Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security

Diptiban Ghillani[1]

[1]Affiliation not available

September 21, 2022

Department of Computer Engineering, Gujrat Technological College, Ahmedabad, India

Email address:

Shezi1131@gmail.com

To cite this article:

Diptiben Ghelni. Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. *American Journal of Artificial Intelligence* . Vol. x, No. x, 2022, pp. x-x.

Abstract: Deep learning derived from an artificial neural network (ANN), is one of the essential technologies for today's intelligent cyber security systems or policies. The benefits and drawbacks of using artificial intelligence (AI) in cyber risk analytics to improve organizational resilience and better comprehend cyber risk. Multilayer perceptron, convolutional neural network, recurrent neural network or long short-term memory, self-organizing map, auto-encoder, restricted Boltzmann machine, deep belief networks, generative adversarial network, deep transfer learning, and deep reinforcement learning, as well as their ensembles and hybrid approaches, can be used to tackle the diverse cyber security issues intelligently. The backpropagation algorithm's ultimate goal is to correctly maximize the network weights to translate the inputs to the intended outputs. During the training phase, several optimization approaches such as Stochastic Gradient Descent (SGD), Limited Memory BFGS (L-BFGS), and Adaptive Moment Estimation (Adam) are applied. These neural networks may be utilized to handle a variety of cybersecurity problems. MLP-based networks are used to construct an intrusion detection model, malware analysis, security threat analysis, identify malicious botnet traffic, and build trustworthy IoT systems. MLP is sensitive to feature scaling and requires tuning a variety of hyperparameters such as the number of hidden layers, neurons, and iterations, which might make solving a complicated security model computationally costly.

Keywords: Cyber Security, Artificial Intelligence, Deep Learning, Internet of Things

1. Introduction

Industry 4.0, an IoT phrase coined in 1999, is built on the Internet of Things (IoT) technology, providing the first glimpse of what an IoT-based ecosystem would look like in the future. CPS refers to the interdisciplinary and complex characteristics of intelligent systems constructed and relies on the interplay of physical and computational components. CPS theory evolved from control theory and control systems engineering. It focuses on the connectivity of physical features and the utilization of sophisticated software entities to create new network and system capabilities. CPSs connect biological and engineering systems, bridging the cyber and physical worlds [1].

On the other hand, IoT theory is based on computer science and Internet technologies, and it focuses

primarily on the interconnection, interoperability, and integration of physical components on the Internet. This integration effort is expected to lead to advances such as IoT automation of CPSs as the IoT industry matures over the next decade. CPS systems and automated CPSs guide trained employees in production situations in real-time. In this context, we look at how such systems enable artificial intelligence (AI) breakthroughs in real-time processing, sensing, and actuation across these new systems and give cyber structure system analysis capabilities. As a result, we'll concentrate on artificial intelligence, which is a notion that encompasses both the cyber-physical and social components of the hazards associated with new technology deployment [2].

There are two research aims in this study. To begin, we provide an up-to-date summary of current and emerging cyber risk analytics breakthroughs. This incorporates current standards into a new risk analytics feedback loop by combining existing literature to generate shared core terminology and techniques. Second, by providing a novel understanding of cyber network risk and the role of AI in future CPS, we capture best practices and spark debate among practitioners and academia. Throughout the article, this architecture is explored and may be used as a best practice for designing and prototyping AI-enabled dynamic cyber risk analyses [3].

2. Artificial intelligence, CPS, and predictive cyber risk analytics literature review

The IoT has been defined as a revolutionary technological augmentation that transforms the traditional living into a high-tech lifestyle in terms of data streams. CPSs and IoT generate massive amounts of data, necessitating powerful analytical tools for analysis. We almost likely need AI-assisted analytical tools to clean up the data's noise and inconsistencies. On the other hand, CPS architectures cover a wide range of topics. These many notions must be integrated into a system [4].

Furthermore, CPS mandates anti-counterfeiting and supply chain risk management to combat malicious supply chain components that have been altered from their original design to create disruption or perform illegal functions. Hyper-connectivity in the digital supply chain must be promoted in addition to design and process standardization. It is proposed that restricting source code access to critical and experienced employees can offer software assurance and application security and may be required to prevent the introduction of purposeful faults and vulnerabilities in CPSs. Forensics, prognostics, and recovery plans should be included in security measures for cyber-attack analysis and coordination with other CPSs and entities that detect external cyber-attack vectors [5]. An internal track and trace network procedure can help by recognizing or avoiding gaps in logistical security measures. To prevent the exploitation of CPS vulnerabilities discovered by reverse engineering assaults, a method for anti-malicious and anti-tamper system engineering is required. Taxonomic analysis was performed using the Smart literature review approach based on latent Dirichlet allocation. The resulting areas of concentration are organized into a taxonomy with acronyms to aid in the integration of artificial intelligence with the current CPS. Deep learning (DL) is a subset of machine learning (ML) and artificial intelligence (AI), and it is one of the primary technologies of the Fourth Industrial Revolution. It is derived from an artificial neural network (ANN) (Industry 4.0) [6]. "Cyber security" and "Deep learning" are becoming increasingly popular worldwide, as demonstrated in Figure 1.

