

Technical & Industrial Sponsors



Proceedings of The First International Conference on ICT for National Development and Its Sustainability

**Theme: The Role of Information and Communication Technology
for National Development and Its Sustainability
(ICT4NDS 2018)**

**Organised by the Faculty of Communication and Information
Sciences, University of Ilorin, Ilorin, Kwara State, Nigeria**

Tuesday 17th – Friday 20th April, 2018

**Print ISSN: 2141-3959
Online ISSN: 2141-3959**

Copyright © 2018

Editors

**Prof. R. A. Lawal
Dr. R.G. Jimoh
Dr. A. Tella**

COPYRIGHT INFORMATION

The First International Conference on ICT for National Development and Its Sustainability (ICT4NDS 2018).

The author(s) warrant that the manuscript submitted is his/her/their own original research. All participated authors in this work take public responsibility and have approved that the manuscript has not been sent any other publication media. All matter included in the manuscript does not violate any existing copyright rules and any intellectual property rights of any person or entity. The manuscript meets ethical standards applicable to the research discipline. I/We indemnify *ICT4NDS 2018* and the editors of the Conference and hold them harmless from any loss, expense or damage occasioned by a claim or suit by a third party for copyright infringement, or any suit arising out of any breach of the foregoing warranties as a result of publication of my/our article.

The undersigned with the consent of all the authors, hereby transfer, to the extent that there is copyright to be transferred, the exclusive copyright interest in the above-cited manuscript, in this and all subsequent editions of this manuscript, and in derivatives, translations or ancillaries, in English and in foreign translations, in all formats and media of expression now known or later developed, including electronic, to *International conference on Information and Communication Technology for National Development and Its Sustainability (ICT4NDS)*.

Print ISSN: 2141-3959

Online ISSN: 2141-3959

PREFACE

This book contains the Proceeding of research papers presented at the First International Conference on ICT for National Development and Its Sustainability held between Tuesday 17th – Friday 20th April, 2018 at the University of Ilorin, Ilorin, Kwara State, Nigeria.

The conference was organized by the Faculty of Communication and Information Sciences, University of Ilorin.

In all, total of over (100) papers, including (3) lead papers were submitted. Apart from Nigeria, submissions were received from such countries as Malaysia, South Africa and China. The papers were subjected to a peer review process with respect to the actual content and the level of originality. The papers which appear in this proceeding were those that substantially met the set acceptance criteria.

I wish to appreciate all who contributed in one form or the other towards making this Proceeding a reality.

Thank you.

Dr. R.G. Jimoh, Ph.D., FICENT, MNCS, MCPN, MIEEE, MISCO, MITSSP, MAIT
Dean FCIS, General Editor,

Proceedings of the 1st International Conference on ICT for National Development and Its Sustainability (ICT4NDS 2018).

Chair Central Planning Committee

Dr. R.G Jimoh

Local Organizing Committees/LOC

Technical Programme Committee (TPC)

- Dr. Nasir Faruk
- Dr. A. O. Bajeh

Hotel & Accommodation

- Dr. M.T. Bashorun
- Dr. (Mrs.) K. K. Kadiri

Budget and Finance

- Dr. (Mrs.) AbdulBaqi
- Mrs Mustapha

Entertainment

Dr. (Mrs.) M. A. Mabayoje

Logistics

Dr. N. A. Balogun

Registration

- Dr. A. O. Bajeh
- Dr. Nasir Faruk
- Miss Ahmed Aminat (CISSA VP)

Publicity

Dr. La'aro

Publication

- Dr. A. Tella
- Dr. L. Mustapha

Website Creation and Maintenance Committee

- Dr A.O. Bajeh
- Dr. N. A. Naem,
- Dr. K. K. Kadiri
- Dr. A. A. Salman
- Dr. A.A Oloyede

Editors and Reviewers

- | | |
|-------------------------------------|---------------------------------|
| 1. Dr. M.B. Lawal | 23. Prof. R. A. Lawal |
| 2. Dr. M.T. Bashorun | 24. Dr. R.G. Jimoh |
| 3. Dr. S. Faki | 25. Dr. A. Tella |
| 4. Dr. Kayode Adewole | 26. Dr. Amos O. Bajeh |
| 5. Dr. Mrs. A.G. Akintola | 27. Dr. Nasir Faruk |
| 6. Dr. Shefiu Ganiu | 28. Dr. A..A. Oloyede |
| 7. Dr Lere Jide | 29. Dr. L.A. Olawoyin |
| 8. Dr. Mrs. T. O. Oladele | 30. Dr. N.T. Surajudeen Bakinde |
| 9. Dr. Mrs K. K. Kadiri | 31. Dr. Y.A Abdulrahman |
| 10. Mrs. S. A Salihu | 32. Engr. Segun Popoola |
| 11. Dr. Obiseye Obiyemi | 33. Dr. N. A. Balogun |
| 12. Mr. Abdulrahman Abdullahi Tosho | 34. Mr. A. O. Balogun |
| 13. Dr. Abdulmumin Isah | 35. Dr Rafiat Oyekunle |
| 14. Dr Aliyu Alhaji, | 36. Dr. Tella Adeyinka |
| 15. Prof. Dahiru Sani Shu'aib | 37. Dr. Mrs. F. E. Usman-Hamza |
| 16. Dr. Olarangbe | 38. Dr. K. L. Mustapha |
| 17. Dr. A. Salman | 39. Dr. Haruna Chiroma |
| 18. Mr. H. A. Mojeed | 40. Dr Mrs. O.C. Abikoye |
| 19. Dr. A. O. Ameen | 41. Dr R. O. Oladele |
| 20. Dr. D. R. Aremu | 42. Dr Omopupa |
| 21. Mr. Sowande S. O | 43. Dr. Modinat A. Mabayoje |
| 22. Dr. A. O. Ameen | 44. Dr. D. R. Aremu |

Secretariat Registration Committees & Others

Adeniyi Shamsudeen Femi
Ajayi Oluwaseun
Musliudeen Toyeeb Abiodun
Balogun Victor Segun
Ganiyu Afeez Ishola
Subair Jemima
Henrybless Esther Kelechi
Dhikrulllah Hizkeel Bolade

