Business, Management and Economics Engineering
ISSN: 2669-2481 / eISSN: 2669-249X
2024 Volume 22 Issue 02

CYBERSECURITY AND DATA PRIVACY IN FINANCIAL SERVICES: ANALYZE THE USE OF BIG DATA ANALYTICS AND ARTIFICIAL INTELLIGENCE FOR DETECTING AND PREVENTING CYBER THREATS, PROTECTING SENSITIVE FINANCIAL DATA, AND ENSURING COMPLIANCE WITH DATA PRIVACY REGULATIONS IN THE FINANCIAL SERVICES INDUSTRY

Dr. Suresh Kumar M. A.
Professor
Department of Management Studies,
Adhiyamaan College of Engineering (AUTONOMOUS), Hosur, India.
ORCID 0000-0002-4927-1931

Dr. Saravanan R
Professor
Happy Valley Business School, Coimbatore, Tamil Nadu, India

Dr. Dhanasekaran M
Professor and Head
Department of Management Studies,
Adhiyamaan College of Engineering (Autonomous), Hosur, India.

Mr. Sanjay B
Assistant Professor
Department of Management Studies,
Adhiyamaan College of Engineering (Autonomous), Hosur, India.

Abstract
In the realm of cybersecurity and data privacy within financial services, leveraging big data analytics and artificial intelligence (AI) is crucial for detecting, preventing, and mitigating cyber threats. These technologies enhance proactive defense mechanisms, safeguard sensitive financial data, and ensure compliance with data privacy regulations like GDPR and CCPA. Implementation of advanced analytics and AI solutions fortifies cybersecurity posture, protects financial data, and fosters regulatory adherence in the financial services industry.

Keywords: Cybersecurity; Data Privacy; Financial Services; Big Data Analytics, Artificial Intelligence.

1.1 INTRODUCTION

At the junction of financial services and cyber security, where the data privacy and the cutting-edge technologies like data analytics and AI is applied, protecting the financial data and mitigating the cyber risks have become crucial. The tandem of these technologies furnishes unparalleled chances of discovering, preventing, and retaliating against cyber-attacks in a more effective and accurate way. Through the use of big data analysis, financial institutions will evaluate huge amounts of data continuously to detect unusual patterns which might be an indication of impending threats, thereby improving their defense capabilities. Additionally, AI driven algorithms can improve predictive abilities of cybersecurity measures, particularly in selecting advanced preventive steps.

1.2 BACKGROUND

The Financial services sector increasingly uses big data and AI technologies to fight cyber-threats and define privacy standards. In terms of the Grand View Research report, the AI banking industry would reach $41.1 billion by 2026 and grow subsequent to improved security measures. Also, the massive exposure of the confidential financial information encourages strict cybersecurity policies and regulations to be put in place. In 2020, cybercriminals launched 125% more attacks on financial institutions, according to data published by VMware. Similarly, the application of big data analytics is growing at a fast pace, as per the predictions of Market Research Future which estimating the market of big data in banking will reach US$ 14.8 billion by the year 2027. The given numbers strongly suggest that AI and Big Data will be key for resistance to cyber-attacks and regulate data privacy in the financial service institutions.