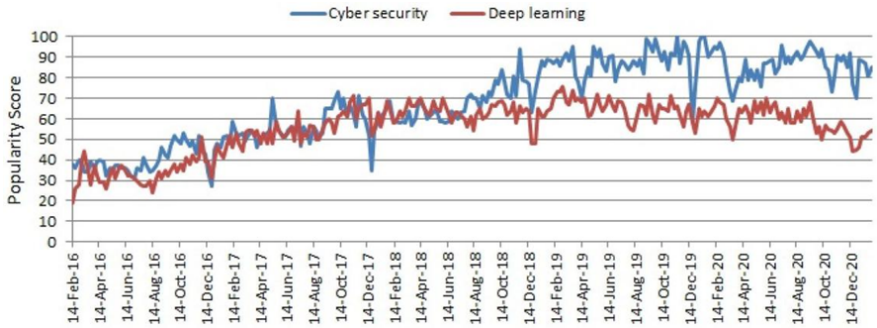

Figure 1. "Cyber security" and "Deep learning" popularity scores in a range of 0 (min) to 100 (max) through time, with the x-axis representing timestamp information and the y-axis representing the associated popularity score.

The popularity trend in Figure 1 is based on Google Trends data collected over the previous five years. In this research, we consider several standard neural networks and deep learning approaches in the context of cybersecurity, including supervised, semi-supervised, unsupervised, and reinforcement learning. These include I multilayer perceptron (MLP), convolutional neural network (CNN or ConvNet), (ii) recurrent neural network (RNN) or long short-term memory (LSTM), (iv) self-organizing map (SOM), (v) auto-encoder (AE), (vi) restricted Boltzmann machine (RBM), (vii) deep belief networks (DBN), (viii) generative adversarial network (GAN) (DRL or deep RL). These deep neural network learning techniques and their ensembles and hybrid approaches can intelligently solve various cybersecurity problems, including intrusion detection, malware or botnet identification, phishing, and predicting cyber-attacks such as DoS fraud detection and cyber-anomalies [7]. Construct security models because they are more accurate, especially when learning from massive security datasets. This paper's contribution may be summarised as follows:

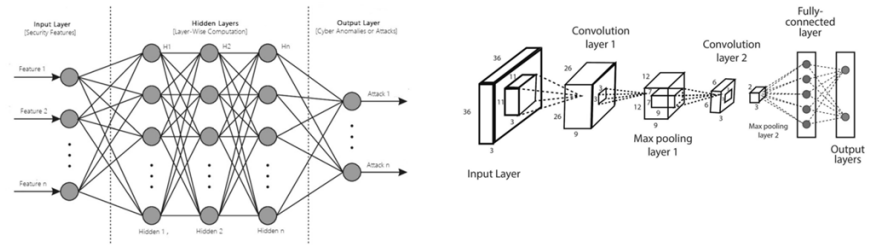

Figure 2. "Cyber security" and "Deep learning" popularity scores in a range of 0 (min) to 100 (max) through time, with the x-axis representing timestamp information and the y-axis representing the associated popularity score [8].

Deep learning provides advantages for extensive data analytics and statistical machine learning to detect cyber dangers in a cognitive state. However, designing extensive data systems for edge computing environments might be difficult. One of the most critical concerns for CPS is security, both electronic and physical, and the interconnection of physical and cyber systems. Information assurance and data protection in transit from physical and electronic domains and storage facilities are required for such security. Furthermore, asset management and access control are essential for granting or refusing requests for information and processing services, mainly because CPS will interact with nontechnical users and may have an impact beyond administrative borders. Techniques are required to handle unique vulnerabilities resulting from life cycle difficulties such as dwindling manufacturing resources and asset updates. These include technologies such as flexibly time-triggered architectures and structural dynamics control for designing system dynamics over many time scales [9]. In 1998, DARPA (Defense Advanced Research Project Agency) launched the first effort to create an intrusion detection system dataset. The datasets are generated and provided by the MIT Lincoln Laboratory's Cyber Infrastructure and Technology Division (previously the DARPA Intrusion Detection Assessment Group) to evaluate computer network intrusion detection systems under the supervision of DARPA and AFRL/SNHS. One of the most often used datasets for intrusion detection is the KDD Cup 99 dataset, which contains network traffic records with over forty feature characteristics and one class identification. There are four forms of assaults in the dataset: DoS, R2L, U2R, PROB, and regular data. To better understand security data, we've shown the features of intrusion detection datasets, including the elements and their different forms, such as integer, float, or nominal [10].

