment can be crucial to economic recovery, as it contributes to gross domestic product, stimulates employment and raises productivity. A recent survey of ACCA and IMA members identified mobile technology as the most important for business in the years ahead. Accountants will need to:

1. identify and deploy effective mobile solutions that can work in the decade ahead
2. manage the transition to full mobility in a consistent and safe manner
3. consider the potential offered by an interconnected internet of things, from mobile devices to appliances, cars, and industrial equipment.

According to Usman and Shah (2013), the challenges of mobility:

1. The profession must understand which services are best delivered 'on the move'.
2. Security concerns on potential theft or loss of information.
3. Implementing the right mobile technology at the right time is paramount.
4. Working patterns will change as the internet becomes more pervasive.

2. Cloud

The internet has evolved from a platform that connects millions of computers, into the network of interactive computing platforms now known as 'the cloud' (Usman and Shah, 2013). It can deliver IT resources (such as software applications, computing power and data storage) flexibly and efficiently online, as a service. These resources can be scaled up and down to meet demand, and accessed anytime, anywhere, from fixed and mobile devices. Numerous services are offered from 'public clouds', businesses are creating their own 'private clouds' and these are evolving into 'hybrid clouds' that meet spikes in demand with public cloud services (Rahman & Lackey, 2013). The organisations work with and for, are exploiting the cloud - in business, practice and the third sector. Accounting systems were among the first software to become available online where they (and their associated data) have been joined by a growing range of business 'software as a service' (SaaS): from budgeting to spreadsheets (Rahman & Lackey, 2013). Using cloud-based infrastructure such as computers and data storage can provide access to unlimited resources without the need for up-front investment, maintenance or IT expertise. But the consumption-based, pay-as-you-go approach is a mixed blessing.

The challenges are false perception that pay-as-you go is 'cheaper' than other ways to resource IT, difficult to monitor/control/analyse IT costs (particularly for infrastructure), inadequacy of traditional approaches to IT cost/benefit analysis and expectation that IT systems will be available online (often 24/7).

3. Social Collaboration

Social media has come a long way in the 20 years that have passed since people first started using the internet to create, share and exchange information and ideas, but the biggest changes have emerged over the past few years. Social media sites for blogging, crowdsourcing, instant messaging, internet telephony, and sharing pictures and music quickly gained critical mass as popular personal tools for communication and collaboration (Yee, 2013). Then they were picked up and exploited by businesses, government bodies, charities and other organisations that want to improve communication and collaboration with and between their many internal and external stakeholders. As the use of social tools becomes the 'new normal' all users will be affected by changing approaches to, and expectations of, communication and collaboration. Social Collaboration has helped to remove barriers to communication, speeding up month-end processes, enhance decision-making and productivity and opening up new routes to investment.

4. Digital Service Delivery

Digital services are transforming business, practice, central and local government, charities and other third sector organisations, by exploiting new IT architectures and technologies to deliver web-based business processes, e-commerce, mobile commerce, and cloud-based software and services using the internet and intranets (Permvattana, Armstrong & Murray, 2013). Many digital services include key features such as self-help and self-assessment solutions for service users, and use technologies such as chat bots to handle initial enquiries and requests for support

(rather than, or in addition to, email), offer interactive live chat from websites and portals, and communicate using social media channels such as Facebook and Twitter Permvattana, Armstrong & Murray, 2013). As users and those they work with and for deliver more products and services electronically, new skills are required and new risks must be addressed.

The challenges of digital service delivery are digital connectivity is central to cultures and hence business models, robust business cases can be hard to build, lack of interoperability of legacy systems, time taken to develop classifications and use of multiple taxonomies and financial benefits can be hard to unlock.

5. Big Data

The world creates 2.5 quintillion (10^{18}) bytes of data each day in the form of barcodes, phone signals, digital images, transactional databases, personal location records, statutory reporting systems, online searches, radio-frequency identification tags, social data, video clips, website visits, and more. Converging technology trends, the shift from analogue to digital, widespread mobile device adoption, internet-connected systems and 'exhaust data' from physical objects (the internet of things) are constantly creating vast amounts of structured and unstructured data (Adeoluwa, Aboderin, and Omodara, 2013). The ability to collate, manage and analyse it effectively can lead to better decisions and generate a competitive advantage for business, and the technology to do this is becoming more accessible and affordable.

The big data has improved understanding of market conditions, forward planning and risks, potential to increase business effectiveness and lower process costs, transform audit and forensic accounting by improving corporate and level playing field for small businesses and larger organizations (Adeoluwa, Aboderin, and Omodara, 2013).