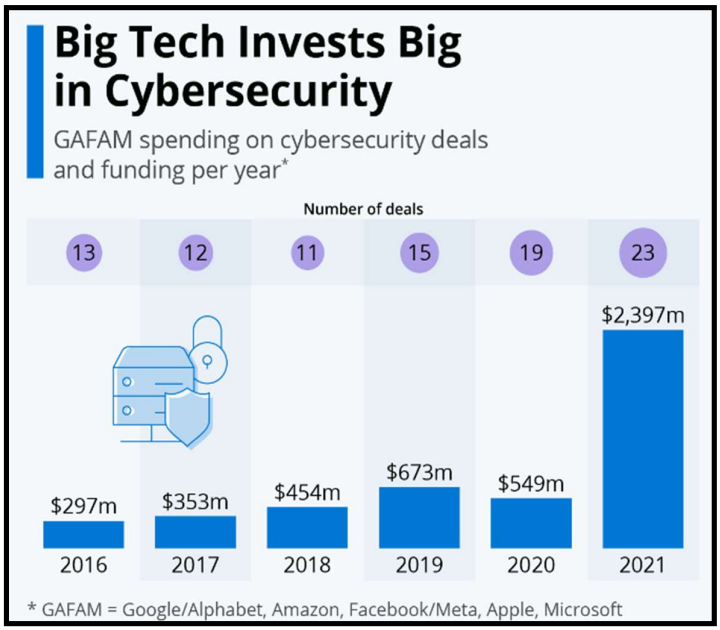

Fig.1. Big Tech Invests Big in Cybersecurity
(Source: statista.com, 2024)

While rapid progress in the digital era is undoubtedly beneficial, regulators must take a particular care to strike a balance between innovation and legal requirements. The analysis

discussed is targeted at identifying the various ways in which big data analytics and AI help in and protect sensitive financial data as well as on the way that the industry navigates through the intricate data privacy regulations.

1.3 AIM AND OBJECTIVES

Aim: To achieve cybersecurity resilience, protect confidential financial data, as well as comply with the data privacy regulation, it is important to apply big data analytics together with artificial intelligence in the financial services sector.

Objectives

- To improve proactive cyber threat surveillance and defense by integrating analytics of big data and AI technologies.
- To strengthen the cyber resilience through data analytics utilization i.e. data-driven cybersecurity measures.
- To fulfill the requirements of potent data governance and risk management by leveraging AI assisted governance tools.
- Taking advantage of big data analytics to predict and prevent, thus mitigating potential risks in finances and operations that could potentially be caused by cyber threats.

1.4 PROBLEM STATEMENTS

In the modern era of financial services, several pressing problems persist in the realm of cybersecurity and data privacy:

- While modern technologies do quite a bit to secure the banking sector, it is still susceptible to such sophisticated threats as ransomware and data breaches, which can ruin access to people's confidential finances [3].
- With the high demand for digital and online transactions and banking, the scope of attacks has expanded resulting in cyber-attacks targeting the financial institutions' security infrastructure that may be vulnerable to weaknesses present.
- Data protection compliance being mandatory and continuously evolving, for example GDPR and CCPA, means that financial organizations need to provide huge resources in order to make sure that they are in compliance while still adhering to the operational efficiency.
- Skilled cybersecurity professionals' shortage exacerbates the problem, as it issues efforts to fight cyber threats and protect financial data affected by the most sophisticated attacks more often.

2. LITERATURE REVIEW

2.1 INTRODUCTION

The literature on cyber protection and data privacy of financial services sector highlights the fact that adopting advanced technologies such as big data and artificial intelligence (AI) is the way to meet the evolving cyber threats. The studies demonstrate a higher efficiency of AI algorithms in recognizing outliers and predicting possible breaches which helps proactive security measures. Also, research highlighted that it is necessary for data privacy frameworks to be strong and to follow the mandatory regulations for the protection of individual sensitive financial data. Experts also highlight the possibility of having cybersecurity workforce shortages and stress the need for spending in training and

development. This literature calls upon the financial institutions to adopt a technical approach to strengthen their cybersecurity position and make sure they keep up with privacy policies.

2.2 REVIEW OF THE LITERATURE

Cybersecurity is one of the most vital problems on the international level which can be encountered by such sectors as the financial industry, for instance. Therefore, the graph below underlines the financial service industry as one of the main industries targeted by malicious agents, which is not encouraging at all as the cyber-attacks are becoming more complex. The cyber security risks that financial institutions and other similar organizations face are usually higher due to the high amounts of money that they keep and the valuable data of their customers being exposed.