The Canadian Institute for Cybersecurity established another dataset, the ISCX. The notion of profiles was used to explain assault and distribution techniques in a network setting. Several genuine traces were processed to build reliable profiles of assaults and other events to evaluate intrusion detection systems. The

Canadian Cyber Security Institute recently established a new dataset, CSE- CIC-IDS2018, based on a user profile that records network events and behavior. The MAWI dataset is a collection of research and academic institutions that the Japanese network uses to compute the global internet situation across a large territory. The dataset is updated daily to track new traffic. Some researchers utilize this data collection to detect DDoS attacks. Because MAWI involves actual data traffic, the sorts of attacks caught there are diverse. The ADFA data set is a collection of host-level intrusion detection system data sets published by the Australian Securities Academy (ADFA) and widely utilized in intrusion detection product testing. Hydra-FTP, Hydra-SSH, Add Consumer, Java-MeterPerter, Webshell, and two forms of simple assaults, such as Training and Validation, is among the five types of attacks [11].

Equinix tracks legitimate and attacks traces in the CAIDA'08 dataset (Chicago and San Jose data centers). The attack generally comprises SYN, ICMP, and HTTP flood traffic. This dataset is highly skewed towards DDoS assaults since much of the excellent material was deleted after collecting the traffic. Fractions were obtained in Chicago and San Jose on March 19, 2008 and July 17, 2008. The ISOT'10 dataset combines malicious and non-malicious datasets created by research in Information Security and Object Technology at the University of Victoria (ISOT). ISCX'12 simulates traffic from a real-world physical test environment that generates network traffic containing centralized botnets. The Ericsson Research Laboratory and Lawrence Berkeley National Lab retrieved non-harmful traffic, whereas Hon-eynet obtained decentralized botnet data for malicious traffic [12].

The CTU- 13 dataset is a botnet traffic dataset registered at the University of CTU in the Czech Republic in 2011. The Alexa Top Sites list is a popular source of innocuous domain names because it contains one million domain names. The malicious domain names are OSINT and DGArchive. The University of New South Wales created the UNSW-NB15 dataset in 2015. It has 49 distinct features and about 257,700 documents that span nine main types of contemporary assaults. A method for creating benchmark datasets for intrusion detection has been given in. In recent years, the malware industry has evolved into a well-organized market involving enormous money. The most prevalent source of regular information in malware tests is top applications from the Google Play Store. While these applications are not guaranteed to be malware-free, they are the most likely to be because of Google's testing and the apps' widespread availability [13].

Perceptron Multilayer (MLP) A supervised learning approach, the multilayer perceptron is a feedforward artificial neural network (ANN). Deep learning or deep neural networks (DNN) use it as their foundation architecture.

Because MLPs are entirely linked, each node in one layer connects to each node in the next layer at a certain weight. Several activation functions are employed to determine the output of a network, including ReLU (Rectified Linear Unit), Tanh, Sigmoid, and Softmax. These activation functions, sometimes called transfer functions, introduce non-linear features into the network, allowing it to learn complicated functional mappings from the input. MLP trains feedforward neural networks using a supervised learning technique known as "Backpropagation," the most "basic building block" of a neural network and the most extensively used algorithm for training feedforward neural networks. Convolutional neural networks were created with the diversity of 2D forms in mind. Image and video recognition, medical image analysis, recommender systems, image classification, image segmentation, natural language processing, financial time series, and other applications employ CNN's extensively. Although CNNs are most typically employed to analyze visual information, they may also be utilized in cybersecurity. For example, in IoT Networks, CNN-based deep learning models are used for intrusion detection, such as denial-of-service (DoS) assaults, malware detection, and android malware detection. A phishing detection model based on convolutional neural networks has also been demonstrated. A multi-CNN fusion-based model can be deployed for intrusion detection in the region. Although CNN has a higher computational cost, it has the benefit of automatically discovering essential characteristics without the need for human intervention, making it more potent than traditional ANN. Depending on the problem domain and data characteristics, several advanced CNN-based deep learning models, such as AlexNet, Xception, Inception, visual geometry group (VGG), ResNet, and others, or

alternative lightweight architecture of the model can be employed to reduce the difficulties.

Learning with Deep Transfer (DTL or Deep TL) Transfer learning is an essential strategy for tackling the fundamental problem of insufficient training data in machines and deep understanding. It is now prevalent in data science since most real-world situations do not have millions of labeled data points to train such complicated models. As a result, it reduces the requirement to train AI models by allowing neural networks to be prepared with tiny quantities of data.