TABLE OF CONTENT

Authentication mechanisms in public payment systems: challenges and solutions <i>Yusuf Olayinka Abduljelil, Jimoh Rasheed Gbenga</i>	1
Adoption of spi in nigeria software houses: a literature review <i>Bajeh, A. O., Adeleke, H.O., Mojeed, H.A.</i>	12
Leveraging on the relevance of social media for the development of Nigeria political economy <i>Ajobiewe, Damilola. N., Segun Omotosho and Florence Babalola</i>	23
Ensemble-based streaming approach for spam detection on twitter network <i>K. S. Adewole, R. G. Jimoh, A. G. Akintola, O. C. Abikoye</i>	35
A non-cooperative spatial management game for high efficiency wlan (ieee 802.11ax) <i>Yusufu Ramat, Suleiman Zubair, Adeiza Onumanyi, Kehinde Oyegbola</i>	52
Steganography: Increasing the Size of Hidden Messages <i>Bajeh A. O., Abdulkadir, A.B. and Yusuf A. O.</i>	61
Influence of online gambling on academic performance of students: a case of university of ilorin, ilorin, Nigeria. <i>Alimi Adebayo Emmanuel and Falade Ayotunde Atanda</i>	76
Analysis of huffman and run-length encoding compression algorithms on different image files <i>Aliyu Ishola Nasiru and Afolayan Tolulope Ambibola</i>	88
Comparative analysis of discrete cosine transform and discrete wavelet transform on different image files <i>Ishola N. Aliyu, Ositadinma K. Nwana, Ismaeel A. Sikiru, Yusuf O. Imam-Fulani</i>	100
Development of a system for extraction of patient drug prescription from clinical notes <i>Abikoye, Oluwakemi Christiana, Salihu, Shakirat Aderonke and Shodolu, Wasiu Olabode</i>	112
Digital revolution and national security: dynamics of information communication technology in sustainable development in Nigeria <i>Haruna I.Abdullahi</i>	122
Institutional policy implementation and adoption of learning management system in osun state universities <i>Jimoh, T. B. & Fasasi, Y. A.</i>	135

Study of downlink scheduling algorithms for real-time multimedia services in lte networks. <i>Maniru Malami Umar, Sadiq Aliyu Ahmad, Asma'u Shehu & Ziya'u Bello</i>	143
Secured voting system in nigeria general election <i>Yusuf I.T, Akanbi M.B, Bolaji-Adetoro, D.F, Jimoh, R.G</i>	152
Determining risk factors in the formulation of anfis model for the security risk assessment of sdlc phases <i>Olusanya Olufunmilayo Olayinka, Jimoh Rasheed Gbenga</i>	162
Hactivism or bloggerpreneurship: a critical political economy of the nigerian blogosphere <i>Badmus, Idowu Rasheed, Okaiyeto, Simon Ayodele</i>	181
Soft-output maximum likelihood receiver for quadrature spatial modulation <i>Muhammed Adekilekun Tijani and Abdulmajeed Adekilekun Tijani</i>	195
An enhanced fault tolerant in wireless sensor network using intelligent multi-agent system <i>Raji Ayodele Kamaldeen, Gbolagade Kazeem Alagbe</i>	205
Redefining the directivity value of radial-lines-slot-array antenna for direct broadcast satellite (dbs) service <i>Monebi Matthew Ayodeji, Caroline O. Alenoghena, and J.A. Abolarinwa</i>	217
Review of selected spectrum occupancy models <i>T. A. AbdulRahman, R. O. Oladele, and N. Faruk</i>	229
The relevance of data mining techiques in alleviating cybersecurity breaches in nigeria healthcare sector <i>Ayoade Oluwafisayo Babatope, Oladele Tinuke Omolewa, and Saheed Yakub Kayode</i>	247
A classified media access control algorithm for traffic management in ieee 802.11ah networks <i>Kehinde Oyegbola, Suleiman Zubair, Elizabeth Onwuka , Yusufu Ramat, Ademoh A. Isah</i>	263
A bat-inspired algorithm for the detection of hidden nodes in ieee802.11ah networks <i>Fapohunda K. O., Zubair S., David M. and Nuhu B. K., Nwaocha V. O.</i>	272
Information literacy for sustainable development: a review <i>Agboola, O.M., Bajeh, A.O., Dada, O. M.</i>	280
Hierarchy extraction for covert network destabilization and counterterrorism mechanism <i>Ismail A. A., Ganiyu, S. O., Alabi, I. O., Abdulrazaq, A. A., Muritala S.</i>	290

Assessing urban transport sustainability for people with disabilities in the digital era <i>Ayantoyinbo, Boye. B. and Kolawole, Olusola. J</i>	303
Adoption of cyberspace in sustaining community development in Nigeria <i>Abdulrauf Tosho, Muhammad Thani Sefinat, Shakirat Oluwatosin Sulyman-Haroon</i>	316
Social media and sexual expression among adolescents <i>Amina Shehu, Aishat AbdulRauf-Salau, Naeem Atanda Balogun</i>	328
Role of information and communication technologies (icts) in curbing corruption among public servants in kwara state inland revenue service (kwirs) <i>Aishat Abdulrauf-Salau, Adesina Lukuman Azeez, Rukayat Ololade Adegoke</i>	344
Stock market prediction using combination of five (5) data mining techniques <i>Idepefo Olutokunbo Felix, Awotunde Joseph Bamidele, Ayo Emmanuel Femi, Oladipo Idowu Dauda, and Adeniyi Aruna Adekunle</i>	355
Improving performance of principal component analysis based face recognition using illumination normalization techniques: proposed study <i>Shoyemi Olufunmilayo Iyabo, Abikoye Oluwakemi Christiana, and Aro Taye Oladele</i>	371
Adoption of virtual reality for learning among students <i>Shakirat Oluwatosin Sulyman-Haroon, Sulyman Age Abdulkareem, Abdulrauf Tosho</i>	380
Strategies for knowledge sharing in nigerian agricultural research institutes <i>Kabiru Dahiru Abbas</i>	390
Usage of social media among student entrepreneurs in Nigeria University <i>Shakirat Oluwatosin Sulyman-Haroon, Kadijat Kehinde Kadiri</i>	398
Mobile based test (mbt) system <i>Ogunyinka Oluwaseun Joshua, Usman–Hamza Fatima. E, Bajeh Amos Orenyi</i>	413
The journey of 5g mobile communication networks <i>Olugbenga A. Sowande, F. E. Idachaba, E. Agboje, Q. R. Adebowale, N. Faruk , L. A. Olawoyin, S. O. Onidare, A.O. Ilesanmi</i>	419
Quality of service (qos) evaluation of mobile network services: a case study on the federal polytechnic bida, nigeria <i>Salihu Alhaji Bala, Caroline O. Alenoghena, Aliyu Alhaji Ndakotsu</i>	434