The challenges are shortage of data mining and interpretations skills, knowing which questions to ask to gain insights, affordability, interoperability and standards, obtaining high quality data. Lots of data is not the answer, and data security, privacy and other important legal issues.

6. Payment System

The internet has become both a centre and a platform for commerce and this is reshaping payment systems across the world. Changes include moves to phase out cheques and a decline in the rate at which the use of credit and debit cards increases. But the most significant change to payment systems has been the rise of electronic banking – and numerous associated payment platforms (Adeoluwa, Aboderin, and Omodara, 2013). Services offered by traditional banks are increasingly accessed online from internet-connected fixed and mobile devices; statutory payments must increasingly be made electronically; payment options using mobile phones are proliferating; businesses and consumers have a myriad of ways to make and accept payments for goods and services.

7. Cybersecurity

Cybersecurity refers to the measures, practices and systems used to protect digital devices, networks, applications and information from unauthorised access, misuse, disruption or destruction. It encompasses technical controls such as authentication, encryption, software updates and network monitoring, as well as organisational measures such as staff training, security policies and incident-response planning. Cybersecurity is increasingly important because individuals and institutions depend on digital systems for financial transactions, communication, recordkeeping

and service delivery. A security failure may expose confidential information, interrupt essential operations or cause financial and reputational damage. Cybersecurity should therefore be treated as an ongoing responsibility rather than a one-time technical intervention.

Cyber threats take different forms, including phishing, malware, ransomware, identity theft, account compromise and fraudulent electronic transactions. The original manuscript identifies cybercrime, cyber-fraud and the theft of digital information as major concerns associated with growing dependence on computers and online services. Anah (2002) is cited in the manuscript in connection with cybercrime in Nigeria, although the reference requires bibliographic verification. Usman and Shah (2013), in their study of critical success factors for preventing electronic-banking fraud, provide a more specifically identified reference for considering the protection of digital financial services. These sources connect cybersecurity to practical risks that affect individuals and organisations, particularly where electronic transactions and sensitive information are involved. Effective cybersecurity requires a combination of user awareness, sound technical design and institutional accountability. Individuals can reduce exposure by using strong and unique passwords, enabling multifactor authentication where available, updating software and verifying unexpected requests for personal or financial information. Organisations should restrict access to sensitive records, maintain reliable backups, train staff and establish procedures for detecting and responding to incidents. Security measures must also be reviewed as systems and threats change. A secure digital environment cannot be achieved solely through technology because user behaviour, organisational practices and the handling of information also influence risk. Cybersecurity is therefore best understood as a continuing process involving prevention, detection, response and recovery.

Theoretical Framework

Technological Determinism Theory

Technological determinism is a perspective used to examine the influence of technological development on social structures, communication practices and human behaviour. The perspective emphasises the capacity of technological innovations to change how individuals interact, how organisations operate and how societies organise their activities. In the context of cyberspace and virtual reality, technological determinism provides a basis for examining how mobile devices, internet connectivity, artificial intelligence and immersive technologies have changed established patterns of communication and information exchange. The spread of digital platforms has made it possible for individuals and organisations to perform activities that previously depended on physical presence or conventional communication channels. Technology can therefore be examined as an important influence on the transformation of contemporary social and institutional practices. The relevance of technological determinism is evident in the development of cloud computing, electronic payments, online collaboration and virtual environments. Cloud services have changed how organisations store and access information, while social platforms have expanded the opportunities for public communication and participation. Similarly, virtual reality has introduced new methods of simulation, training and experiential learning. These developments illustrate how technological innovations can reshape established practices and create new expectations about speed, convenience and accessibility. The original manuscript's discussion of mobility, cloud computing, social collaboration and digital service delivery supports this argument by identifying technological developments that have altered how individuals and organisations communicate and conduct their activities. However, the existence of a technological innovation does not automatically establish that it will produce the same outcomes in every social context.

Technological determinism is useful for this paper because it draws attention to the transformative potential of emerging technologies, but it must be applied critically. Social outcomes also depend on institutional decisions, economic conditions, public policies, cultural practices and the choices made by users. A technology may improve access for one group while excluding another because of differences in income, infrastructure or digital literacy. Similarly, artificial intelligence may improve the speed of certain processes while introducing concerns about bias, privacy and accountability. The paper therefore uses technological determinism as an interpretive perspective for examining technological change without assuming that technology alone determines social outcomes. This approach allows the discussion to consider both the opportunities created by innovation and the conditions that influence its consequences.

Discussion

The discussion is organised around the three objectives of the paper and relates the observations to the literature cited in the original manuscript and relevant scholarly work. Because the paper adopts a literature-based approach, the observations are analytical interpretations rather than results from original fieldwork.