Transfer learning by induction The target task is different from the source task. Several ways are essential to this, including instance transfer, feature representation transfer, parameter transfer, and relational knowledge transfer.

Learning transferable The source and target tasks are the same in this scenario, but the source and target domains are distinct. This is when technologies like instance transfer and feature representation transfer come in handy.

Transfer learning without supervision It's comparable to the previously described inductive transfer learning, in which the target and source tasks are distinct yet connected. It's usually investigated in the context of feature representation transfer.

Deep transfer learning may be used for natural language processing (NLP), sentiment classification, computer vision, image classification, speech recognition, medical imaging, and spam filtering, among other things. It also plays an essential part in cybersecurity because of its multiple modeling advantages, such as decreasing training time, boosting output accuracy, and using less training data. For example, the authors offer a ConvNet model for network intrusion detection that uses transfer learning. The authors present a deep feature transfer learning-based signature generation approach that drastically decreases signature production and dissemination time. In, the categorization accuracy was increased to 99.5 percent. The authors describe a feature-based transfer learning strategy utilizing a linear transformation in which they address transfer learning to discover unknown network assaults. The transfer variable enhanced the byte classifier accuracy from 94.72 to 96.90 percent in a semi-supervised transfer learning model for malware detection. Using deep neural network resnet-50 transfer learning, the authors provide the categorization of harmful software. Their results from an experiment on a sample show a 98.62 percent accuracy in categorizing malware families [14].

3. Learning using Deep Reinforcement (DRL or Deep RL)

Deep reinforcement learning (DRL or deep RL) is a machine learning and AI category in which intelligent robots may learn from their actions the same way people do. It integrates reinforcement learning (RL) methods such as Q-learning and deep understanding, such as neural network learning. The job of learning how agents in an environment might execute sequences of behaviors to maximize cumulative rewards is known as reinforcement learning (RL). The problem of a computer agent learning to make decisions through trial and error is addressed in RL. Deep learning is a type of machine learning that uses numerous layers to extract higher-level properties from raw data and make intelligent judgments using neural networks. Deep RL uses deep learning models, such as the deep neural network (DNN), as policy and value function approximators, based on the Markov decision process (MDP) concept. "A tuple S, A, T, R, where S is a collection of states, A is a set of actions, T is a mapping specifying the transition probabilities from every state-action pair to every conceivable new state, and R is a reward function that attaches a real value (reward) to every state-action pair," according to Wikipedia. Deep reinforcement learning can be applied to cybersecurity. Compared to typical machine learning models, the authors show that deep RL models employing deep Q-network (DQN) and double deep Q-network (DDQN) yield significant intrusion detection results [15].

Similarly, a deep RL-based adaptive intrusion detection framework for cloud infrastructure based on deep-Q-network (DQN) was given. They claimed greater accuracy and reduced false-positive rates for detecting and identifying novel and sophisticated threats. Furthermore, a hybrid network model, such as an ensemble of networks, may be utilized to construct a practical model that considers their combined benefits. For example, an LSTM network with CNN may be used to identify cyber-attacks, such as virus detection, and

detect and mitigate phishing and Botnet assaults across numerous IoT devices. As a result, we may infer that the artificial neural network and deep learning techniques outlined above and their variations or modified approaches can play an essential role in meeting contemporary cybersecurity concerns [16].

4. Conclusion

We thoroughly examined cybersecurity from the standpoint of artificial neural networks and deep learning techniques. To form the perspective of this study, we also evaluated current studies in each area of neural networks. As a result, we've briefly covered how different types of neural networks and deep learning methods might be applied for cybersecurity solutions in various situations, as per our aim. Depending on the data properties, a successful security model must include the appropriate deep learning modeling. Before the system can aid with intelligent decision-making, the advanced learning algorithms must be taught using the acquired security data and information linked to the target application. Finally, we've outlined and addressed the obstacles that have been encountered, as well as future research possibilities and future initiatives in the field. As a result, the difficulties that have been highlighted present exciting research possibilities in the domain that must be addressed with practical solutions to improve security with time and expand popularity. Overall, we feel that our research on neural networks and deep learning-based security analytics points in the right direction and may be utilized as a reference guide for future research and applications in the field of cybersecurity by both academic and industry specialists.

References

[1]. Li, J. h., *Cyber security meets artificial intelligence: a survey.* Frontiers of Information Technology & Electronic Engineering, 2018. 19 (12): p. 1462-1474.

[2]. Zhang, Z., et al., *Artificial intelligence in cyber security: research advances, challenges, and opportunities.* Artificial Intelligence Review, 2021: p. 1-25.