Provision and utilization of offline electronic resources in Nigerian academic libraries and its implication for sustainable national development <i>Usman Hassan, Binta Ladan Farouk, Aminu Musa Umar, Askia Nasiru Kabara, Muktar Mohammad Magaji, Jamila Mansur Chiranchi</i>	447
Perceptions of academic librarians on knowledge management for sustainable development in northwest federal universities in Nigeria <i>Musa Aminu Umar, Usman Hassan, Ja'afaru Sani, Musa Abubakar Mohammed, Mustapha Mannir, Amata S. Bello</i>	456
Performance analysis of empirical propagation models for fixed wireless application <i>Quadri R. Adebawale, Caroline T. Adeniran, Olugbenga A. Sowande, Yusuf O. Imam-Fulani, Samuel O. Onidare, Ismael A. Sikiru</i>	470
A survey of application of nature-inspired computational methodologies in radio propagation <i>Quadri R. Adebawale, Shamsudeen A. Olanipekun, Nasir Faruk, Lukman A. Olawoyin, Abdulkarim A. Oloyede, Nazmat T. Surajudeen-Bakinde, Segun I. Popoola</i>	482
Prospects and challenges of different technology options for public safety and disaster relief networks in nigeria <i>Nazmat T. Surajudeen-Bakinde, Nasir Faruk, Adeseko. A. Ayeni, Olayiwola.W. Bello, O.A. Fadipe-Joseph and Olabanji Kolade</i>	493
Assessment of the utilization of e-learning facilities among lecturers in kaduna polytechnic for sustainable national development in Nigeria <i>Ali Garba, Abubakar Mohammed and Abubakar Mohammed Jega</i>	504
Awareness, use and satisfaction of collections and services of college libraries in federal university of petroleum resources <i>A.A. Salman, A.S. Sambo, H.Shehu, K.A. Saka</i>	518
Undergraduate students' preferences for web-based and conventional library services in kwara state university, malete <i>A. O. Aleem and A. A. Salman</i>	530
Information access using web 2.0 as panacea for attaining sustainable development goals: a review of related models <i>A. A. Olajide, A. A. Salman, and Ashaver Doosuur D.</i>	548
Social networking as a tool for library services and knowledge management in academic libraries in Nigeria <i>M.T. Bashorun, Abdulmumin Isah and Ajibola, S. Adejumo</i>	559

Congestion as index of quality of service of mobile communication networks in osogbo metropolis, osun state	571
<i>Lasisi Hammed, Aderinkola B. Fatimah and Olawoyin Lukman A.</i>	
Knowledge management and 21 st century libraries as panacea for sustainable development	586
<i>Tella Adeyinka, Ajibola Tunde Shamsudeen, Akanbi Mohammed Lawal, Bashorun M.T, Ajao Adelodun Muhammed and Ogunlade O.R</i>	
New media and satisfaction with democracy among students of selected universities in kwara state, Nigeria	604
<i>Lambe Kayode Mustapha, Aminat Bukola Anafi and Maryam Lasisi Mustapha</i>	
On backhauling options for future heterogeneous networks	621
<i>Nafiu Adetokun, Nazmat T. Surajudeen-Bakinde, Nasir Faruk, Segun I. Popoola, A.Abdulkarim</i>	
An enhanced salting fingerprint transformation algorithm for securing biometric system	634
<i>Omotosho Folorunsho Segun, Babalola Florence Moyin</i>	
An investigation into packet routing in mobile ad-hoc network using a nomadic community scenario	647
<i>Oyelakin A.M., Jimoh R.G</i>	
Development of an Integrated Digital Library in a Networked Environment	658
<i>Akanbi Bola Mulikat and Raji Ayodele Kamaldeen</i>	
ICT skills and Use of Electronic Information Resources by National Open University Students in South-West Nigeria	670
<i>Adedokun Titilayo Oludayo and Babalola Yemisi T.</i>	
Scrum process model for the development of smart payroll integrated with task manager	679
<i>Musa Nehemiah, Mustapha L. Abdulrahman, Ramson Emmanuel N., Babangida Mubarak, Muhammad M. Aliyu, Gazali M. Abdulhamid, Lubna A. Gabralla, Amina Nuhu Muhammad Abdulsalam Y. Gital, Haruna Chiroma</i>	
Assessment of patients' knowledge and perception towards conventional and digital radiograph in dental imaging.	693
<i>Moshood Adeyemi, Junaid Ayinde, Issa Aremu, Hassan Kalejaye, Halimat Akande</i>	
The Prospect of Addressing Property Management Challenges with Information and Communication Technology (ICT): A Survey of Minna Metropolis, Niger State	703
<i>S.O. Ganiyu, C.F. Essien, I.O. Alabi, V.J. Ukam</i>	

Promoting Local Content Software Products through Agile Process Models <i>Nehemiah Musa, Emmanuel Nannim Ramson., Umar Sa'idu Abashe, Amina Nuhu Muhammad, Abdulsalam Ya'u Gital, Gazali Muhammed, Lubna A. Gabralla, Haruna Chiroma</i>	714
Appraising the role of information and communication technology (ict) as a change agent for university libraries in Nigeria <i>Kennedy Arebamen Eiriemiokhale (CLN)</i>	730
SQL Injection Attack: A Systematic Literature Review on Detection, Prevention and Classification with Machine Learning Approach <i>Morufu Olalere, Raji Abdullahi Egigogo, Umar Rukayya, Shafi'i Muhammad Abdulhamid, Yisa Victor Legbo, Rasheed Gbenga Jimoh</i>	743
Assessment of the Use of Social Media by Undergraduate Student of University of Ilorin <i>Ibrahim Latifat Ahuoiza and Afolayan Oluyinka Titilope</i>	759
An online diagnostic model for detecting severity of diabetes <i>O. M. Omisore, L. Wang, A. E. Babalola, B. A. Ojokoh and O. S. Adewale</i>	774
Providing information access to all and sundry: a panacea for better livelihood and sustainability in the 21 st century <i>Tella Adeyinka, Bamidele Sunday Segun, Adigun Ganiyu Ojo, Olaniyi Oluwakemi Titilola, Firdausi Abdullahi</i>	787
Electronic voting system implementation in nigeria higher institutions <i>Murtala K., and Adeniyi A. E.</i>	809
Cryptographic system using Caesar cipher and DNA sequences <i>Akintola A.G. Dael A.O. Bajeh,A.O, Balogun, A.O</i>	820
Effect of repetitive search on binary and linear search algorithms <i>Balogun Ghaniyyat Bolanle</i>	828
A spatiotemporal decision support system for software collaboration using x-kruskal algorithm <i>Femi Emmanuel Ayo1, Olusegun Folorunso2, Joseph Bamidele Awotunde3, Olusakin Muiyiwa Fatokun4</i>	837
English competence and search for information resources for academic development among colleges of education students in kwara state, nigeria <i>Omopupa, Kamal Tunde, Iliyas, Rasaq Ayodeji, Adio, Saliu Wahab</i>	862

THE RELEVANCE OF DATA MINING TECHNIQUES IN ALLEVIATING CYBERSECURITY BREACHES IN NIGERIA HEALTHCARE SECTOR

¹Ayoade, Oluwafisayo Babatope

¹Oladele, Tinueke Omolewa

²Saheed, Yakub Kayode

¹Department of Computer Science, University of Ilorin, Ilorin, Kwara State, Nigeria.