Emerging Technological Developments in Cyberspace and Virtual Reality

The first objective examined major technological developments shaping cyberspace and virtual reality. The review identified mobile connectivity, cloud computing, social collaboration, digital service delivery, big-data analytics, electronic payment systems, cybersecurity, robotics, augmented reality, virtual reality and artificial intelligence as significant areas of technological development. These developments demonstrate that digital transformation extends beyond internet access to include the integration of connected devices, data systems and automated processes into everyday activities. Korchmaros et al. (2013), whose study examined teen dating violence in a networked society, provide a source relevant to the social implications of networked interaction. Their specific research focus should, however, be distinguished from broader claims about mobile technology and economic productivity. The literature therefore supports the importance of examining the social contexts in which networked technologies are used, rather than treating connectivity as a purely technical development.

The discussion of cloud computing and electronic commerce also demonstrates the importance of examining the infrastructure supporting digital activity. Rahman and Lackey (2013) considered security in e-commerce systems for small businesses, drawing attention to the need to protect online commercial processes. Usman and Shah (2013) examined factors associated with preventing electronic-banking fraud, making their work relevant to the risks accompanying digital financial services. These studies provide a basis for connecting technological development with security and organisational responsibility. Their implications extend to the adoption of cloud services, online payment systems and other applications that depend on the safe handling of information. The benefits of digital services should consequently be evaluated alongside the capacity of organisations to protect users and maintain dependable operations.

The emergence of AR, VR and artificial intelligence further illustrates the changing relationship between users and digital information. The original manuscript identifies immersive technologies as tools for simulation, visualisation and interactive experiences, while its discussion of artificial intelligence highlights automation, conversational systems and software-supported decision-making. These developments create opportunities for education, training, communication and service delivery, but they also require careful assessment of cost, accessibility, reliability and user

safety. The literature cited in the original manuscript does not provide sufficient evidence to establish that all these applications consistently improve performance across different contexts. The defensible observation is therefore that emerging technologies create new possibilities whose effectiveness depends on their design, implementation and suitability for specific purposes.

Benefits and Risks of Emerging Technologies

The second objective examined the benefits and risks associated with emerging technologies. The literature-based discussion indicates that digital systems can improve communication, expand access to services, support organisational coordination and facilitate electronic transactions. Permvattana et al. (2013), in their work on e-learning for people with visual impairments, provide a relevant basis for considering how digital technologies may support educational access when designed around users' needs. Their work also reinforces the importance of accessibility in evaluating technology. Digital learning should not be considered inclusive simply because educational content is available online; the design of the platform and the accessibility of its resources influence whether users can benefit from it.

The risks associated with digital services are illustrated by Rahman and Lackey's (2013) examination of e-commerce system security and Usman and Shah's (2013) work on electronic-banking fraud prevention. These studies connect digital participation with the need to protect transactions and sensitive information. Cybercrime, fraudulent messages, compromised accounts and unauthorised access can undermine confidence in online services. Anah (2002) is also cited in the original manuscript in relation to cybercrime in Nigeria, although the complete bibliographic details should be verified before the source is relied upon for specific factual claims. Taken together, these references support the argument that technological expansion should be accompanied by practical security measures, user awareness and clear procedures for handling incidents. The risks extend beyond financial fraud and technical vulnerabilities. The collection of personal information, the circulation of misleading content and unequal access to digital infrastructure may affect privacy, trust and participation. Big-data analytics and AI-enabled services may also produce unreliable conclusions when the underlying information is incomplete or biased. These issues suggest that the consequences of technology depend partly on how systems are governed and how users understand their operation. A balanced approach should therefore recognise the potential benefits of technological innovation without assuming that every application is safe, effective or equally accessible. Responsible adoption requires institutions to assess foreseeable risks and provide appropriate safeguards.

Measures for Responsible and Inclusive Use

The third objective examined measures for promoting the responsible use of cyberspace and virtual reality. The literature suggests that security, accessibility and effective management should be integrated into technological adoption rather than addressed only after problems arise. Rahman and Lackey (2013) and Usman and Shah (2013) are particularly relevant to this argument because their respective studies address e-commerce security and the prevention of electronic-banking fraud. Their subject areas demonstrate the importance of assessing the vulnerabilities associated with digital transactions. Organisations adopting online services should therefore consider authentication, access controls, data protection, staff training and incident response as essential components of their operations. Digital literacy is another important measure because users influence the safety and effectiveness of online environments through their decisions and behaviour. Yee (2013), whose study examined international students' perceptions of online

learning in an Australian university, provides a reference for considering users' experiences of digital learning environments. However, the precise findings of that study should be consulted before attributing particular outcomes to it. More broadly, institutions should ensure that users can navigate digital services, evaluate information, protect their accounts and seek assistance when systems fail. Inclusive design is equally important because people differ in their access to devices, connectivity, language support and accessible interfaces. Digital services should be assessed in relation to the needs of their intended users rather than their technical capabilities alone.