[3]. Oak, R., Du, M., Yan, D., Takawale, H., & Amit, I. (2019, November). Malware detection on highly imbalanced data through sequence modeling. In *Proceedings of the 12th ACM Workshop on artificial intelligence and security* (pp. 37-48).

[4]. Morel, B. *Artificial intelligence and the future of cybersecurity* . in *Proceedings of the 4th ACM workshop on Security and artificial intelligence* . 2011.

[5]. Khisamova, Z. I., I. R. Begishev, and E. L. Sidorenko,*Artificial intelligence and problems of ensuring cyber security.* International Journal of Cyber Criminology, 2019. 13 (2): p. 564-577.

[6]. Yampolskiy, R. V. and M. Spellchecker, *Artificial intelligence safety and cybersecurity: A timeline of AI failures.* arXiv preprint arXiv:1610.07997, 2016.

[7]. Soni, V. D., *Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA.* Available at SSRN 3624487, 2020.

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

[9]. Wirkuttis, N. and H. Klein, *Artificial intelligence in cybersecurity.* Cyber, Intelligence, and Security, 2017. 1 (1): p. 103-119.

[10]. Taddeo, M., T. McCutcheon, and L. Floridi, *Trusting artificial intelligence in cybersecurity is a double-edged sword.* Nature Machine Intelligence, 2019. 1 (12): p. 557-560.

[11]. Truong, T. C., et al., *Artificial intelligence and cybersecurity: Past, presence, and future* , in *Artificial intelligence and evolutionary computations in engineering systems* . 2020, Springer. p. 351-363.

[12]. Sedjelmaci, H., et al., *Cyber security based on artificial intelligence for cyber-physical systems.* IEEE Network, 2020. 34 (3): p. 6-7.

[13]. Demertzis, K. and L. Iliadis, *A bio-inspired hybrid artificial intelligence framework for cyber security* , in *Computation, cryptography, and network security* . 2015, Springer. p. 161-193.

[14]. Patil, P., *Artificial intelligence in cybersecurity.*International journal of research in computer applications and robotics, 2016. 4 (5): p. 1-5.

[15]. Mohammed, I. A., *ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE.* ARTIFICIAL INTELLIGENCE, 2020. 7 (9).

[16]. Sagar, B., et al. *Providing Cyber Security using Artificial Intelligence–A survey* . in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)* . 2019. IEEE.

[17]. Mosteanu, N. R., *Artificial intelligence and cyber security–face to face with cyber attack–a maltese case of risk management approach.* Ecoforum Journal, 2020. 9 (2).

[18]. Aliyu, K. N., Alawsh, S. A., Muqaibel, A. H., Al-Dharrab, S. I., Mesbah, W., Reddy, V. A., . . . Stüber, G. L. (2021). DOA-based Localization Using Deep Learning for Wireless Seismic Acquisition.

[19]. Azim, A. W., Bazzi, A., Shubair, R., & Chafii, M. (2022). Dual-Mode Chirp Spread Spectrum Modulation. *arXiv preprint arXiv:2205.09421.*

[20]. Azim, A. W., Bazzi, A., Shubair, R., & Chafii, M. (2022). Dual-Mode Chirp Spread Spectrum Modulation. *IEEE Wireless Communications Letters*, 1-1. doi:10.1109/LWC.2022.3190564

[21]. Bazzi, A. (2017a). Parameter estimation techniques for indoor localisation via WiFi. *Diss. Télécom ParisTech.*

[22]. Bazzi, A. (2017b). *Techniques d'estimation de paramètres pour la localisation à l'intérieur via WiFi.* Paris, ENST.

[23]. Bazzi, A., & Chafii, M. (2022). On Outage-based Beamforming Design for Dual-Functional Radar-Communication 6G Systems. *arXiv preprint arXiv:2207.04921.*

[24]. Bazzi, A., Cottatellucci, L., & Slock, D. (2017). *Blind on board wideband antenna RF calibration for multi-antenna satellites.* Paper presented at the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

[25]. Bazzi, A., & Meilhac, L. (2022). Method for decoding an rf signal bearing a sequence of symbols modulated by cpm and associated decoder: Google Patents.

[26]. Bazzi, A., & Slock, D. (2019). *Joint Angle and Delay Estimation (JADE) by Partial Relaxation.* Paper presented at the 2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP).

[27]. Bazzi, A., & Slock, D. (2020). *Robust Music Estimation Under Array Response Uncertainty.* Paper presented at the ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

[28]. Bazzi, A., Slock, D. T., & Meilhac, L. (2015). *Efficient maximum likelihood joint estimation of angles and times of arrival of multiple paths.* Paper presented at the 2015 IEEE Globecom Workshops (GC Wkshps).