²Department of Computer Science, Al-Hikmah University, Ilorin, Nigeria.

¹oluwafisayoadeb.oba@gmail.com; ¹tinuoladele@gmail.com; ²yksaheed@alhikmah.edu.ng
+234-803-306-7974 +234-816-491-6082 +243-814-26-3364

ABSTRACT

In the face of threat of viruses, malware and spyware almost from the inception of computing, awareness of data security and clarity of computer systems data didn't make a pull until the explosive growth of the Internet. This points to the exposure of so many different organizations' devices on the web which provided an absolute environment for hackers to test their expertise –now called cybersecurity breaches (cybercrimes). Recently, healthcare organizations, clients/payers and regulatory bodies have been exposed to ever-increasing data confidentiality, integrity and security perils affecting their operations and governmental environment as well as patient self-confidence. Cybercrimes are on the rise as healthcare organizations' devices access to internet increases. Healthcare organizations has increasingly moved outside the hospital walls into various homes and communities using consumer-based technologies, thereby building patients' and government confidence in order to secure patient's data and information. Health organizations in Nigeria must balance prudently how to address patient's confidentiality and develop security measures in a cost effective manner. This paper attempt to provide an overview of cybercrimes and cybersecurity in healthcare sector; identify various reasons for cybercrimes and document a propose process of annihilation through the involvement of data mining techniques. In addition, it looks at the approaches of stepping up cybersecurity and recommendations that would help healthcare organizations and government policy makers in checking the increasing rate of cybercrimes.

Keywords: Cybersecurity, Cybercrime, Healthcare, Internet, Information and communication technology (ICT),

1. INTRODUCTION

The information and communication technology (ICT) industry has advanced positively and greatly over the last fifty years. This technology is pervasive and increasingly essential and relevant to almost every aspect of contemporary civilization where Healthcare is one prominent industry. Devices and communication components of healthcare ICTs are interdependent and so interruption of one may have either positive or negative impact on others. Concerns of protecting and securing these healthcare ICT systems from internal or external attacks has increased likewise in the last several years. ICT experts have concluded that these might increase in frequency and sternness over the next couple of years. On this wise, the act of protecting these healthcare ICT systems, components and their contents is what is known as *Cybersecurity* (Fischer, 2016; Schaeffer et al., 2009).

These technologies (ICT) have transformed how people interact, socialize, shop, communicate with government and engage in business transactions as well as receive medical attentions. The internet and the World Wide Web have created massive amounts of information communication instantly available, and today smartphones and tablets have supported the duo by bringing the information at our fingertips everywhere we go. Hence, our communication with the outside world is not being altered by the Internet of Things (IoT) (Abomhara & Køien, 2015). Current surveys have estimated the internet users to be around 15 billion of the world populace; and an estimate of 26 billion to 50 billion has been postulated for 2020. Data and information storage is already increasingly ever-changing to the Cloud which is increasing data availability and usefulness but at the same time increasing its intricacy (Cameron F. & Gallagher, 2012; James, 2016; Royal Society, 2016).

Therefore, current cybersecurity practices in healthcare are not up to the task for demanding evidence-based standards of security. This has subjected the healthcare data and information systems to be vulnerable, both to upcoming threats and to those already well understood. Healthcare digital systems are already central to our security, wellbeing and development, but the threats and risks against the healthcare data and information constantly increasing and progressing. Hence, cybersecurity tools, processes and institutions need to draw level and carry on with these threats (CGI, 2015; ESET, 2016).

The healthcare sector, in different under-developed nations such as Nigeria, is confronted with a distinctive set of business, environmental and technical drivers of threat, along with exceptional set of regulations and policies for patients' PHI (Patient Health Information), Electronic Health Records (EHR) and Health Data management (HDM) (Brookson, 2016). Hence, healthcare information technology sectors concentrating on clinical transformation agenda often treat patients' confidentiality as policy thereby subjecting IT security as a secondary function. There are few nations' sectors that need strong cyber security as much as the nation's healthcare. Personal health and lifestyle information is increasingly valued as a product of tool by cyber-attackers. Therefore, from personal medical devices to enterprise-wide platforms, computer systems

are being targeted maliciously with resulting losses of data. Time-consuming compliance are worsened by the scarcity and high cost of skilled confidentiality and security resources, complex and risky information and communication technology (ICT) and ever increasingly dangerous and pervasive cyber threats (Serianu & Paladion, 2016).

In nations around the world, patients are dealing with life threatening conditions, thereby exchanging huge amount of money and financial information (such as bank accounts numbers, social security numbers - SSN and biometric verification number – BVN, in Nigeria) and these must have their confidentiality protected when it comes to medical records. Unfortunately, the healthcare sector is one of the biggest targets for cybercriminals of which Nigeria is not an exception. Efforts has been made by the Nigerian government (with supports from regulatory bodies like Code of Conduct Bureau, Independent Corrupt Practices Commission – ICPC, Economic and Financial Crime Commission, and so on) to checkmate most of the insubordinates in terms of corruption in different sectors like banking, education, including healthcare since the inception of BVN (Serianu & Paladion, 2016). The Nigerian government has mandated the citizens to be enrolled for the BVN and in same vein trying to connect this scheme with the National Identity Cards being controlled by the National Identity Management Commission (NIMC) (ESET, 2016; Serianu & Paladion, 2016)

In 2015 alone, for instance, according to IBM survey, there were over 100 million healthcare breaches of medical records (CGI, 2015). Frequently, healthcare organizations, most especially in Nigeria, do not understand their patient's data and information confidentiality and security risks, or do they know where to commence the improvement of their security stance. Correspondingly, with the increase of amalgamated system access to data and information, many healthcare organizations in Nigeria are not compliance with progressing regulation to protect the confidentiality of their PHI (Fischer, 2016).

