Analysis of Interdependency of ICCT Underlying Technologies and Related New Research Opportunities with Special Emphasis on Cyber Security and Forensic Science

P. S. Aithal[1] & Shubhrajyotsna Aithal[2]
[1]Professor, Srinivas University, Mangalore - 575001, Karnataka State, India
E-mail: psaithal@gmail.com
[2]Dept. of Chemistry, College of Engineering & Technology, Srinivas University, Mangalore, India
E-mail: shubhraaithal@gmail.com

ABSTRCT

Information Communication and Computation technology (ICCT) is a 21st-century name of Information Communication Technology (ICT) covers a broader definition of advances in computer science technologies and covers about twelve underlying emerging technologies. ICCT and Nanotechnologies are considered as building blocks of the Universal Technology System. These 12 underlying technologies include: Artificial intelligence & robotics, Blockchain technology, Data science & business intelligence, Cloud computing, Cybersecurity & forensic science, 3D-printing, Internet of Things, Information storage technology, Mobile business technology, Online education technology, Quantum computing, and Virtual & augmented reality. These ICCT underlying technologies are expected to change the current solutions for various problems in industries and society and hence considered as emerging technologies of the 21st century and expected to convert the current human generation as tech-generation. While studying these technologies, it is found that they are capable to solve many problems of human beings in society including problems related to human comfortability and dreamy desires. It is observed that the application patterns of these technologies while solving real-world problems show a strong interdependency and hence enhanced opportunities. In this paper, some of the current status and future prospective new research opportunities using a combination of two or more ICCT underlying technologies with special emphasis on cyber security and forensic science in primary, secondary, tertiary, and quaternary industries are discussed.

Keywords: ICT, ICCT, Universal Technologies, Emerging technologies, Cyber security, Forensic science, Blockchain technology, IoT, AI, VR, Cyber-physical systems, Industry applications of technology

1. Introduction :

CS, IT, ICT and emerging technologies with the base of Electronics & Communication technology, Telecommunications, Computer Science, and Information technology are now combined called as Information Communication and Computation Technology (ICCT). ICCT is growing its base through 12 identified underlying technologies and becoming part of emerging technologies of 21st century [1-3]. These ICCT underlying technologies are considered as general-purpose technologies contributing substantially to solve many problems of various industry sectors to make human life comfortable. ICCT underlying technologies along with another important general-purpose technology called nanotechnology forms a group of technologies called Universal technologies [4-5]. These 12 underlying technologies include: Artificial intelligence & robotics, Blockchain technology, Data science & business intelligence, Cloud computing, Cybersecurity & forensic science, 3D-printing, Internet of Things, Information storage technology, Mobile business technology, Online education technology, Quantum computing, and Virtual & augmented reality. These ICCT underlying technologies are expected to change the current solutions for various problems in industries and society and hence considered as emerging technologies of the 21st century and expected to convert the current human generation as tech-generation [6-9]. While studying these technologies, it is found that they are

capable to solve many problems of human beings in society including problems related to human comfortability and dreamy desires. It is observed that the application patterns of these technologies while solving real-world problems show a strong interdependency and hence enhanced opportunities [10-13]. In this paper, some of the current status and future prospective new research opportunities using a combination of two or more ICCT underlying technologies with special emphasis on cyber security and forensic science in primary, secondary, tertiary, and quaternary industries are discussed.

2. ICCT Underlying Technologies:

ICCT deals with generation, processing, storing, transmitting, receiving, further processing, and use of data and information to carry out certain pre-defined functions in any digital system. ICCT comprises mainly 12 underlying technologies including Artificial intelligence & robotics, Blockchain technology, Data science & business intelligence, Cloud computing, Cybersecurity & forensic science, 3D-printing, Internet of Things, Information storage technology, Mobile business technology, Online education technology, Quantum computing, and Virtual & augmented reality [1-13].

Cyber security technology is a set of processes, practices, and procedures in digital systems designed for protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious arrack, damage, or unauthorised access by third party during any stage of communication and processing. Cyber security deals with testing and protecting digital systems and to make it inherent to such security attacks by means of studying checking vulnerability of digital systems through ethical hacking. Precaution is better than curing is rightly applicable slogans for digital system security. The objectives of all organizations & individuals who are using digital system and digital communication want to protect all digital systems from malicious arrack, damage, or unauthorised access by third party during any stage of communication and processing, and the objectives of the hackers of Cyber systems are to hack systems or networks for their illegal tangible or intangible benefits [14].

Similarly, Forensic science, also called as criminalistics, is the application of science to criminal and civil laws, mainly during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure. It also includes preservation, identification, extract, protection, documentation and use of criminal evidence to support the procedure of catching and punishing the criminals and proving their illegal activities scientifically so that it is legally acceptable by Court for prosecution. If the evidence is electronic – digital data form, you can do some processes to go deep into it. On other hand, these digital data can be manipulated illegally by cyber hackers.

The objectives of oorganizations & Individuals are to protect all digital systems from malicious arrack, damage, or unauthorised access by third party during any stage of communication and processing. The objectives of Cyber system Hackers are to hack systems or networks for illegal benefits. The objectives of criminals are how to make a Crime without exposing evidence. The objectives of forensic experts are how to make identification, protection, and use of criminal evidence to support the procedure of catching the criminals and proving their illegal activities scientifically. Thus, the rresearch strategy in cyber security and forensic science is to develops ideas, techniques, Procedure & Software, to control fraudulent activities which are carried out by third party either for profit or for intentional to troubling others.

The objective of ICCT underlying technologies is to develop super intelligent machine which thinks and makes optimum decisions faster than human beings. This will lead to human robotics which can mimic human intelligence and supports total automation in all industries. But such system/machine has a potential threat of software security for malfunction, which may lead total disaster. Thus, research in cyber security and forensic science should go in parallel with research and development in other areas of ICCT underlying technologies.

3. Objectives of the Paper :

(1) To discuss the importance of ICCT underlying technologies towards developing super-intelligent machine and security aspects of such machines.

(2) To show the interdependency of ICCT underlying technologies based on previous, current scholarly research publications.