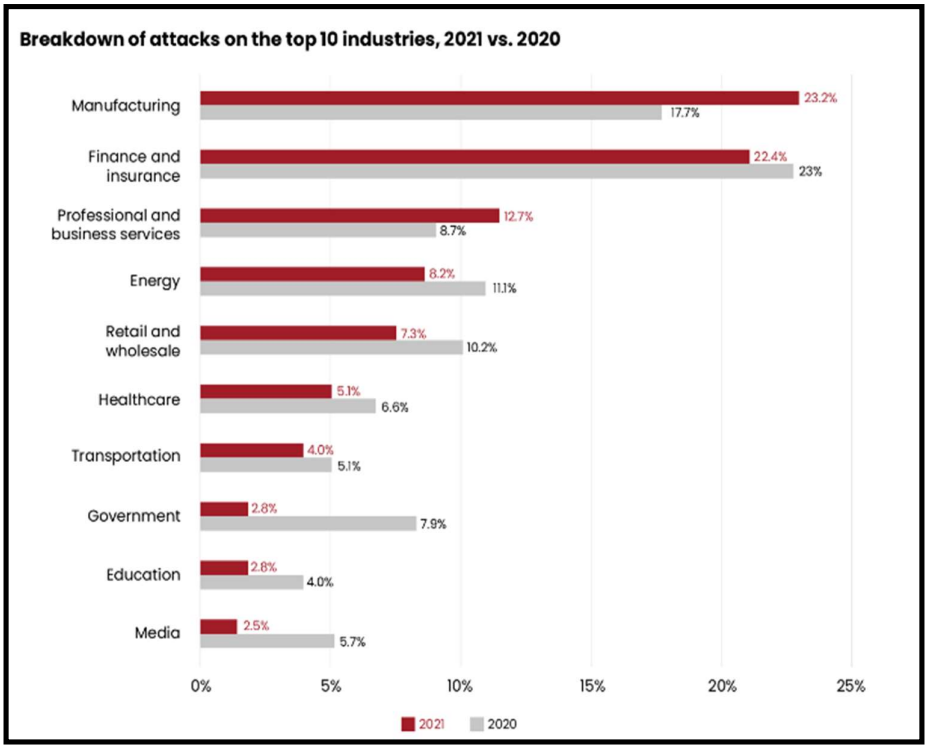

Fig.2. Breakdown of attacks on the top 10 industries, 2021 vs. 2020

It can be a different way of going under cyber-attacks for different organizations. Besides, there is no denying the fact that it is accompanied by many problems among which can be mentioned the financial loss, reputational harm, loss of customers' trust as well as paying the penalty. Organizations need to invest and devote their work to protecting data hence they will avoid such consequences and minimize inappropriate things arising. The organizations cannot hold responsibility alone for cybersecurity maintenance. One of the objectives of the new cyber security controls developed by many regulators, commissions, and institutions is to prevent, detect, and neutralize cyber threats. Cybersecurity frameworks are explained in documents that are called best practices, guidelines and standards which are developed to manage cybersecurity. Cybersecurity frameworks often include control frameworks, program frameworks, and risk frameworks. In cybersecurity, threat surveillance is the process of regular checking networks and endpoints for threats to limit the impact and maximize the whole data protection. The latest network threat monitoring technologies and

tools enable organizations to gain in a broader range of visibility that makes them able to find any irregularity or possible weakness and help better defense.

2.3 SUMMARY

The review of the literature claims that the development of new technologies, in particular big data analytics and AI, are of utmost importance for strengthening cybersecurity and data privacy for the financial services. It focuses on the additional investment of Big Tech into cybersecurity firms as well as the ever-increasing spending on information security globally. The next trends that form in an IT environment are securing the cloud and addressing remote work challenges. A prime example of this is the growing financial impact of cybercrime, such as business email compromise and data breaches, as well as the Russian cyber-attack concern.

3. METHODOLOGY

3.1 INTRODUCTION

The research methodology adopted in this study is a secondary research approach which is based on the investigation of the complex ecosystem of cybersecurity and data privacy within the financial sector. This part of the study encompasses meticulous study and combined analysis of the accessible sources of information such as studies, reports, and data related to the selected issue. This research through analysis and synthesis of various secondary sources intends to build a platform where crucial information on changing landscape of cybersecurity threats, resolves and regulatory practices in the financial sector can be gained.