According to Jim Finkle of Reuters in CGI (2015), on April 23, 2014, the US Federal Bureau of Investigation (FBI) has cautioned healthcare organizations that "*The healthcare sector is not as resistant to cyber intrusion compared to financial institutions and retail sectors, therefore the possibility of increased cyber intrusion is likely for healthcare sector*". Most healthcare organizations lack the capacity or financial resources to effectively address their increasing challenges in areas such as:

- compliance with patients' confidentiality, consent and other regulatory requirements
- identity and data loss theft
- lack of skilled security professionals
- consumerization of healthcare or BYOD – Bring Your Own Device
- assessing their safeguard effectiveness, and

- improving and maintaining employee confidentiality and security awareness (CGI, 2015)

Cybersecurity has shown to be more than just ordinary policies, security protectors and assessments. But, recently, they have shown to be standing as a solid backbone to support existing and future business growth in a way that is compliant, cost effective and secure. Hence, without a solid data confidentiality and security framework, health organizations in Nigeria will operate with an increasing amount of risk in the nearest future as they attempt to deal with ever rising threats and progressing regulation (Frank & Odunayo, 2013; Schaeffer et al., 2009)

Hence, this paper would address the concept of cybercrimes and cybersecurity measures, identify reasons for imminent cybercrimes in healthcare, those likely to be involved and their involvement, the involvement of data mining methods of stepping up healthcare cybersecurity and suggestion of checkmating the likely increasing rate of cybercrimes. Finally, it would itemize various possible combinatorial data mining techniques for alleviating healthcare cybercrime challenges to their looming threats.

This paper is organized as follows; first section presents the outline of cybersecurity, cyberspace and cybercrimes. Thereafter, classes of cybercrimes is propose then the cyber-attack stages. In addition, various proposed data mining techniques for expected solution to cybersecurity threats is presented. Conclusion and recommendation are however presented at the end of the paper.

1.1 Outline of Cybersecurity, Cyberspace And Cybercrimes

Cybersecurity is the act of protecting ICT systems and their content from both internal and external attacks (Fischer, 2016). In another perspective, cyberspace is an interactive field comprising of digital networks that are used to store, modify and communicate information. It also includes the internet and other information systems that support human daily businesses, infrastructure and services (Lobban, 2012). Hence, cybersecurity is thus concerned with ensuring cyberspace is safe from threats viz a viz cyber threats (Olayemi, 2014). In addition, cybersecurity can also be termed as the act of securing systems processes, data or information thereby hindering their exploitation (James, 2016).

Decades ago, IT experts and policy makers have expressed the increased concerns about the act of cybersecurity from cybercrimes processes which are deliberate attempts by unauthorized persons to access ICT systems usually with the aim of inflicting destruction, damage, disruption or other ungoverned actions (Schaeffer et al., 2009). Vulnerabilities increases at an alarming rate and breaches cause substantial impairment to individual and businesses alike. Healthcare clinical data and information are bond to face more threats in Nigeria as they become more complex and also as the attackers' pay offs increases. Hence, research, policy and analysis practices all have a paramount role to play

in protecting these data against these looming threats as each stages faces challenges that are distinct to cybersecurity (Abomhara & Køien, 2015).

Cybersecurity is fundamentally multidisciplinary, which points to the fact that it takes account of both technical and mathematical intuitions deeply and also of the social and behavioural sciences. The understanding of the real-world scenarios of digital systems and human systems behaviour depends solely on the wide range of disciplines. Therefore, effective cybersecurity measures will need to integrate insights from all area. Cybersecurity challenges, threats and opportunities are global, with diverse networks, services and attacks rarely confined to a single authority. Data are easily transmitted and transferred around the world which can be rapidly replicated and are sometimes extremely long-lived. This tends to make it harder to respond to attacks, identify the attackers and secure the data (Royal Society, 2016).

Cybersecurity domain is inherently a dynamically changing one, hence newer attacks such as multi-stage exploits and zero-day attacks can be significantly more diverse than old attacks in terms of technical implementation as well as the underlying protective measures themselves in the unending knowledge race between attackers and protectors (Tianfield, 2017). As cyber-attacks have evolved and grown in sophistication, cybercrimes detection techniques have also become much more sophisticated by monitoring an ever increasing amount of diverse heterogeneous security event sources. Cybersecurity basically is about the capability to defend the information infrastructure from cyber-attacks (Tianfield, 2017). Looking at the trend cybercrimes get increasingly persistent, advanced, and stealthy, cyber defence has to rely upon systematic and intelligence oriented methodologies. Steven Noel *et.al.* (2002) in (Barbara & Jajodia, 2004) presents an overview upon various techniques under different detection models, from misuse detection to anomaly detection respectively and introduce degree of susceptibility to attack as a way of characterizing intrusion detection activities. In overall, getting a grip of the data view is very important. Therefore, across different cyber control domains and over a practical period of time, there are actually voluminous and diverse sources of security information data. Hence, the ability to exploit and comprehend cybersecurity data enables or otherwise restricts the capability of cyber defence (Schultz, Eskin, & Stolfo, 2002; Varun, *et.al.*, 2006)

Furthermore, in order to deal with increasing information security threat in large scale data networks such as healthcare clinical data, countless kinds of security devices have been used in the past and these devices produce lots of security events. It can be very difficult to correlate events over such large amounts of data where they are heterogeneous in nature. The heterogeneity within a myriad of security techniques and systems which do not integrate well would cause difficulties for correlating security events. Hence, in order to mitigate or prevent attacks, awareness of attack is essential to be able to react and defend against attackers. Therefore, cybersecurity defenses can further improved by utilizing security analytics to look for hidden attack patterns and trends in healthcare

clinical data through the involvement of data mining techniques (Barbara & Jajodia, 2004; Lawrence, Kudyba, & Klimberg, 2008; Thuraisingham, *et.al.*, 2008)

1.2 Healthcare Cybersecurity Objectives

The following are the important objectives of healthcare cyber-security (Frank & Odunayo, 2013).

- reduce the vulnerability of patients' PHI, HER Information and Communication Technology (ICT) systems and networks.
- develop and nurture a culture of cyber security for both healthcare users and authority
- to work collaboratively with public, private and international entities to secure healthcare cyberspace.
- to help healthcare organizations understand the current trends in IT/cybercrime, and develop effective solutions.
- Availability of security measures.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality of healthcare data and information.