(3) To analyse the future prospective and the new research opportunities using a combination of two or more ICCT underlying technologies with special emphasis on cyber security and forensic science in primary, secondary, tertiary, and quaternary industries.

4. Interdependency of ICCT Underlying Technologies :

4.1 Cybersecurity and Blockchain Technology :

Cybersecurity and Blockchain Technology are Complementary & interdependent technologies used for information-based theft, corruption control [15-16]. The blockchain/Distributed Ledger Technology (DLT) has the following attractive features :

(1) It cannot be corrupted by a third party.
(2) It uses decentralized technology which transfers control and decision-making from a centralized entity to a distributed network.
(3) Enhanced security due to distributed ledger control.
(4) Distributed ledgers enhance openness and decentralization.
(5) Consensus mechanism for fault tolerance.
(6) Faster settlement time by means of longer secured blocks of information.

The above features of blockchain technology promise solutions to many current problems and challenges different industrial applications related to IoT, cryptocurrency, digital medical records, etc. Thus, blockchain technology is anticipated to be a breakthrough technology and provides a paradigm shift to digital transactions, especially in the areas of authentic information communication, including financial services, energy, healthcare, educational training, and IoT-based production and service industries. One of the challenges of blockchain technology is to improve the technology to make it further vulnerable to cybersecurity threats. This includes how companies manage cybersecurity risks using their strategic and operational objectives for identifying, analysing, and controlling their relevant risk levels. Researchers use various information security risk assessment models to classify and understand the incidents that happened against cybersecurity vulnerabilities in blockchain technology usage [17 -30]. This shows the interdependency of cybersecurity and blockchain technology and the research in blockchain technology indirectly contributes to improve various cybersecurity challenges and creates new ideas & concepts in it and vice-versa.

4.1.1 Reported Research:

A good amount of research and developments are reported in journals and magazines on improving the quality of cybersecurity in blockchain technology applications and the use of blockchain concepts in the industrial applications where high-level securities are required. This include:

- Blockchain's roles in strengthening cybersecurity aspects to protect the privacy of documents.
- A comparative study of blockchain application and cybersecurity issues in cryptocurrencies like Bitcoin.
- How to use blockchain for enhancing cybersecurity and privacy in various systems including architectures, challenges, and applications.
- Analyses and assessment of blockchain technology potentials for improving the cybersecurity of financial transactions.
- Examining and improving Critical Infrastructure Protection using Blockchain-Based Technology.
- Blockchain technology usage in the future of business cyber security and accounting.
- Use of blockchain for cybersecurity, optimization, and compliance of various supply-chain systems.
- The role of blockchain technology and concepts in strengthening cybersecurity and protecting the privacy of human beings.

4.1.2 Future Research Scope :

(1) Blockchain technology from the cybersecurity perspective in healthcare sectors.

(2) Handling blockchain threats and vulnerabilities using cybersecurity ideas to provide security and privacy.
(3) Development of blockchain cybersecurity vulnerability assessment framework.
(4) Application of Blockchain within *various Industry* Cybersecurity Framework.
(5) Blockchain-based cybersecurity models in various networks including IoT.
(6) Blockchain as a solution to Drone Cybersecurity, Autonomous vehicle Cybersecurity.
(7) Optimization of Blockchain Solution for Enhancing Cybersecurity Defence of IoT networks.
(8) Enhancing Cybersecurity through Blockchain technology in Smart manufacturing using IoT.
(9) Perspectives of Blockchain in Cybersecurity for industrial information transactions for system & process automation.
(10) How to achieve ideal security for digital systems through integrated Blockchain-Cybersecurity techniques.

4.2 Cybersecurity and Internet of Things :

Internet of Things (IoT) are vulnerable for Cybersecurity attacks. Being a backbone of many industries to connect and automate cyber-physical systems, it is considered as 4th generation technology called technology of industry 4.0. It is found that IoT are vulnerable for Cybersecurity attacks [31-45]. As per the definition, IoT is a wired and wireless network of various things including electronic, computing, optical devices/objects, and human beings connected virtually by means of internet or intranet for enabling them to exchange data and information. Every object in IoT network has a unique identifier (UID) and involves in transfer data and information over a network without interaction or control of human-to-human or human-to-computer. Such a connection of physical things/objects to the Internet makes it possible to access remote sensor data and to control the physical world from a distance [13].

4.2.1 Reported Research:

- Legal aspects of Cybersecurity in the Internet of Things,
- An ontology-based cybersecurity framework for the internet of things,
- Computational intelligence enabled cybersecurity for the internet of things,
- New Generations of Internet of Things Datasets for Cybersecurity Applications
- Cryptographic technologies and protocol standards for Internet of Things

4.2.2 Future Research Scope:

(1) New challenges for cybersecurity in Industrial IoT applications.
(2) Use of Blockchain Cybersecurity ideas in IoT secured performance
(3) Ideas & concepts from IoT models & Cybersecurity methods to develop new manufacturing systems.
(4) Building Cyber-Resistant Interactions in the Industrial Internet of Things.
(5) Internet of Things in Cybersecurity: The Future trends and Risks.

4.3 Cybersecurity and Artificial Intelligence :

Artificial intelligence is a field of ICCT with an objective of adding human intelligence to machines to help them to make independent decisions. Such machines are vulnerable to cybersecurity attacks [46-52]. Machines with artificial intelligence capability are specialized to carry out functions like speech recognition, learning, planning, problem-solving, pattern recognition, and hence decision-making. Artificial intelligence machine mimics cognitive functions of human beings associated with human minds, such as learning & memorizing and decision-making for solving both structured and unstructured problems [13].

4. 3. 1 Reported Research:

- Artificial intelligence in cyber security systems through new concepts and automation,

- Harnessing artificial intelligence capabilities to improve cybersecurity in physical systems,
- A bio-inspired hybrid artificial intelligence framework for cyber security,
- Ethical challenges of applications of artificial intelligence in cybersecurity,
- Providing Cyber Security using Artificial Intelligence–A survey,

Role of artificial intelligence, machine learning, and deep learning in cyberspace shows the interdependency of cybersecurity and blockchain technology and the research in blockchain technology indirectly contributes to improve cybersecurity challenges and creates new ideas & concepts in it and vice-versa.