3.2 RESEARCH APPROACH

The theoretical and principles of deductive research in this study are used to derive hypotheses to be tested. It begins with a general theory or principle and later gets particular data or predictions. This approach is started with the hypothesis or theoretical framework and then the data is collected to test the validity of it [7]. Applying inductive reasoning, this study undertakes to prove or disprove the thesis related to cybersecurity and data privacy in the financial services sphere and hence to contribute to the scientific knowledge in this area.

3.3 RESEARCH DESIGN

The used qualitative research design of this study exposes the figured-out opinions, attitudes and behaviors of the stakeholders within the banking industry on cybersecurity and data privacy. By utilizing research methods like interviews, focus groups, and theme analysis, qualitative research seeks to extract the intricacies surrounding cybersecurity behaviors, organizational cultures, and regulatory frameworks [7]. In this research design, key stakeholders will be explored based on their subjective experiences and perspectives thus enabling deeper knowledge into the human element in cybersecurity operations in financial institutions.

3.4 RESEARCH METHOD

As a result, the research takes a secondary standpoint whereby thematic analysis is used as the approach. In this stage, sources that are accessible and semi-structured comprising of books, literature and reports are scanned in order to identify the recurrent issues and emerging patterns regarding cybersecurity and data privacy in financial services sector.

3.5 DATA COLLECTION TECHNIQUES

Thematic analysis is the most widely used data collection method among qualitative research approaches that involve the use of secondary documents as a data source [8]. Exploring the secondary data, which entails getting recurring themes or patterns from published reports, literature, and other documents by means of thematic analysis, and which is a systematic identification, analysis, and interpretation of the themes is one of our approaches. Given such technique allows to handle complex story topics and find necessary information from scientific research put forward.

3.6 SUMMARY

The method is based on secondary research which incorporates qualitative techniques like thematic analysis. It includes not only the disclosure of current knowledge and data resources, but also analysis regarding cybersecurity and data breaches in the financial industry. This chapter's concise analysis is designed to drive towards what to do about the changing security landscape, including protective strategies, and regulatory compliance.

4. RESULTS AND FINDINGS

4.1 INTRODUCTION

Consequently, the Results and Findings section provides the viewer with the summarized information from the secondary data analysis, hence, giving a thorough preview of the growth in cybersecurity and data privacy in the banking industry.

4.2 FORTIFYING THE DIGITAL FORTRESS: BIG TECH'S BILLION-DOLLAR BET ON CYBERSECURITY

On 8th of March, Google announced the buying of cybersecurity company Mandiant for $5.4 billion plans. This is likely the biggest acquisition of Big Tech vendors of cybersecurity in recent years. Some time ago, GAFAM clarified that course as the field worth investing in, but starting from last year, it substantially increased its financial injections to it, the chart shows. According to CB Insights' data on funding or acquisitions, in 2021 Alphabet, Amazon, Meta, Apple and Microsoft invested $2.4 billion in cybersecurity, an increase of approximately $1.8 billion or 336 percent from the previous year. In fact, most deals in this field are not takeovers. Since 2016 up till now, there were only 17 companies which were bought or acquired by the GAFAM corporations, and Microsoft and Amazon being the ones with the highest number of buyouts, i.e., 8 and 4, respectively.