2. CLASSES OF CYBER-CRIMES

Cybercrimes are the major threats that every organization experienced when a loop hole is discovered by the attackers. There are diverse classes of cyber-crimes with respect to various organizations including the healthcare sector. The following are some of the classes of cybercrimes according to Ford & Siraj, (2015; Frank & Odunayo, (2013); James, (2016); and Schaeffer et al., (2009)

- (i.) Spamming– involves mass amounts of email or SMS being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/eliminating spam mail.
- (ii.) Viruses and worms: This is a major threat to everyday users and organizations. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software or operating system. Trojan horse is dicey. It appears to do one thing but does something else.
- (iii.) Cyber-Theft: Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a

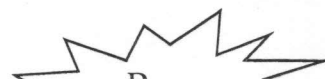
popular cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort

- (iv.) Financial Fraud- This is also known as “Phishing” scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim’s bank.
- (v.) Hacking: Hackers use the weaknesses and loop holes in organizations operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what u do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal. Important data of a company can also be hacked to get the secret information of the future plans of the organization.
- (vi.) Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.
- (vii.) Cyber harassment- is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.
- (viii.) Cyber laundering- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
- (ix.) Website Cloning: One recent trend in cyber-crime is the emergence of fake ‘copy-cat’ web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering financial details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster’s personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

3. CYBER ATTACKS STAGES

Regardless of whether an attack is performed internally (within) or externally (from hackers), targeted or untargeted or the attackers is using commodity or personalized tools, cyberattacks have a numbers of stages in common. Some of the attacks may meet their intended goals while others may be blocked by the measures in placed by the recipient.

An attack may consist of recurrent stages if it is carried out by a persistent enemy. The attacker is effectively probing target defenses for weaknesses such that if exploitable



will take them closer to their ultimate objective. Understanding the stages will help the targeted organization to prepare better in defending themselves. Quite a number of attack model describe the stages of cyber-attacks(NCSC, 2016). A sample of the stages of attacks is demonstrated in a simplified model below



Figure 1: Stages in a Cyber-attack (NCSC, 2016)

- Survey - investigating and analyzing available information about the target in order to identify potential vulnerabilities
- Delivery - getting to the point in a system where a vulnerability can be exploited
- Breach - exploiting the vulnerability/vulnerabilities to gain some form of unauthorized access
- Affect - carrying out activities within a system that achieve the attacker's goal

3.1 Characteristics of Healthcare Data Breaches

Healthcare organization data breaches of patient health information (PHI) that affected 500 or more individuals according to surveys (ESET, 2016; Serianu & Paladion, 2016)were characterized by:

1. type of breach and
2. location or mode of breached information.

However, data breach types can be categorized according to the following six (6) categories:

- hacking/IT incident,
- improper disposal,
- loss,
- unauthorized access/disclosure,
- theft, and
- other/unknown

In the same vein, data breaches are also categorized to the following locations or modes. The locations or modes includes seven (7) categories namely:

- desktop computer,
- Electronic Health Records (HER),
- email, laptop computer,
- network server,
- paper/films, and
- other location.

3.2 Types of Data Mining Techniques For Cybersecurity

There are several major data mining techniques that have been developed and used in data mining projects recently. Different data mining techniques including association, classification, clustering, prediction, and decision tree are used for detecting cyber-attacks either run on system audit data or network data like healthcare clinical data. We will briefly examine those data mining techniques in the following sections.

3.2.1 Association Rule Mining

Association is one of the best-known data mining technique. In association, a pattern is discovered based on a relationship between items in the same transaction. It looks for correlation that exists between different attributes in a dataset. It also discovers patterns based on a relationship of a particular item when such item are in transaction. That's is the reason why association technique is also known as relation technique. It captures implications between attributes values using the association rule mining algorithm. The concept of association rule mining is to find all co-occurrence relationships called associations. It finds frequent sets of items (e.g. combinations of items that are purchased together in at least N transactions in the database), and from the frequent items sets such as {X,Y}, generates association rules of the form: $X \rightarrow Y$ and/or $Y \rightarrow X$ (Barbara & Jajodia, 2004; Tianfield, 2017). In general, association rule mining is considered as an unsupervised techniques.

$$\begin{array}{l}
 \text{Rule: } X \Rightarrow Y \begin{cases} \nearrow \text{Support} = \frac{\text{freq}(X, Y)}{N} \\ \longrightarrow \text{Confidence} = \frac{\text{freq}(X, Y)}{\text{freq}(X)} \\ \searrow \text{Lift} = \frac{\text{Support}}{\text{Supp}(X) \times \text{Supp}(Y)} \end{cases}
 \end{array}$$

Figure 2: Association Rule Mining (Barbara & Jajodia, 2004)

The aim of association rule mining is to discover previously unknown association rules from the data. The technique would be a useful tool for cybersecurity in healthcare clinical data

3.2.2 Classification

Classification is a classic data mining technique based on machine learning. Basically, classification is used to classify each item in a set of data into one of a predefined set of classes or groups. Classification is the task of assigning database records to one out of a pre-defined set of target classes. The difficulty is that the target classes are not explicitly given in the database records but must be derived from the available attribute values

(Barbara & Jajodia, 2004). According to Tianfield (2017), Classification is the process of assigning data items to pre-defined classes. The result of these process will be a classifier based on association rules or decision trees. Classification method makes use of mathematical techniques such as decision trees, linear programming, neural network, and statistics. In classification, software models are developed that can learn how to classify the data items into groups.

There are two steps in classification : training and prediction stages (Tianfield, 2017). In the first step, classifier is trained by analyzing a training set made up of data instances and their associated class labels. Due to the class label of each training instance is provided, this is known as supervised learning. In the second step, the trained classifier is used to predict the class for unlabeled data instance.

3.2.3 K-Nearest Neighbour

The -Nearest Neighbour (k -NN) algorithm is a simple classification algorithm (Aggarwal & Chaturvedi, 2013; Barbara & Jajodia, 2004). Here all available cases (training data) are stored and new cases (test data) are classified based on a similarly measures (e.g. Euclidean distance) in the feature space. In the training data, the feature vectors are associated with respective class labels. For a new observed data, k -NN computes the distance between the new case an unlabeled vector) and all existing cases (labelled vectors) and then the test data is allotted to the class most common amongst its k nearest neighbours. It can be understood that the new observed data is categorized by the majority vote of its neighbours. If $k=1$, then the new data, without any doubt, is assigned to the class of its nearest neighbour. Large prediction time is needed if the value of k is large (Tianfield, 2017; Varun, *et.al.*, 2006)

3.2.4 Clustering

Clustering is a data mining technique that makes a meaningful or useful cluster of objects which have similar characteristics using the automatic technique. Clustering seeks to group database records so that the records within a given group/cluster are similar, whereas the records of different groups/clusters are dissimilar (Barbara & Jajodia, 2004). Evidently, the notion of similarity is key to this definition. According to Tianfield (2017); and Varun et al., (2006), classification is the process of seeking to describe the available datasets by grouping them into common clusters or categories.