4. 3. 2 Future Research Scope:

(1) Use of Artificial intelligence techniques and systems in improving cybersecurity for total vulnerability.
(2) Cybersecurity systems for new artificial intelligence models.
(3) Providing cybersecurity using Artificial Intelligence & robotics.
(4) Role of artificial intelligence, machine learning, and deep learning in designing and developing cybersecurity systems.
(5) ABCD stakeholders' analysis of artificial intelligence in cybersecurity and cybersecurity in artificial intelligence.

4. 4 Cybersecurity and Cloud Computing :

Cloud computing is a system of using shared computing resources from distance through internet technology. Cloud computing is one of the advents of ICCT. Due to the ubiquitous nature of usage of computing and storage facilities remotely, cloud computing technology is flexible in scaling and has become an important topic of research related to value creation for computing processes in the business. Cloud computing model provides both hardware as well as software to its clients to process the data and information online as a rental service. Cloud computing systems are also vulnerable to cyber-attacks [53-64].

4. 4. 1 Reported Research:

- Various cybersecurity models in cloud computing environments.
- Teaching cybersecurity using the cloud.
- Cybersecurity management in cloud computing: semantic literature review and conceptual framework.
- Measuring the cybersecurity of cloud computing: A stakeholder cantered economic approach.
- New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks.
- Cybersecurity and Cloud Computing in the Health Care and Energy Sectors.
- Cybersecurity threats in cloud computing.
- Next-generation cybersecurity through a blockchain-enabled federated cloud framework.
- A deep learning approach on cyberattack detection in a mobile cloud computing environment.

4. 4. 2 Future Research Scope:

(1) Cybersecurity in cloud computing-based systems and environments.
(2) Use of cybersecurity and cloud computing in various industry sectors.
(3) Quality assessment of cybersecurity systems used in a cloud computing environment.

4. 5 Cybersecurity and Data science & business intelligence :

Big data generated by various live events are analysed to find inherent patterns of useful information as business intelligence is an integral part of all business intelligence systems. Data Science and business intelligence focus on handling a huge amount of data that are continuously generated in any data capturing process or business process, to analyse using various qualitative analytical techniques

and mathematical models. This will help the decision maker to study the information pattern as descriptive information, predictive information, or prescriptive information for supporting improvements in their decisions related to future business aspects.

Predictive analytics has huge advantages in decisions related to various functional areas like marketing analytics, Retail Analytics (Customer Analytics / Supply Chain Analytics), Pricing Analytics, Financial analytics, social media analytics, sports analytics, and Healthcare analytics. The security aspects in both big data and business intelligence processing systems are important for making information fool-proof [65-71].

4. 5. 1 Reported Research:

- Identifying pitfalls of using data science in cybersecurity,
- Security analytics in Bigdata analytics for cybersecurity,
- Necessity of Data Science for Enhanced Cybersecurity,
- Data Science and its applications in Cyber Security,
- How to Overcoming Cyber Security Challenges Using Data Science.
- Cybersecurity in the big data era from securing big data to data-driven security.

4. 5. 2 Future Research Scope:

(1) Challenges of using Data Science in Cybersecurity,
(2) Big data analytics for Cybersecurity called Security analytics,
(3) Principles of data science for enhanced Cybersecurity and models,
(4) How cybersecurity is important in Data science technology ?
(5) New era of Cyber-secured the big data to data-driven security.

4. 6 Cybersecurity and 3D-printing :

3D printing is also called an additive digital manufacturing system. 3D printing is an ICCT application where a 3D object can be created using materials that are joined layer by layer and solidified using various processes under computer control. In 3D printing, an object is created by laying down successive layers of material until the object is physically formed. 3D printing can be divided into metal, fabrics, bio, and a whole host of other industries with many applications in many industries worldwide [72-80].

4. 6. 1 Reported & Future Research:

- Detecting and preventing attacks using cybersecurity principles in 3D printing systems,
- Identifying positioning-based attacks against 3D printed objects and the 3D printing process.
- Cyber security for additive manufacturing.
- Physical security and cyber security issues and human error prevention for 3D printed objects and detecting the use of incorrect printing material.
- Cybersecurity for digital design & manufacturing,
- Cybersecurity risks and mitigation strategies in additive manufacturing.

4.7 Cybersecurity and Information Storage Technology :

Information storage technology is used to design and develop various digital storage devices to store and retrieve data and information in digital form. The current trend is to enhance the capability of storage devices to store huge amounts of data and information at high speed and low cost. Many new approaches of storing digital signals are under consideration to fulfill the demand, including semiconductor storage, hologram storage, optical storage, DNA-based digital storage, etc. that have anticipated capability to store data & information in Terabytes, Petabytes, Exabytes, Zettabyte, and even Yottabyte in order to cater the demand of forthcoming information storage applications. Security

aspects both in small scale and large scale storage devices are important issues in the digital era [81 – 90].

4. 7. 1 Reported & Future Research:

- Study on data security policy based on cloud storage,
- Ensure data security in cloud storage,
- Data security and privacy protection for cloud storage,
- Self-encryption scheme for data security in mobile devices,
- Enhanced three-factor security protocol for consumer USB mass storage devices,
- Various adaptive techniques using advanced encryption standards to implement Hard Disk Security, and
- Improving hard disk data security using hardware encryptors.

4. 8 Cybersecurity and Mobile Business Technology :

E-business and M-business are two new business models called as click and mortar business model. The internet, online marketing, and customer servicing technologies provide ubiquitous selling proposition without the constraints of country boarders. The digital devices and medium used for mobile business models including mobile phones, other digital display devices, need information security aspects to monitor and control accurate information communication and storage. Thus, security aspects are inherent part of mobile devices especially for financial information transactions [91-100].