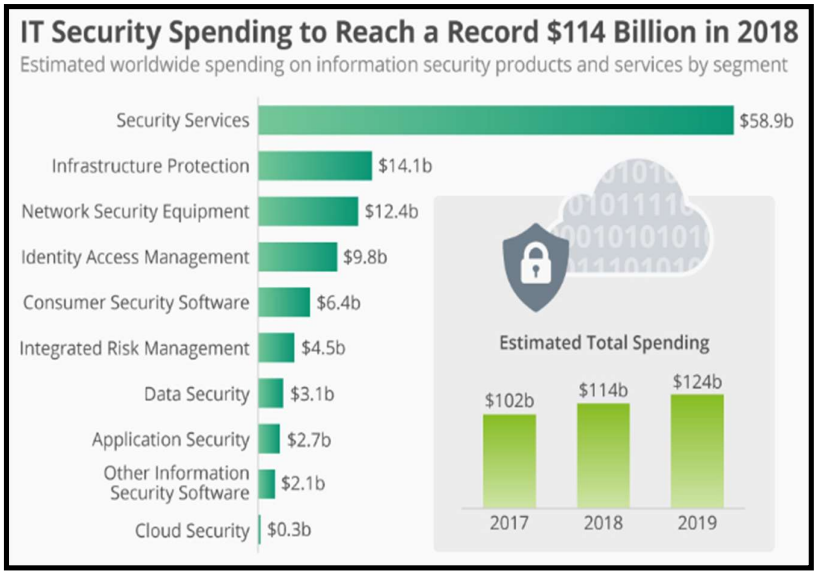

Fig.3. Information Security Spending to Reach a Record $114 Billion in 2018 (Source: statista.com, 2024)

Cyber-attacks and online scams are at the time more common as there is need for protection of information that is private or confidential which in turn organizations spends billions of money to keep it safe. When referring to Gartner's data, worldwide spending on information security products and services is estimated to reach $114 billion this year, an increase from $102 billion in 2017. This graph demonstrates that the biggest portion of that gigantic portion of the huge total will be spent on security services, followed by infrastructure security, and network equipment security.

4.3 EMERGING TRENDS IN CYBERSECURITY: NAVIGATING REMOTE WORK CHALLENGES AND RISKS

In term of technology, the cloud and the Internet of Things is an expanding topic which has to become the top priority right now. While this is a positive development for an individual, the use of a remote or hybrid work model also outstrips the capacity of the cybersecurity infrastructure since it allows hackers to have more attack points. In 2021, the cost of cybercrime was approximated to be more than $6 trillion and in 2025, it is forecasted to think more than $10 trillion by Cybercrime Magazine.

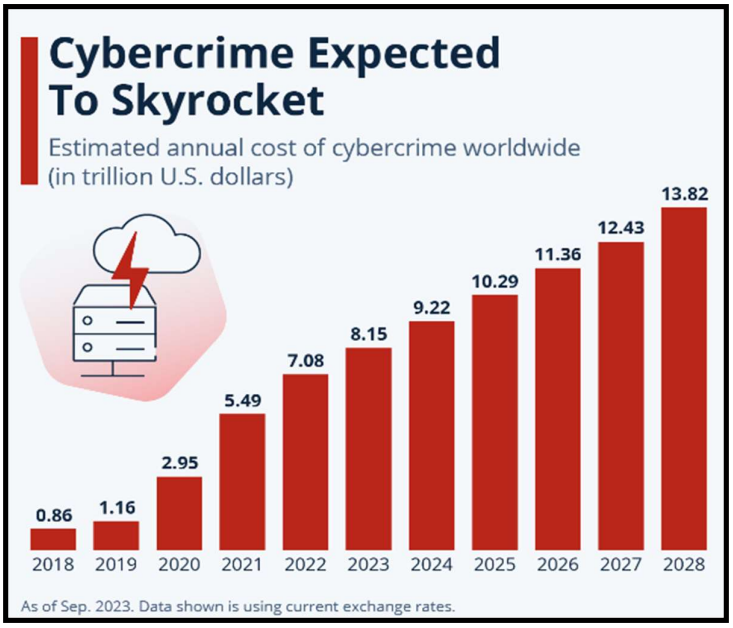

Fig.4. Cybercrime Expected to Skyrocket in Coming Years
(Source: statista.com, 2024)

Cybercrime according to Cyber Crime Magazine is "theft, attack or damage of software, losses of money, lost productivity, intellectual property theft, personal or financial data theft, embezzlement, fraud, post-attack disruption to the normal proceedings of work, forensic investigation, restoration and deletion of data and systems compromised by hackers, and reputational damage." With the boom of online activities, be However, the attackers become more advanced as attacker techniques start getting more advanced with more tools that help the scammers.