Clustering could be utilized to detect anomaly. Unlike misuse detection which requires labelled data set and supervised algorithms, anomaly detections works on unlabeled dataset and uses unsupervised administrators. The clustering technique defines the classes and puts objects in each class, while in the classification techniques, objects are assigned into predefined classes. To make the concept clearer, we can take book management in the library as an example. In a library, there is a wide range of books on various topics available. The challenge is how to keep those books in a way that readers can take several books on a particular topic without hassle. By using the clustering

technique, we can keep books that have some kinds of similarities in one cluster or one shelf and label it with a meaningful name. If readers want to grab books in that topic, they would only have to go to that shelf instead of looking for the entire library. The classification scenario is also very applicable to cybersecurity in healthcare clinical data. Examples of clustering models are *k*-means algorithm, *k*-medoids clustering algorithm, expectation maximization clustering (EMC), etc.

3.2.5 Prediction – Support Vector Machine (SVM)

The prediction, as its name implied, is one of a data mining techniques that discovers the relationship between independent variables and relationship between dependent and independent variables. Support Vector Machine (SVM) is supervised learning for classification and prediction methods. SVM is a classifier based on finding a separating hyperplane in the feature space between two classes in such a way that the distance between the hyperplane and the closest data points of each class is maximized (Tianfield, 2017). SVM separates data points into two classes +1 and -1 using hyperplane. Class +1 represents normal data and class -1 for suspicious data. SVM maps the input vector into a higher dimensional feature space and obtains the optimal separating hyperplane in the higher dimensional feature space. In the event when the two classes are not separable, slack variables are added and a cost parameter is assigned for the overlapping data points (Thuraisingham, *et.al.*, 2008). SVMs are well known for their generalized tendency and are particularly useful when the number of features, *m*, is high and the number of data points, *n*, is low (i.e. $m \gg n$).

3.2.6 Decision Trees

The decision tree is one of the most commonly used data mining techniques because its model is easy to understand for users. Decision tree is a recursive and tree-like structures for expressing classification rules (Tianfield, 2017). It uses divide and conquer method for splitting of the data according to attribute values. The splitting process repeats for every child node till all elected attributes are considered. In decision tree technique, the root of the decision tree is a simple question or condition that has multiple answers. Each answer then leads to a set of questions or conditions that help us determine the data so that we can make the final decision based on it. Decision tree converts the given dataset into a tree structure. The nodes of the tree represent the features and the edges represent the association between the features by value or features. Each leaf node i.e. the lowest level of the node represents the child label (Tianfield, 2017), decision tree is supervised learning and it takes a set of classified data as input, executes the algorithm on that and provides a tree as output, where each leaf can be expressed as a decision and each intermediate node epitomizes a test. To classify a data item, it proceeds from root node to leaf node. The name of the class at the leaf node is the class of an unknown data item.

4. REVIEW OF RELATED LITERATURE

Several studies have been proposed by using diverse techniques in data mining to carry out data analysis and prediction of cyber-attacks detection. First on the list of cyber-attacks detection is the data analysis. The massive data collected by acquisition layer is for centralized storage and analysis in analysis tier, so as to extract the major information concerned. These studies includes:

CGI (2015) focused on the importance of cyberprivacy and cybersecurity for health data. They tried to make a clear explanation between cyberprivacy and cybersecurity to solve numerous misconceptions about the two elements with respect to health data. They develop a framework in a five stage element and demonstrate how they are aligned. The five key elements are for privacy (minimized data, limited use, data quality and assurance, security, audit and accountability) while for security (identification, protection, detection, respond and recovery)

Antony, Singh, & Leavline (2013) focused on using data mining techniques based on supervised learning based intrusion detection system to tackle cybersecurity in network systems. They analyzed the various changes of threats and attacks in network in recent times, various network sniffing, snooping tools for capturing network data and log data for analysis and learning. They make use of Naïve Bayes IB1 (nearest neighbour principles), C4.5 supervised learning algorithms and simulated it by the use of data training tool Weka with standard benchmark training and testing datasets.

Thuraisingham et al., (2008) applied different data mining techniques for cybersecurity. Their work were applied to applications not limited to malicious code detection by mining binary executables, network intrusion detection by mining network traffic anomaly detection, and data stream mining. They developed different tools for data mining such as link analysis and association rule mining for detecting abnormal patterns. One of their future projects is exploring researching active defense. They also implement data mining techniques for Botnet detection.

Varun et al., (2006) predicted a model they tagged MINDS for cybersecurity. They focused on the use of clustering algorithm with emphasis on Anomaly detection approach. Their own work is a batch-mode implementation procedure that analyzes data in windows of 20 minutes. For each 20 minute observation period, they transform the Netflow data into a summary data set. With their focus on incoming scans, each new summary record correspond to a potential scanner i.e. pair of external source IP and destination port (SIDP)

Kalus Julisch (2002) in Barbara & Jajodia (2004) proposed data mining techniques for intrusion detection using a stand-alone technique of data mining. The use of data mining in isolation has adversely affect the quality of their results obtained. They discovered that the use of data mining isolation application is a dangerous activity, easily leading to the discovery of meaningless or even misleading patterns.

5 METHODOLOGY

Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. The projected methodology would be tailored to meet the imminent trends of threats and vulnerabilities looming the healthcare sector in Nigeria. The following are the various projected methodology for cybersecurity breaches in healthcare sector in Nigeria.

- (i.) Access Control and Identity Management: The username/password combination has been a fundamental of computer access control since the early 1960s.
- (ii.) Authentication: Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered.
- (iii.) Malware scanners: Software that regularly scans files and messages for malicious code.
- (iv.) Firewalls: A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage.
- (v.) Cryptography: It is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit

6. EXPECTED SOLUTION TO CYBERSECURITY BREACHES IN NIGERIA HEALTHCARE SECTOR

The results of a breach involved in the healthcare sector be it hospitals, clinics, researchers and patients can range from annoying to catastrophic. Patients could be harmed or even die. Several people both patients and healthcare workers equally could be inconvenienced by systems going down. Likewise, bad publicity could harm clinics and hospitals in areas where consumers have choices. Prevention is the best solution but it, too, poses challenges. Experts, according to CGI (2015); Cheung, *et.al.*, (2011); Reddy & Reddy, (2015); and Serianu & Paladion, (2016), offer these ideas for shoring up security to prevent or mitigate attacks within the healthcare sector:

- Education and awareness: In the past, it was much more challenging implementing cybersecurity features because people didn't consider it a must having the notion of never been hacked, nobody stole any of my information, so I'm fine. But nowadays, the awareness is global. Continued education will help ensure that the people who need to use the secure systems are on board.
- Simplicity. The more complex a system is, the harder it can be to keep updated to guard against cyberattacks. Keep it simple idea is better. Organizations are advised not to have too many disparate things where updates are required as it breaks everything else. Hence, the hotter, new devices that a healthcare organization have, the more openings they should have.