[29]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016a). *Detection of the number of superimposed signals using modified MDL criterion: A random matrix approach.* Paper presented at the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

[30]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016b). *JADED-RIP: Joint Angle and Delay Estimator and Detector via Rotational Invariance Properties.* Paper presented at the 2016 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT).

[31]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016c). *A mutual coupling resilient algorithm for joint angle and delay estimation.* Paper presented at the 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP).

[32]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016d). *On a mutual coupling agnostic maximum likelihood angle of arrival estimator by alternating projection.* Paper presented at the 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP).

[33]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016). On AoA Estimation in the Presence of Mutual Coupling: Algorithms and Performance Analysis. *IEEE Transactions on Signal Processing, Submitted.*

[34]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016e). *On joint angle and delay estimation in the presence of local scattering.* Paper presented at the 2016 IEEE International Conference on Communications Workshops (ICC).

[35]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016f). *On spatio-frequential smoothing for joint angles and times of arrival estimation of multipaths.* Paper presented at the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

[36]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016g). *Online angle of arrival estimation in the presence of mutual coupling.* Paper presented at the 2016 IEEE Statistical Signal Processing Workshop (SSP).

[37]. Bazzi, A., Slock, D. T., & Meilhac, L. (2016h). *Sparse recovery using an iterative variational Bayes algorithm and application to AoA estimation.* Paper presented at the 2016 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT).

[38]. Bazzi, A., Slock, D. T., & Meilhac, L. (2017a). *A Newton-type Forward Backward Greedy method for multi-snapshot compressed sensing.* Paper presented at the 2017 51st Asilomar Conference on Signals, Systems, and Computers.

[39]. Bazzi, A., Slock, D. T., & Meilhac, L. (2017b). *On Mutual Coupling for ULAs: Estimating AoAs in the presence of more coupling parameters.* Paper presented at the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

[40]. Bazzi, A., Slock, D. T., & Meilhac, L. (2017c). *Performance Analysis of an AoA estimator in the presence of more mutual coupling parameters.* Paper presented at the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

[41]. Bazzi, A., Slock, D. T., Meilhac, L., & Panneerselvan, S. (2016). *A comparative study of sparse recovery and compressed sensing algorithms with application to AoA estimation.* Paper presented at the 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC).

[42]. Bazzi, A., Slock, D. T. M., & Meilhac, L. (2016, 22-27 May 2016). *Single snapshot joint estimation of angles and times of arrival: A 2D Matrix Pencil approach.* Paper presented at the 2016 IEEE International Conference on Communications (ICC).

[43]. Kianoush, S., Rampa, V., Nicoli, M., Popoola, W. O., Sinanovic, S., Bazzi, A., . . . Meilhac, L. ICC16-Workshops-W06-ANLN: IEEE ICC2016-Workshops: W06-Workshop on Advances in Network Localization and Navigation (ANLN).

[44]. Meilhac, L., & Bazzi, A. (2020). Pre-coding steering matrix for MU-MIMO communication systems: Google Patents.

[45]. Meilhac, L., & Bazzi, A. (2022). Digital pre-distortion method for OFDM-based communication systems: Google Patents.

[46]. Njima, W., Bazzi, A., & Chafii, M. (2022). DNN-based Indoor Localization Under Limited Dataset using GANs and Semi-Supervised Learning. *IEEE Access, 10*, 69896-69909.

[47]. Reddy, V. A., Bazzi, A., Stüber, G. L., Al-Dharrab, S., Mesbah, W., & Muqaibel, A. H. (2020). Fundamental Performance Limits of mm-Wave Cooperative Localization in Linear Topologies. *IEEE Wireless Communications Letters, 9*(11), 1899-1903.

[48]. Waqar Azim, A., Bazzi, A., Shubair, R., & Chafii, M. (2022). A Survey on Chirp Spread Spectrum-based Waveform Design for IoT. *arXiv e-prints*, arXiv: 2208.10274.

[49]. Ghelani, D., & Hua, T. K. (2022). Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain. *International Journal of Information and Communication Sciences*, *7*(1), 10.

[50]. *Ghelani, D., & Hua, T. K. A Perspective Review on Online Food Shop Management System and Impacts on Business.*

[51]. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, *6*(3), 52-63.

[52]. Dr. John Ughulu. The role of Artificial intelligence (AI) in Starting, automating and scaling businesses for Entrepreneurs.. *ScienceOpen Preprints.* DOI: 10.14293/S2199-1006.1.SOR-.PP5ZKWJ.v1

[53]. *Ughulu, J. Entrepreneurship as a Major Driver of Wealth Creation.*

[54]. Sarfraz, S., Javed, A., Mughal, S. S., Bashir, M., Rehman, A., Parveen, S., ... & Khan, M. K. (2020). Copper Oxide Nanoparticles: Reactive Oxygen Species Generation and Biomedical Applications. *Int. J. Comput. Theor. Chem*, *8*, 40-46.