4.4 ESCALATING CYBER CRIME: FBI REPORT REVEALS SOARING LOSSES IN 2021

According to the FBI report published today, cybercrime losses have increased dramatically this year. An estimated $6.9 billion disappeared globally in 2021 as compared to $4.2 billion in 2020, and most of the shortfalls were recorded in the US. The latter crime category recorded by the FBI was business email compromise and personal email compromise that targets companies and people who transfer money over the wire by breaking into their emails. A total of USD 2.4 billion was lost in 2021 through this way. The report was published right before US warnings about a surge in Russian cyber-attacks as retaliation for the sanctions imposed on the country in the wake of its invasion of Ukraine. U.S. President Joe Biden advised businesses on Monday that their vulnerabilities might be exploited by Russian hackers. Another costly cybercrime with businesses at their center was personal data breaches and corporate data breaches, when criminals steal or release previously stored personal data of individuals or companies.

The U.S. government additionally cautioned of possibility of Russian cyber-attacks on infrastructure like the power grid, water treatment plants and hospitals. The US, along with many countries internationally, was also hit with cybercrimes that were costly with investment, romance, real estate and tech support scams all costing more than $3 billion. The fastest growing cybercrime category for 2020 was investment fraud which increased 333 percent in

cost compared to the previous year and was followed by personal data breaches and tech support scams. Out of all subjects observed by the FBI, 59 percent were discovered in the US, 38 percent in the UK, and 3 percent elsewhere.

4.5 SUMMARY

From the results, it is evident that having efficient cybersecurity and compliance with the regulations is ultimately what safeguards financial information The data demonstrates major developments, the main problems and the potential avenues to fight cyber threats in the financial sector.

5. CONCLUSION

Finally, the multilayered review of the cybersecurity and data protection in the area of finance expounds the significant role of big data analysis and artificial intelligence in containing cyber risks and protecting financial data. The literature review indicates the loss of cybercrime is getting higher, as well as it emerges the new tendency and problems which financial institutions are faced with. It highlights the challenges of cybersecurity, compliance, and supporting innovation in the while simultaneously identifying the opportunities than arise from it. The outcome will help cybersecurity authorities to comprehend platform security issues, regulatory issues like data privacy, and evolving risks of financial services thus mobilizing proactive measures for the dynamic environment.

Recommendations

- Implementation of cutting-edge Big Data Analytics and AI technologies to beef up and expand cyber threat detection and anticipation capacities.
- Improve the privacy infrastructure by implementing the strict data privacy policy of the GDPR and CCPA guidelines.
- Aim to eliminate the lack of cybersecurity expertise through a variety of workforce development projects.
- Partner financial institutions and regulators to be able to face new cyber threats effectively.

References

[1] Casillo, Mario, Liliana Cecere, Francesco Colace, Angelo Lorusso, and Domenico Santaniello. 2024. "Integrating the Internet of Things (IoT) in SPA Medicine: Innovations and Challenges in Digital Wellness." Computers 13 (3): 67. doi: https://doi.org/10.3390/computers13030067. https://www.proquest.com/scholarly-journals/integrating-internet-things-iot-spa-medicine/docview/2989395881/se-2.

[2] Demertzi, Vasiliki, Stavros Demertzis, and Konstantinos Demertzis. 2023. "An Overview of Privacy Dimensions on the Industrial Internet of Things (IIoT)." Algorithms 16 (8): 378. doi:https://doi.org/10.3390/a16080378. https://www.proquest.com/scholarly-journals/overview-privacy-dimensions-on-industrial/docview/2856753566/se-2.

[3] Faccia, Alessio. 2023. "National Payment Switches and the Power of Cognitive Computing Against Fintech Fraud." Big Data and Cognitive Computing 7 (2): 76. doi:

https://doi.org/10.3390/bdcc7020076. https://www.proquest.com/scholarly-journals/national-payment-switches-power-cognitive/docview/2829699545/se-2.

[4] Mircea Constantin Șcheau, Mihail Rangu Călin, Vasile Popescu Florin, and Daniel Mihail Leu. 2022. "Key Pillars for FinTech and Cybersecurity." Acta Universitatis Danubius.Oeconomica 18 (1). https://www.proquest.com/scholarly-journals/key-pillars-fintech-cybersecurity/docview/2769349027/se-2.

[5] PDF. 2024. "Prominent Security Vulnerabilities in Cloud Computing." International Journal of Advanced Computer Science and Applications 15 (2). doi: https://doi.org/10.14569/IJACSA.2024.0150281. https://www.proquest.com/scholarly-journals/prominent-security-vulnerabilities-cloud/docview/2992551149/se-2.