4. 8. 1 Reported & Future Research:

- The need for antivirus applications for smart phones, to provide cybersecurity and to handle mobile communication threats.
- To handle cybersecurity challenges in digital economy,
- To develop a resilient cybersecurity framework for Mobile Financial Services,
- To study on User's Response to Cyber Security Challenges related to Mobile Devices & systems,
- A Cybersecurity Approach for Evaluating Mobile Agents,
- M-commerce liability and security breaches in mobile payment for m-business sustainability,
- Emerging cybersecurity threats in large and small firms in primary, secondary, tertiary, and quaternary industries,
- Cybersecurity vulnerabilities in mobile fare & rent payment Ap plications.

4. 9 Cybersecurity and Online Education Technology :

Online education is an ideal solution to educate every one irrespective of their geographical and financial background. Transformation of traditional classroom-based education system to massive online open access (MOOC) system need advanced, low cost, ubiquitous ICCT. Initially MOOC is considered as complementary to traditional campus-based education system, but as time progress, it may replace entire higher education industry online & ubiquitous. Higher education system is originally designed to enhance knowledge, skills, experience, and confidence to improve the living conditions of human beings, can be now offered online using wireless video channels with better effectiveness. The ubiquitous online education offered through ICCT online technology in all subjects at any level using simulation may out pass the traditional laboratory-based training in higher education system [101-108].

4. 9. 1. Reported & Future Research:

- The role of cyber-security in information technology education,
- E-Learning using the blackboard system in light of the Quality of Education and Cyber security,
- Cyber threats to online education based on customers and service providers perception.

- Security Issues Related to E-Learning Education,
- Privacy and security issues in online social networks,
- Security risks and protection in online learning & payments,
- Security issues in e-learning platforms,
- Implementation of e-learning into the process security education in universities.

4. 10 Cybersecurity and Quantum Computing :

High-speed computers are essential to fulfill the computation needs of various industries. Quantum computers based on optical signals have the capability to switch faster and provides computation requirements to many organizations simultaneously. Researches on advanced quantum and optical computers using optical logic gates and flip-flops fabricated by nanocomposites are in progress and expected to break through with full potentiality during this century. High-speed computation and data storage using nanotechnology-based quantum computers expected to revolutionize the entire computer industry. Security aspects in quantum computers are expected to pose new challenges and new opportunities for engineers and scientists [109-119].

4. 10. 1 Reported & Future Research:

- Cybersecurity in a Post-Quantum World to know how quantum computing will change the world of Cybersecurity.
- Quantum Computing Era with new research and design perspective of cybersecurity,
- Will cybersecurity be compromised in Quantum computing?,
- Research on unsettled topics concerning the impact of Quantum Technologies on Automotive Cybersecurity,
- Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications.
- A Pragmatic Analysis of Pre-and Post-Quantum Cyber Security Scenarios.
- Towards a Quantum Internet and Post-pandemic Cyber Security in a Post-digital World.
- How Quantum Cryptography and Quantum Computing can make Cyber-Physical systems more secure.

4. 11 Cybersecurity and Virtual Reality :

Virtual and augmented reality are applications of ICCT to create an artificial environment using computer-based software to mimic a real environment to the user to suspend their belief to accept it as a real environment. Virtual reality is primarily experienced by users through any two of the five senses supported by sight and sound. Virtual reality is currently used in simulated training and education as well as the simulated game environment. Cyber security technology also plays an important role in providing security solutions while processing information [120- 127].

4. 11. 1 Reported & Future Research:

- Using virtual reality to enforce principles of cybersecurity,
- Towards designing agent based virtual reality applications for cybersecurity training,
- Alert Characterization by Non-expert Users in a Cybersecurity Virtual Environment: A Usability Study.
- A distributed virtual laboratory architecture for cybersecurity training.
- Industrial security solution for virtual reality.
- Virtual Reality Surveillance.
- Ethics emerging: the story of privacy and security perceptions in virtual reality.

4.12 Cybersecurity and Forensic Science :

Forensic science is a multidisciplinary technique that uses systematic scientific methods and expertise to investigate crimes or examine crime related evidence to support the prosecution of criminals in the

court of law. It uses various evidence from a diverse array of disciplines from fingerprints, retinal & DNA analysis, to anthropology and wildlife forensics. Since digital processes are used to generate, process, store, transmit and regenerate crime information in forensics, security aspects are considered to be important [128-134].

4. 12. 1. Reported & Future Research:

- Cybersecurity and Mobile Device Forensic.
- Cyber Forensic Science to Diagnose Digital Crime.
- Current Challenges of Digital Forensics for evidence management in cybersecurity.
- Non-invasive Biosensors for Forensics, Biometrics, and Cybersecurity.
- ICCT underlying technology trends in Digital Forensics and Cybersecurity.
- Challenges and future paradigms of next-generation digital forensics.
- Digital forensic readiness framework for smart systems and smart homes.

5. Conclusion :

Based on the above analysis, it can be concluded that:

- ICCT underlying Technologies are emerging as 21st Century technologies.
- They are growing as independent technologies.
- It is observed that they are also inter-dependent Technologies.
- Blockchain and Cybersecurity are Complementary technologies.
- By considering ICCT underlying technologies as inter-dependent technologies, the scope of application of these technologies becomes multi-fold.
- Huge opportunity for Researchers in CS & FS as interdisciplinary to create new security ideas, processes, devices, and systems that are vulnerable to any type of cyber-attack as ideal cyber systems.

References :

[1] Aithal, P. S. (2019). Information Communication & Computation Technology (ICCT) as a Strategic Tool for Industry Sectors. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *3*(2), 65-80.

[2] Aithal, P. S., & Aithal, S. (2019). Management of ICCT underlying Technologies used for Digital Service Innovation. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *4*(2), 110-136.

[3] Ganesha, H. R., & Aithal, P. S. (2020). Inappropriate Adaptation of Information Communication and Computation Technologies (ICCT) by Indian Brick-and-Mortar Lifestyle Retailers–Insights from an Experiment. *Information Communication and Computation Technologies–The Pillar of Transformation, New Delhi Publishers, India*.

[4] Aithal, P. S., & Aithal, S. (2018). Study of various General-Purpose Technologies and Their Comparison towards developing Sustainable Society. *International Journal of Management, Technology, and Social Sciences (IJMTS), (2018), 3*(2), 16-33.