Responsible governance should also include periodic risk assessment, transparency and accountability. Institutions introducing AI, cloud services or immersive technologies should identify the purpose of adoption, assess likely benefits and risks, protect sensitive information and determine who is responsible for reviewing errors. Human oversight is particularly important when automated systems influence consequential decisions. These measures follow from the central argument of this paper: technological progress is most useful when accompanied by appropriate infrastructure, informed users and accountable institutions. Collaboration among government, industry, educational institutions and the public can help establish practices that protect users while allowing beneficial innovation to continue.

Summary of Findings and Recommendations

The findings revealed that emerging technologies, including mobile connectivity, cloud computing, artificial intelligence, robotics and virtual reality, are transforming communication, education, commerce and organisational activities. It is recommended that institutions adopt these technologies based on clearly defined objectives, affordability, accessibility and suitability for users' needs. The paper found that although digital technologies improve communication, information access and service delivery, they also expose users to cybercrime, fraud, privacy violations and digital exclusion. Therefore, organisations should strengthen cybersecurity, protect personal information and provide continuous digital-literacy training to promote safer and more inclusive technology use. The findings further indicated that responsible technology adoption depends on effective governance, risk assessment, accessibility and institutional accountability. It is recommended that government agencies, technology providers and educational institutions establish clear policies, conduct regular risk assessments and ensure appropriate human oversight to encourage the responsible and sustainable use of cyberspace and virtual reality.

Conclusion

Cyberspace and virtual reality have become significant environments for communication, education, commerce and organisational activity. Developments in mobile connectivity, cloud computing, social collaboration, electronic payments, robotics, AR, VR and artificial intelligence have expanded the ways individuals and institutions exchange information and perform tasks. The literature discussed in this paper indicates that these technologies offer important opportunities, but their benefits must be considered alongside risks involving cybersecurity, privacy, accessibility and accountability.

The central argument is that technological progress should not be measured solely by the adoption of new devices or platforms. Its value also depends on whether technologies are secure, accessible, reliable and appropriate for their intended purposes. The literature on e-commerce security, electronic-banking fraud and accessible digital learning reinforces the importance of considering users' needs and the conditions under which digital services

operate. Responsible use consequently requires a combination of technical safeguards, digital literacy, inclusive design and institutional accountability.

RJMCIT

References

Adeoluwa, O. V., Aboderin, O. S. & Omodara, O. D. (2013). An appraisal of educational technology usage in secondary schools in Ondo State, Nigeria. *International Journal of Innovational and Applied Studies,* 2(3), 265-271.

Adnan, M. H. (2010). *A dictionary for communication and public relations practice*. University Publication Centre (UPENA).

Anah B.H. (2002). "Cyber crime in Nigeria" Causes, Effects and Wayout". *ARPN Journal of Science and Technology*, 7, p.626.

Anah, B. H. (2002). Cyber crime in Nigeria: Causes, effects and way out. *ARPN Journal of Science and Technology*, (7), 626. The issue, title, and page information require verification.

Korchmaros, J.D., Ybarra, M.L., Langhinrichsen-Rolling, J., Boyd, D. & Lenhart, A. (2013). Perpetration of teen dating violence in a networked society. *Cyberpsychology, Behavior and Social Networking*, 16(8), 561-567.

McGraw-Hill Dictionary of Computing and Communications (2003). New York: McGraw-Hill Co. Inc.

Permvattana, R., Armstrong, H. & Murray, I. (2013). E-learning for the vision impaired : A holistic perspective. *International Journal of Cyber Society and Education*. 6(1), 15-30.

Pfaffenberger, B. (2000). *Dictionary of computer terms* (8th ed.). Webster's New World.

Rahman, S. M., & Lackey, R. (2013). E-commerce system security for small businesses. *International Journal of Network Security & Its Applications*, 5(2), 193–210.

Usman, A. K., & Shah, M. H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, 18(2), 1–15.

Usman, A.K. & Shah, M.H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, 18(2), 1-15.

Vakharia, A.B., Mishra, V. & Kumar, S. (2013). Security glitches related to e-commerce and their solutions. *International Journal of Computer Application,* 2(3), 85-94.

Yee, R.C.S. (2013). Perception of online learning in an Australian university: An international students' perspective – support for learning. *International Journal of Cyber Society and Education,* 6(1), 45-50.