- Backup systems: When cybersecurity systems fail to prevent an attack, good backups can make it easier to recover.
- Emergency planning: Cybersecurity may be an emerging challenge, but emergency managers can tackle it by using strategies similar to those they use for other situations.
- Constant vigilance: Both manufacturers and owners of devices bear some responsibility for preventing attacks. Users and operators devices should be prepared to follow best practices for installing and testing the updates. This is done by starting with the fundamentals of evaluating bugs and vulnerabilities as well as information sharing.
- Realistic regulations: Cybersecurity plans need to keep in mind the mission and culture of the health-care industry. It is common in Nigeria for government agencies that regulate the healthcare systems to be slow with their approval. The regulatory space is not equipped today to handle the evolving nature of threats and the speed with which technological development is happening.
- Healthy attitude toward risk: It's easy to blame doctors for being reluctant to learn a new electronic medical record system, for example, update for their computer systems. Researchers need to be able to share information and produce new drugs. Healthcare providers need to be able to exchange patient information. The key is to consider cybersecurity through the lens of risk management.
- Cooperation: So many of the players in the healthcare sector are connected to each other and thus an attack on one entity with weaker security could threaten others. Hence, hospitals need to notify each other of attempted attacks so other hospitals can prevent them. In addition, a long-term solution would be for device developers to "develop products and services that are hard to compromise.

7. CONCLUSION AND RECOMMENDATIONS

Data mining techniques for cybersecurity in healthcare clinical data is a very active research area. Different data mining techniques has been itemized in this paper with their relevance to clinical data which can be used to detect abnormal patterns or intrusions in healthcare database system. Due to the involvement of these techniques, developers and users can now make all kinds of correlations which also raises privacy concerns. There's no doubt that cyber-attacks detection is big data processing and analytics problem. Data driven framework makes a systematic approach to addressing cyber-attacks detection issues. As an domain in itself, data mining for cybersecurity has a fairly established set of models ad techniques, however, facing advanced cyber-attacks problems, one of the practical challenges lying ahead is how the models of supervised and unsupervised learning, the models of cyber-attacks detection and the offline and online system models should be interwoven all together into an organic robust cyber-attack detection system to curb the looming menace in Nigeria healthcare sector There is no single answer for success, but by working across both public and private healthcare sector through

partnerships and by advancing security measures particularly with regard to mission critical systems, processes and applications that are connected into cyberspace, healthcare systems will be able to work towards a future environment that is both open and secure and prosperous.

REFERENCES

- Abomhara, M., & Køien, G. M. (2015). Cyber Security and the Internet of Things : Vulnerabilities , Threats , Intruders. *Journal of Cyber Security*, 4, 65–88. <http://doi.org/10.13052/jcsm2245-1439.414>
- Aggarwal, P., & Chaturvedi, M. M. (2013). Application of Data Mining Techniques for Information Security in a Cloud: A Survey. *Int'l J. of Computer Applications*, 80(13), 11–17.
- Antony, D. A., Singh, G., & Leavline, E. J. (2013). Data Mining in Network Security - Techniques & Tools: A Research Perspective. *Journal of Theoretical and Applied Information Technology*, 57(2), 269–278.
- Barbara, D., & Jajodia, S. (2004). Applications of Data Mining in Computer Security. *Kluwer Academic Publishers*, 1–273.
- Brookson, C. (2016). Tackling the Challenges of Cyber Security. *ETSI Whitepaper*, (18), 1–11.
- Cameron F., K., & Gallagher, P. (2012). Cybersecurity, Innovation and the Internet Economy. *The Department of Commerce Internet Policy Task Force*, (June).
- CGI. (2015). Cyberprivacy and Cybersecurity for Health Data. *CGI Group Inc*, 1–8.
- Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge Based Learning in Cybersecurity Education. *University of Massachusetts Journal*, 1–6.
- ESET. (2016). The State of Cybersecurity in Healthcare Organizations in 2016. *Ponemon Institute Research*, 1–32.
- Fischer, E. A. (2016). Cybersecurity Issues and Challenges: In Brief. *Congressional Research Service*, 1–9.
- Ford, V., & Siraj, A. (2015). Applications of Machine Learning in Cyber Security. *ResearchGate*, (December), 1–7.
- Frank, I., & Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *Int'l Journal of Cognitive Research in Science, Engineering and Education*, 1(1), 1–11.
- James, C. (2016). Cybersecurity: Threats, Challenges, Opportunities. *ACS*, (November).
- Lawrence, K. D., Kudyba, S., & Klimberg, R. K. (2008). *Data Mining Methods and Applications*. Taylor & Francis Group, LLC.
- Lobban, I. (2012). 10 Steps to Cyber Security. *Centre for the Protection of National Infrastructure*, 1–20.
- NCSC. (2016). Common cyber attacks : reducing the impact. *National Cyber Security Ceter*, (January), 1–16.

- Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *Int'l Journal of Sociology Ad ANthropology*, 6(3), 116–125. <http://doi.org/10.5897/IJSA2013.0510>
- Reddy, G. N., & Reddy, G. J. U. (2015). A study of Cyber Security Challenges and its emerging trends in latest technologies. *Int'l Journal of Scientific & Engineering Research*, 1–6.
- Royal Society, T. (2016). *Progress & Research in cybersecurity - Supporting a resilient and trustworthy system for the UK*. Science Policy Centre.
- Schaeffer, B. S., Chan, H., Chan, H., Ogulnick, S., Schaeffer, B. S., Chan, H., ... Ogulnick, S. (2009). Cyber Crime and Cyber Security : *Whitepaper for Franchisors, Licensors and Others*, 1–17.
- Schultz, M. G., Eskin, E., & Stolfo, S. J. (2002). Data Mining Methods for Detection of New Malicious Executables. *Columbia Univ. Journal*, 1–12.
- Serianu, & Paladion. (2016). Nigeria Cyber security report 2016. *United States International University - Africa*, 1–60.
- Thuraisingham, B., Khan, L., Masud, M. M., & Hamlen, K. W. (2008). Data Mining for Security Applications. *IEEE/IFIP Int'l Conference on Embedded and Ubiquitous Computing*, (June), 1–6. <http://doi.org/10.1109/EUC.2008.62>
- Tianfield, H. (2017). Data Mining Based Cyber-Attack Detection. *System Simulation Technology*, 13(2), 90–104.
- Varun, C., Eric, E., Levent, E., Gytogy, S., & Vipin, K. (2006). Data Mining for Cyber Security. *Springer*, 1–20.