[5] Aithal, P. S., & Aithal, S. (2019). Digital Service Innovation Using ICCT Underlying Technologies. In *Proceedings of International Conference on Emerging Trends in Management, IT and Education* (Vol. 1, No. 1, pp. 33-63).

[6] Aithal, P. S. (2019). Industrial Applications of Information Communication & Computation Technology (ICCT)–An Overview. In *Proceedings of National Conference on Recent Advances in Technological Innovations in IT, Management, Education & Social Sciences ISBN* (No. 978-81, pp. 941751-6).

[7] Gade, S. & Aithal, P. S. (2021). Smart City Waste Management through ICT and IoT driven Solution. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *5*(1), 51-65.

[8] Aithal, P. S. (2018). Emerging Trends in ICCT as Universal Technology for Survival, Sustainability, Differentiation, Monopoly and Development. In *Proceedings of National Conference on Advances in Information Technology, Management, Social Sciences and Education, (2018)* (pp. 130-141).

[9] Aithal, P. S., & Aithal, S. (2019). Strategic Management of Universal Technologies for Redefining Productivity & Performance. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *3*(2), 81-95.

[10] Aithal, P. S., & Aithal, S. (2020). Information Communication and Computation Technology (ICCT) and its Contribution to Universal Technology for Societal Transformation. *Information, Communications and Computation Technology (ICCT) The Pillar for Transformation" edited by PK Paul et al. published by New Delhi Publishers, New Delhi, India*, 1-28.

[11] Aithal, P. S., & Aithal, S. (2020). Conceptual Analysis on Higher Education Strategies for various Tech-Generations. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *5*(1), 335-351.

[12] Aithal, P. S., & Aithal, S. (2019, October). Management of Universal Technologies & Their Industry Implications. In *Proceedings of International Conference on Emerging Trends in Management, IT and Education* (Vol. 1, No. 2, pp. 318-328).

[13] Madhushree, Revathi, R., & Aithal, P. S. (2019). A Review on Impact of Information Communication & Computation Technology (ICCT) on Selected Primary, Secondary, and Tertiary Industrial Sectors. *Saudi Journal of Business and Management Studies, 4*(1), 106-127.

[14] Paul, P., & Aithal, P. S. (2018). Cyber Crime: Challenges, Issues, Recommendation and Suggestion in Indian Context. *International Journal of Advanced Trends in Engineering and Technology. (IJATET)*, *3*(1), 59-62.

[15] Paul, P., Bhuimali, A., Aithal, P. S., & Rajesh, R. (2018). Cyber security to information assurance: an overview. *International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)*, *6*(4), 8-14.

[16] Sai Manoj, K., Aithal, P. S. (2021). Cyber Security and Privacy Internal Attacks Measurements Through Block Chain. *Journal of Information Technology in Industry*, *9*(1), 1033-1044.

[17] Kabanda, G. (2021). Cybersecurity risk management plan for a blockchain application model. *Trans Eng Comput Sci*, *2*(1), 221.

[18] Bhuvana, R., Madhushree, L., & Aithal, P. S. (2020). Comparative Study on RFID based Tracking and Blockchain based Tracking of Material Transactions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 22-30.

[19] Bhuvana, R., & Aithal, P. S. (2020). Blockchain Based Service: A Case Study on IBM Blockchain Services & Hyperledger Fabric. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 4(1), 94-102.*

[20] Bhuvana, R., & Aithal, P. S. (2020). RBI Distributed Ledger Technology and Blockchain-A Future of Decentralized India. *International Journal of Management, Technology and Social Sciences (IJMTS)*, *5*(1), 227-237.

[21] Gade, Dipak S. and Aithal, P. S. (2020). Blockchain Technology: A Driving Force in Smart Cities Development. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 237-252.

[22] Rangi, P. K., & Aithal, P. S. (2020). A Study on Blockchain Technology as a Dominant Feature to Mitigate Reputational Risk for Indian Academic Institutions and Universities. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 275-284.

[23] Bhuvana R, Madhushree L. M, & Aithal P. S. (2021). Blockchain as a Disruptive Technology in Healthcare and Financial Services - A Review based Analysis on Current Implementations. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(1), 142–155. Retrieved from https://srinivaspublication.com/journal/index.php/ijaeml/article/view/311

[24] Sai Manoj, K., & P. S. Aithal (2020). Blockchain Cyber Security Vulnerabilities and Potential Countermeasures. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9*(5), 1516-1522.

[25] Aithal P. S., Architha Aithal, & Edwin Dias. (2021). Blockchain Technology - Current Status and Future Research Opportunities in Various Areas of Healthcare Industry. *International Journal of Health Sciences and Pharmacy (IJHSP)*, *5*(1), 130–150. https://doi.org/10.47992/IJHSP.2581.6411.0070

[26] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208.

[27] Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060.

[28] Mylrea, M., & Gourisetti, S. N. G. (2018). Blockchain for supply chain cybersecurity, optimization and compliance. In *2018 Resilience Week (RWS)* (pp. 70-76). IEEE.

[29] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 975-979). IEEE.

[30] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, *41*(10), 1027-1038.

[31] Sachin Kumar, S., Dube, D., & Aithal, P. S. (2020). Emerging Concept of Tech-Business-Analytics an Intersection of IoT & Data Analytics and its Applications on Predictive Business Decisions. *International Journal of Applied Engineering and Management Letters, (IJAEML), 4*(2), 200-210.

[32] Paul, P. K., Bhuimali, A., Aithal, P. S., Tiwary, K. S., Saavedra, R., & Mewada, S. (2021). Emerging IT and Computing Gradients in Information Sciences. *International Journal of Applied Science and Engineering*, *9*(1), 1-13.

[33] Paul, P., Ripu Ranjan Sinha, R. R. S., Aithal, P. S., Saavedra M, R., Aremu, P. S. B., & Mewada, S. (2020). Internet of Things (IoT) & Smart Agriculture: With reference to applications & emerging Concern. *Asian Journal of Electrical Sciences*, *9*(1), 37-44.