[55]. Rafique, S., Hassan, S. M., Mughal, S. S., Hassan, S. K., Shabbir, N., Perveiz, S., ... & Farman, M. (2020). Biological attributes of lemon: a review. *Journal of Addiction Medicine and Therapeutic Science*, *6*(1), 030-034.

[56]. Hanif, [56]. Hanif, [56]. Hanif, M. A., Hassan, S. M., Mughal, S. S., Rehman, A., Hassan, S. K., Ibrahim, A., & Hassan, H. (2021). An overview on ajwain (Trachyspermum Ammi) pharmacological effects: current and conventional. *Technology*, *5*(1), 1-6.

[58]. [58]. [58]. Khalid, Z., Hassan, S. M., Mughal, S. S., Hassan, S. K., & Hassan, H. (2021). Phenolic Profile and Biological Properties of Momordica charantia'. *Chemical and Biomolecular Engineering*, *6*(1), 17.

[59]. [59]. [59]. Hassan, S. M., Mughal, S. S., Hassan, S. K., Ibrahim, A., Hassan, H., Shabbir, N., ... & Shafiq, S. (2020). Cellular interactions, metabolism, assessment and control of aflatoxins: an update. update. update. *Comput Biol Bioinform*, , , *8*, 62-71.

[60]. [60]. [60]. Khattak, A. K., Syeda, M. H., & Shahzad, S. M. (2020). General overview of phytochemistry and pharmacological potential of Rheum palmatum (Chinese rhubarb). rhubarb). rhubarb). *Innovare Journal of Ayurvedic Sciences*, , , *8*(6), 1-5.

[61]. [61]. [61]. Latif, M. J., Hassan, S. M., Mughal, S. S., Aslam, A., Munir, M., Shabbir, N., ... & Perveiz, S. (2020). Therapeutic potential of Azadirachta indica (neem) and their active phytoconstituents against diseases prevention. *J. Chem Cheml Sci.*, *10*(3), 98-110.

[62]. [62]. [62Khalid, Z., Hassan, S., Shahzad, S., & Khurram, H. (2021). A review on biological attributes of Momordica charantia. *Adv Biosci Bioeng*, *9*(1), 8-12.

Hafeez, M., Hassan, S. M., Mughal, S. S., Munir, M., & Khan, M. K. (2020). Antioxidant, Antimicrobial and Cytotoxic Potential of Abelmoschus esculentus. *Chemical and Biomolecular Engineering*, *5*(4), 69.

[63]. [63]. Afzal, N., Hassan, S. M., Mughal, S. S., Pando, A., & Rafiq, A. (2022). Control of Aflatoxins in Poultry Feed by Using Yeast. *American Journal of Chemical and Biochemical Engineering*, *6*(1), 21-26.

[64]. [64]. Shabbir, N., Hassan, S. M., Mughal, S. S., Pando, A., & Rafiq, A. (2022). Eletteria cardamomum and Greenly Synthesized MgO NPs: A Detailed Review of Their Properties and Applications. *Engineering Science*, *7*(1), 15-22.

[65]. [65]. Mubeen, N., Hassan, S. M., & Mughal, S. S. (2020). A Biological Approach to Control Aflatoxins by Moringa Oleifera. *International Journal of Bioorganic Chemistry*, *5*(2), 21.

[66]. [66]. Mubeen, N., Hassan, S. M., Mughal, S. S., Hassan, S. K., Ibrahim, A., Hassan, H., & Mushtaq, M. (2020). Vitality and Implication of Natural Products from Moringa oleifera: An Eco-Friendly Approach. *Computational Biology and Bioinformatics*, *8*(2), 72.

[67]. [67]. Aslam, A., Hassan, S. M., Mughal, S. S., Hassan, S. K., Ibrahim, A., Hassan, H., ... & Shafiq, S. (2020). Comprehensive Review of Structural Components of Salvia hispanica & Its Biological Applications. *International Journal of Biochemistry, Biophysics & Molecular Biology*, *5*(1), 1.

[68]. [68]. Mughal, S. S., & Hassan, S. M. (2022). Comparative Study of AgO Nanoparticles Synthesize Via Biological, Chemical and Physical Methods: A Review. *American Journal of Materials Synthesis and Processing*, *7*(2), 15-28.