[6] Ribas Monteiro, Luiz Fernando, Yuri R. Rodrigues, and de Souza A C Zambroni. 2023. "Cybersecurity in Cyber–Physical Power Systems." Energies 16 (12): 4556. doi: https://doi.org/10.3390/en16124556. https://www.proquest.com/scholarly-journals/cybersecurity-cyber-physical-power-systems/docview/2829799885/se-2.

[7] Sampaio, Silvio, Patricia R. Sousa, Cristina Martins, Ana Ferreira, Luís Antunes, and Ricardo Cruz-Correia. 2023. "Collecting, Processing and Secondary using Personal and (Pseudo)Anonymized Data in Smart Cities." Applied Sciences 13 (6): 3830. doi: https://doi.org/10.3390/app13063830. https://www.proquest.com/scholarly-journals/collecting-processing-secondary-using-personal/docview/2791584925/se-2.

[8] Villegas-Ch, William, Jaime Govea, and Iv Ortiz-Garces. 2024. "Developing a Cybersecurity Training Environment through the Integration of OpenAI and AWS." Applied Sciences 14 (2):679. doi: https://doi.org/10.3390/app14020679. https://www.proquest.com/scholarly-journals/developing-cybersecurity-training-environment/docview/2918559767/se-2.

[9] Dr.S.Thanga Ramya, et al, Secure forensic data transmission system in cloud database using fuzzy based butterfly optimization and modified ECC, Transactions on emerging telecommunications technologies, Vol.33June 2022, https://doi.org/10.1002/ett.4558

[10] Dr.S.Thanga Ramya, et al, Hybrid Cloud Data Protection Using Machine Learning Approach, Advanced Soft Computing Techniques in Data Science, IoT and Cloud Computing (Springer),Nov 2021, Vol 89, 151-166, DOI: 10.1007/978-3-030-75657-4_7.

[11] Dr.S.Thanga Ramya, et al, Memory and Time aware Automated Job Ontology Construction with reduced Ontology Size Based Semantic Similarity, Journal of Xi'an Shiyou University, Natural

[12] Dr.S.Thanga Ramya, et al, Modified Mackenzie Equation and CVOA Algorithm Reduces Delay in UASN, Computer Systems Science and Engineering, Vol.41, No.2, 2022, pp.829-847, 829-847, doi:10.32604/csse.2022.020307.

[13] Dr.S.Thanga Ramya, et al, Roadmap to Biomedical Image Segmentation and Processing – Background and Approaches, Design Engineering, 2021, Issue: 7, 8491 – 8504, 8491 – 8504, 0011-9342.

[14] Dr.S.Thanga Ramya, et al, Smart Supermarket Billing Automation System based on barcode recognition using canny Edge detection, Annals of R.S.C.B, 2021,Vol. 25, Issue 4, 19139-19143, ISSN:1583-6258.

[15] Dr.S.Thanga Ramya, et al, Enhanced Features based Private Virtual Card, Annals of R.S.C.B, 2021,Vol. 25, Issue 4, 17867 - 17872, ISSN:1583-6258.

[16] Dr.S.Thanga Ramya, et al, IOT Based an Efficient Image Processing Algorithm for Capture Image in Museum using Localization Service for user Involvement, Revistageintec-gestaoinovacao e tecnologias (Management, Innovation and Technologies) Online, Vol. 11 No. 2 (2021), 2322-2331, ISSN: 2237-0722.

[17] Dr.S.Thanga Ramya, et al, Private virtual card as additional security, Elementary Education Online, 2021; Vol 20 (Issue 5), 7341-734.

[18] Dr.S.Thanga Ramya, et al, Deep Learning Driven Image Segmentation in Medical Science - An Intense Learning, Solid State Technology, 2021 Volume: 64 Issue: 2, 1725-1734.

[19] Dr.S.Thanga Ramya, et al, Software Defined Networking: A Paradigm Shift in Networking for Future, Emerging Trends and Applications., International Journal of Applied Engineering Research., Volume 13, Number 18 (2018) , pp.13475 – 13481., ISSN 0973 – 4562.