[34] Paul, P., Saavedra M, R., Aithal, P. S., Ripu Ranjan Sinha, R. R. S., & Aremu, P. S. B. (2020). Agro informatics vis-à-vis internet of things (iot) integration & potentialities—An analysis. *Agro Economist-An International Journal*, *7*(1), 13-20.

[35] Aithal, P. S., & Aithal, S. (2015). A review on Anticipated Breakthrough Technologies of 21st Century. *International Journal of Research & Development in Technology and Management Science–Kailash*, *21*(6), 112-133.

[36] Aithal, P. S., & Sony, M. (2020). Design of 'Industry 4.0 readiness model' for Indian Engineering Industry: Empirical Validation Using Grounded Theory Methodology. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 124-137.

[37] Paul, P., Bhuimali, A., & Aithal, P. S. (2017). Emerging Internet Services Vis-À-Vis Development: A Theoretical Overview. *International Journal on Recent Researches in Science, Engineering, and Technology*, *5*(7), 19-25.

[38] Sony, M., & Aithal, P. S. (2020). A Resource-Based View and Institutional Theory-Based Analysis of Industry 4.0 Implementation in the Indian Engineering Industry. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *5*(2), 154-166.

[39] Sony, M., & Aithal, S. (2020). Transforming Indian Engineering Industries through Industry 4.0: An Integrative Conceptual Analysis. *International Journal of Applied Engineering and Management Letters (IJAEML), 4*(2), 111-123.

[40] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, *32*(5), 715-728.

[41] Boukerche, A., & Coutinho, R. W. (2020). Design guidelines for machine learning-based cybersecurity in internet of things. *IEEE Network*, *35*(1), 393-399.

[42] Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. *Sensors*, *18*(9), 3053.

[43] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1), 1-14.

[44] Salam, A. (2020). Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. In *Internet of Things for Sustainable Community Development* (pp. 299-327). Springer, Cham.

[45] Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666-674.

[46] Aithal, P. S., & Pai T, V. (2016). Concept of Ideal Software and its Realization Scenarios. *International Journal of Scientific Research and Modern Education (IJSRME)*, *I*(1), 826-837.

[47] HR, G., & Aithal, P. S. (2020). Artificial Intelligence-Based Consumer Communication by Brick-and-Mortar Retailers in India Leading to Syllogistic Fallacy and Trap–Insights from an Experiment. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 211-221.

[48] Paul, P., Bhuimali, A., Aithal, P. S., Kalishankar, T., & Saavedra M, R. (2020). Artificial Intelligence & Cloud Computing in Environmental Systems-Towards Healthy & Sustainable Development. *International Journal of Inclusive Development*, *6*(1), 01-08.

[49] Morel, B. (2011, October). Artificial intelligence and the future of cybersecurity. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence* (pp. 93-98).

[50] Patil, P. (2016). Artificial intelligence in cyber security. *International Journal of Research in Computer Applications and Robotics*, *4*(5), 1-5.

[51] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, 23817-23837.

[52] Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and Machines*, *29*(2), 187-191.

[53] Aithal, P. S., & Pai T, V. (2017). Opportunity for Realizing Ideal Computing System using Cloud Computing Model. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, *1*(2), 60-71.

[54] Pai T, V., & Aithal, P. S. (2017). Cloud Computing Security Issues-Challenges and Opportunities. *International Journal of Management, Technology and Social Sciences (IJMTS)*, *1*(1), 33-42.

[55] Paul, P., & Aithal, P. S. (2019). Cloud Security: An Overview and Current Trend. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *3*(2), 53-58.

[56] Pai T, V., & Aithal, P. S. (2017). A Review on Security Issues and Challenges in Cloud Computing Model of Resource Management. *International Journal of Engineering Research and Modern Education (IJERME)*, *2*(1), 65-70.

[57] Paul, P., Bhuimali, A., Aithal, P. S., Kalishankar, T., & Saavedra M, R. (2020). Artificial Intelligence & Cloud Computing in Environmental Systems-Towards Healthy & Sustainable Development. *International Journal of Inclusive Development*, *6*(1), 01-08.

[58] Paul, P., Aithal, P. S., Saavedra M, R., Aremu, P. S. B., & Baby, P. (2020). Cloud Service Providers: An Analysis of Some Emerging Organizations and Industries. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(1), 172-183.

[59] Paul, P., Aithal, P. S., & Bhuimali, A. (2017). Mobile Cloud Computing Vis-à-Vis Eco friendliness for Sustainable Development. *International Journal of Engineering Research and Modern Education (IJERME)*, *2*(2), 28-32.

[60] Paul, P., Ripu Ranjan Sinha, R. R. S., Aithal, P. S., Saavedra M, R., Aremu, P. S. B., & Mewada, S. (2020). Cloud Computing Vis-à-Vis Agricultural Development—towards Digital & Smarter

Agricultural Informatics Practice. *Asian Journal of Engineering and Applied Technology*, *9*(1), 18-24.

[61] Rabai, L. B. A., Jouini, M., Aissa, A. B., & Mili, A. (2013). A cybersecurity model in cloud computing environments. *Journal of King Saud University-Computer and Information Sciences*, *25*(1), 63-75.

[62] Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching cybersecurity using the cloud. *IEEE Transactions on Learning Technologies*, *8*(4), 383-392.

[63] El-Sofany, H. F. (2020). A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks. *International Journal of Intelligent Engineering and Systems*, *13*(2), 205-215.

[63] Jang-Jaccard, J., Nepal, S., & Guo, Y. (2013). Cybersecurity threats in cloud computing. *Journal of Telecommunications and the Digital Economy*, *1*(1), 4-1.

[64] Malomo, O. O., Rawat, D. B., & Garuba, M. (2018). Next-generation cybersecurity through a blockchain-enabled federated cloud framework. *The Journal of Supercomputing*, *74*(10), 5099-5126.

[65] Paul, P., Aithal, P. S., & Bhuimali, A. (2017). Enhancing Cloud and Big Data Systems for healthy Food and Information Systems Practice: A Conceptual Study. *International Journal of Scientific Research in Biological Sciences*, *4*(5), 18-22.