[69]. [69]. Rafique, S., Hassan, S. M., Mughal, S. S., & Afzal, N. (2020). Asma Shafi 2, Sehrish Kamran 3 Department of Chemistry, Lahore Garrison University, Lahore, Punjab, Pakistan 2 Deparment of polymer, Punjab University Lahore, Pakistan 3 Department of Allied sciences, FMH College of medicine and dentistry. *GSJ*, *8*(9).

[70]. [Abbas, F., Tahir, M. U., Farman, M., Mumtaz, M., Aslam, M. R., Mughal, S. S., ... & Khan, A. R. Synthesis and Characterization of Silver Nanoparticles Against Two Stored Commodity Insect Pests.

[71]. Aslam, A., Hassan, S. M., Mughal, S. S., Perveiz, S., Mushtaq, M., Munir, M., ... & Ayub, A. R. Investigation of Biological Activity of Salvia hispanica.

[72]. Tahir, M. U., Abbas, F., Tahira, M., Shahzad, H. M., Sharif, S., Raza, A., ... & Ziad, M. SYNTHESIS OF MANGANESE-TIN BIMETALLIC MATERIALS AND STUDY OF ITS CATALYTIC APPLICATIONS.

[73]. ul Mustafa, Z., ullah Khan, A., Mudasar, A. S., & Mughal, S. S. Edge Functionalization of Phosphorene with different Chemical Functional Groups.

[74]. Muneer, M., Mughal, S. S., Pervez, S., Mushtaq, M., Shabbir, N., Aslam, A., ... & Abbas, F. DIAGNOSIS AND TREATMENT OF DISEASES BY USING METALLIC NANOPARTICLES-A REVIEW.

[75]. Mughal, S., Abbas, F., Tahir, M., Ayub, A., Javed, H., Mamtaz, M., & Iram, H. (2019). Role of Silver Nanoparticles in Colorimetric Detection of Biomolecules. doi:10.7537/marsbnj050419.04

[76]. Perveiz, S., Hassan, S. M., Mughal, S. S., Pando, A., Rafiq, A., & Shabbir, N. Structural, Morphological and Biotoxicity Studies of Biosynthesized CaO Nanoparticles Via Cuminum Cyminum.

[77]. SHABBIR, N., HASSAN, S. M., MUGHAL, S. S., PERVEIZ, S., MUNIR, M., MUSHTAQ, M., & KHAN, M. K. Peppermint oil, its useful, and adverse effects on human health: a review.

[78]. Perveiz, S., Hassan, S. M., Mughal, S. S., Ullah, H., Shabbir, N., Munir, M., ... & Farman, M. A Review on Heavy metal contamination in water and the Strategies for the Reduction of Pollution Load of Commercial and Industrial Areas of Pakistan.

[79]. Hafeez, M., Hassan, S. M., Mughal, S. S., & Mushtaq, M. Evaluation of Biological Characteristics of Abelmoschus esculentus.

[80]. Hassan, S. M., Mubeen, N., Hassan, S. K., Ibrahim, A., Hassan, H., Mughal, S. S.,. & Haider, G. MORINGA Oleifera, A MULTIFUNCTIONAL PLANT: A REVIEW STUDY.

[81]. Mushtaq, M., S.M. Hassan, and S.S. Mughal, Synthesis, Characterization and Biological Approach of Nano Oxides of Calcium by Piper nigrum. American Journal of Chemical Engineering, 2022. 10(4): p. 79-88.

[82]. Khushi, A., Hassan, S. M., & Mughal, S. S. Antimicrobial and Structural Investigation of Green Synthesized ZnO Nanostructures from Bougainvillea glabra Leaves Extract.

[83]. Khan, Aysha, Syeda Mona Hassan, and Shahzad Sharif Mughal. "Biological Evaluation of a Herbal Plant: Cichrorium intybus." *Science and Technology* 6.2 (2022): 26-38.

[84]. Muneeza Munir, Syeda Mona Hassan, Shahzad Sharif Mughal, Alvina Rafiq, Evaluation of Biological Approaches of Green Synthesized MgO Nanoparticles by *Syzygium aromaticum*, *International Journal of Atmospheric and Oceanic Sciences*. Volume 6, Issue 2, December 2022 , pp. 44-53. doi: 10.11648/j.ijaos.20220602.12

[85]. Lashari, Aamna, Syeda Mona Hassan, and Shahzad Sharif Mughal. "Biosynthesis, Characterization and Biological Applications of BaO Nanoparticles using Linum usitatissimum." *American Journal of Applied Scientific Research* 8.3 (2022): 58-68.

[86]. Hua, T. K., & Biruk, V. (2021). *Cybersecurity as a Fishing Game: Developing Cybersecurity in the Form of Fishing Game and What Top Management Should Understand*. Partridge Publishing Singapore.