[66] Paul, P., Aithal, P. S., & Bhuimali, A. (2018). Business informatics: with special reference to big data as an emerging area: a basic review. *International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)*, *6*(4), 21-29.

[67] Sachin Kumar, S., & Aithal, P. S. (2020). How lucrative & challenging the boundary less opportunities for data scientists?. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *4*(1), 223-236.

[68] Johnstone, M., & Peacock, M. (2020). Seven pitfalls of using data science in cybersecurity. In *Data Science in Cybersecurity and Cyberthreat Intelligence* (pp. 115-129). Springer, Cham.

[69] Mahmood, T., & Afzal, U. (2013). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In *2013 2nd national conference on Information assurance (ncia)* (pp. 129-134). IEEE.

[70] Tewari, S. H. (2021). Necessity of Data Science for Enhanced Cybersecurity. *International Journal of Data Science and Big Data Analytics*, *1*(1), 63-79.

[71] Geetanjali, R., Galaxyaan, C., & Niranjanamurthy, M. (2020). How to Overcoming Cyber Security Challenges Using Data Science. *Journal of Computational and Theoretical Nanoscience*, *17*(9-10), 4116-4121.

[72] Straub, J. (2017, June). 3D printing cybersecurity: detecting and preventing attacks that seek to weaken a printed object by changing fill level. In *Dimensional Optical Metrology and Inspection for Practical Applications VI* (Vol. 10220, p. 102200O). International Society for Optics and Photonics.

[73] Straub, J. (2017, June). Identifying positioning-based attacks against 3D printed objects and the 3D printing process. In *Pattern Recognition and Tracking XXVIII* (Vol. 10203, p. 1020304). International Society for Optics and Photonics.

[74] Bridges, S. M., Keiser, K., Sissom, N., & Graves, S. J. (2015). Cyber security for additive manufacturing. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference* (pp. 1-3).

[75] Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. *Journal of manufacturing systems*, *48*, 3-12.

[76] Padmanabhan, A., & Zhang, J. (2018). Cybersecurity risks and mitigation strategies in additive manufacturing. *Progress in Additive Manufacturing*, *3*(1), 87-93.

[77] Zeltmann, S. E., Gupta, N., Tsoutsos, N. G., Maniatakos, M., Rajendran, J., & Karri, R. (2016). Manufacturing and security challenges in 3D printing. *Jom*, *68*(7), 1872-1881.

[78] Bajaj, M., & Akhilesh, K. B. (2020). Understanding the Need for Cybersecurity in Manufacturing Environment. In *Smart Technologies* (pp. 147-157). Springer, Singapore.

[79] Moore, S., Armstrong, P., McDonald, T., & Yampolskiy, M. (2016, August). Vulnerability analysis of desktop 3D printer software. In *2016 Resilience Week (RWS)* (pp. 46-51). IEEE.

[80] Gao, Y., Li, B., Wang, W., Xu, W., Zhou, C., & Jin, Z. (2018). Watching and safeguarding your 3D printer: Online process monitoring against cyber-physical attacks. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(3), 1-27.

[81] Zhe, D., Qinghong, W., Naizheng, S., & Yuhan, Z. (2017). Study on data security policy based on cloud storage. In *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)* (pp. 145-149). IEEE.

[82] Zhang, X., Du, H. T., Chen, J. Q., Lin, Y., & Zeng, L. J. (2011, May). Ensure data security in cloud storage. In *2011 International Conference on Network Computing and Information Security* (Vol. 1, pp. 284-287). IEEE.

[83] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740.

[84] Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications*, *111*, 120-141.

[85] Khedkar, S. V., & Gawande, A. D. (2014). Data partitioning technique to improve cloud data storage security. *International Journal of Computer Science and Information Technologies*, *5*(3), 3347-3350.

[86] Chen, Y., & Ku, W. S. (2009, January). Self-encryption scheme for data security in mobile devices. In *2009 6th IEEE Consumer Communications and Networking Conference* (pp. 1-5). IEEE.

[87] Polverini, D., Ardente, F., Sanchez, I., Mathieux, F., Tecchio, P., & Beslay, L. (2018). Resource efficiency, privacy and security by design: a first experience on enterprise servers and data storage products triggered by a policy process. *Computers & Security*, *76*, 295-310.

[88] Snyder, R. (2006, September). Some security alternatives for encrypting information on storage devices. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 79-84).

[89] He, D., Kumar, N., Lee, J. H., & Sherratt, R. S. (2014). Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Transactions on Consumer Electronics*, *60*(1), 30-37.

[90] Alekseev, E. K., Akhmetzyanova, L. R., Babueva, A. A., & Smyshlyaev, S. V. E. (2020). Data storage security and full disk encryption. *Prikladnaya Diskretnaya Matematika*, *6*(3), 78-97.

[91] Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smart phones. *Journal of Information Systems Technology and Planning*, *5*(14), 40-60.

[92] Feigelson, J., Pastore, J., Serrato, J. K., & Metallo, J. (2016). New Federal Guidance on Cybersecurity for Mobile Devices. *Intellectual Property & Technology Law Journal*, *28*(3), 25.

[93] Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346).

[94] Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, *1*(3-4), 202-224.

[95] Raghavan, K., Desai, M. S., & Rajkumar, P. V. (2017). Managing cybersecurity and ecommerce risks in small businesses. *Journal of management science and business intelligence*, *2*(1), 9-15.

[96] Adegbite, G. A., Emuoyibofarhe, O. J., Ajala, F. A., & Awokola, J. A. (2017). A Cybersecurity Approach for Evaluating Mobile Agents. *Journal of Applied Security Research*, *12*(2), 253-259.

[97] Chun, S. H. (2019). E-commerce liability and security breaches in mobile payment for e-business sustainability. *Sustainability*, *11*(3), 715.

[98] Grocke, D. (2017). Emerging cybersecurity threats in large and small firms. *Bulletin (Law Society of South Australia)*, *39*(3), 20-22.

[99] Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*(1), 44-55.

[100] Dennis, K., Alibayev, M., Barbeau, S. J., & Ligatti, J. (2020). Cybersecurity Vulnerabilities in Mobile Fare Payment Applications: A Case Study. *Transportation Research Record*, *2674*(11), 616-624.

[101] Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122).

[102] Davidson, P., & Hasledalen, K. (2014). Cyber threats to online education: A Delphi study. In *ICMLG2014 Proceedings of the 2nd International Conference on Management, Leadership and Governance: ICMLG 2014, Academic Conferences Limited* (p. 68).

[103] Gabor, A. M., Popescu, M. C., & Naaji, A. (2017). Security Issues Related To E-Learning Education. *International Journal of Computer Science and Network Security (IJCSNS)*, *17*(1), 60.

[104] Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., & Rodrigues, J. J. (2018). Privacy and security issues in online social networks. *Future Internet*, *10*(12), 114.

[105] Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *International Review of Research in Open and Distributed Learning*, *14*(5), 108-127.

[106] Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. *Proceedings of ICERI2014 Conference*, IATED, 0728-0734. ISBN: 978-84-617-2484-0

[107] Luminita, D. C. C. (2011). Security issues in e-learning platforms. *World journal on educational technology*, *3*(3), 153-167.

[108] Kovacova, L., & Vackova, M. (2015). Implementation of e-learning into the process security education in universities. *Procedia-Social and Behavioral Sciences*, *182*, 414-419.

[109] Nahed, M., & Alawneh, S. (2020). Cybersecurity in a Post-Quantum World: How Quantum Computing Will Forever Change the World of Cybersecurity. *American Journal of Electrical and Computer Engineering*, *4*(2), 81-93.

[110] Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Communications of the ACM*, *62*(4), 120-120.

[111] Easttom, W. (2021). Quantum Computing and Cryptography. In *Modern Cryptography* (pp. 385-390). Springer, Cham.

[112] Meraz, R., & Vahala, L. (2020). Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications. *OUR Journal: ODU Undergraduate Research Journal*, *7*(1), 5-12.

[113] Ali, A. (2021). A Pragmatic Analysis of Pre-and Post-Quantum Cyber Security Scenarios. In *2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST)* (pp. 686-692). IEEE.

[114] Gompert, D. C., & Libicki, M. (2021). Towards a Quantum Internet: Post-pandemic Cyber Security in a Post-digital World. *Survival*, *63*(1), 113-124.

[116] Lindsay, J. R. (2020). Surviving the Quantum Cryptocalypse. *Strategic Studies Quarterly*, *14*(2), 49-73.

[117] Covers, O., & Doeland, M. (2020). How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure. *Journal of Payments Strategy & Systems*, *14*(2), 147-156.

[118] Tosh, D., Galindo, O., Kreinovich, V., & Kosheleva, O. (2020). Towards Security of Cyber-Physical Systems using Quantum Computing Algorithms. In *2020 IEEE 15th International Conference of System of Systems Engineering (SoSE)* (pp. 313-320). IEEE.

[119] Choi, J. W. (2017). Quantum Computation and Its Influence on Cybersecurity. *Charleston L. Rev.*, *12*, 393-399.

[120] Seo, J. H., Bruner, M., Payne, A., Gober, N., & McMullen, D. (2019). Using virtual reality to enforce principles of cybersecurity. *The Journal of Computational Science Education*, *10*(1).

[121] Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). Cyber VR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. In *Proceedings of the International Conference on Advanced Visual Interfaces* (pp. 1-8).

[122] Adinolf, S., Wyeth, P., Brown, R., & Altizer, R. (2019). Towards designing agent based virtual reality applications for cybersecurity training. In *Proceedings of the 31st Australian Conference on Human-Computer-Interaction* (pp. 452-456).

[123] Kabil, A., Duval, T., & Cuppens, N. (2020). Alert Characterization by Non-expert Users in a Cybersecurity Virtual Environment: A Usability Study. In *International Conference on Augmented Reality, Virtual Reality and Computer Graphics* (pp. 82-101). Springer, Cham.

[124] Willems, C., Klingbeil, T., Radvilavicius, L., Cenys, A., & Meinel, C. (2011). A distributed virtual laboratory architecture for cybersecurity training. In *2011 International Conference for Internet Technology and Secured Transactions* (pp. 408-415). IEEE.

[125] Yadin, G. (2016). Virtual Reality Surveillance. *Cardozo Arts & Ent. LJ*, *35*, 707-717.

[126] Mattina, B., Yeung, F., Hsu, A., Savoy, D., Tront, J., & Raymond, D. (2017). MARCS: mobile augmented reality for cybersecurity. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research* (pp. 1-4).

[127] Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., & Redmiles, E. M. (2018). Ethics emerging: the story of privacy and security perceptions in virtual reality. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (pp. 427-442).

[128] Prasanthi, B. V., Kanakam, P., & Hussain, S. M. (2017). Cyber Forensic Science to Diagnose Digital Crimes-A study. *International Journal of Scientific Research in Network Security and communication (IJSRNSC)*, *50*(2), 107-113.

[129] Joseph, D. P., & Norman, J. (2019). An analysis of digital forensics in cyber security. In *First international conference on artificial intelligence and cognitive computing* (pp. 701-708). Springer, Singapore.

[130] Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., ... & Khan, R. A. (2020). Current Challenges of Digital Forensics in Cyber Security. *Critical Concepts, Standards, and Techniques in Cyber Forensics*, 31-46.

[131] McGoldrick, L. K., & Halámek, J. (2020). Recent Advances in Noninvasive Biosensors for Forensics, Biometrics, and Cybersecurity. *Sensors*, *20*(21), 5974-5984.

[132] Sharma, B. K., Joseph, M. A., Jacob, B., & Miranda, L. C. B. (2019, November). Emerging trends in Digital Forensic and Cyber security-An Overview. In *2019 Sixth HCT Information Technology Trends (ITT)* (pp. 309-313). IEEE.

[133] Montasari, R., & Hill, R. (2019, January). Next-generation digital forensics: challenges and future paradigms. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 205-212). IEEE.

[134] Mistry, N. R., & Dahiya, M. S. (2019). Signature based volatile memory forensics: a detection based approach for analyzing sophisticated cyber attacks. *International Journal of Information Technology*, *11*(3), 583-589.