[20] Dr.S.Thanga Ramya, et al, Novel Effective X-Path Particle Swarm Extraction based Retrieval for Deprived Videos, Springer Cluster computing, Online: Oct 2017, , 1573-7543.

[21] Dr.S.Thanga Ramya, et al, Xml Based Approach For Object Oriented Medical Video Retrieval Using Neural Networks, Journal Of Medical Imaging And Health Information, VOL.6., (2016), pp.1-8, 2156-7018.

[22] Dr.S.Thanga Ramya, et al, Knowledge based methods for video data retrieval, International Journal of Computer Science & Information Technology, October 2011 Vol.3, no.5 , pp.165-172, 0975-4660.

[23] Dr.S.Thanga Ramya, et al, Person identification using OODB- A fuzzy logic approach, i-manager's Journal on Software Engineering, Vol. 3l, pp 32-42, 0973-5151.

[24] Pillai, S. R., & Chithirai, P. S. M. (2019). Collision avoidance mechanism in vehicles using neural networks. Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018, 76-81. https://doi.org/10.1109/ICSSIT.2018.8748689

[25] Ramaswamy Pillai, S., Reddy Madara, S., & Pon Selvan, C. (2019). Prediction of kerf width and surface roughness in waterjet cutting using neural networks. In Journal of Physics: Conference Series (Vol. 1276). https://doi.org/10.1088/1742-6596/1276/1/012011

[26] Pillai, S. R., Pon Selvan, C., & Madara, S. R. (2019). Design of PID control to improve efficiency of suspension system in electric vehicles. In Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019 (pp. 570-575). https://doi.org/10.1109/ICCIKE47802.2019.9004322.

[27] Chithirai Pon Selvan, M., Midhunchakkaravarthy, D., Senanayake, R., Ramaswamy Pillai, S., & Reddy Madara, S. (2020). A mathematical modelling of abrasive waterjet machining on Ti-6Al-4V using artificial neural network. Materials Today: Proceedings, 28, 538-544. https://doi.org/10.1016/j.matpr.2019.12.215

[28] Madara, S. R., Pillai, S. R., Chithirai Pon Selvan, M., & Van Heirle, J. (2021). Modelling of surface roughness in abrasive waterjet cutting of Kevlar 49 composite using artificial neural network. Materials Today: Proceedings, 46, 1-8. https://doi.org/10.1016/j.matpr.2020.02.868.

[29] Suresh, A. B., Selvan, C. P., Vinayaka, N., et al. (2024). Computational investigations of aluminum-based airfoil profiles of helical shaped vertical axis wind turbines suitable for friction stir joining and processing. International Journal on Interactive Design and Manufacturing, 18(1), 1491–1506. https://doi.org/10.1007/s12008-022-01181-9

[30] Shivalingaiah, K., Nagarajaiah, V., Selvan, C. P., Kariappa, S. T., Chandrashekarappa, N. G., Lakshmikanthan, A., Chandrashekarappa, M. P. G., & Linul, E. (2022). Stir casting process analysis and optimization for better properties in Al-MWCNT-GR-based hybrid composites. Metals, 12(1297). https://doi.org/10.3390/met12081297

[31] Shankar, V. K., Lakshmikanthan, A., Selvan, C. P., et al. (2023). Prediction of transient temperature at bit-rock interface using numerical modelling approach and optimization. International Journal on Interactive Design and Manufacturing. https://doi.org/10.1007/s12008-023-01543-x

[32] Kumar, S., Lakshmikanthan, A., Selvan, C. P., et al. (2023). Effect of interlock angle and bottom die flange diameter on clinching joint load bearing capacity in cross-tensile loading. *International Journal on Interactive Design and Manufacturing, 17*(1), 2209–2220. https://doi.org/10.1007/s12008-022-00955-5

[33] Nagarajan Thiyaneshwaran, Chithirai Pon Selvan, Lakshmikanthan, A., Sivaprasad, K., & Ravisankar, B. (2021). Comparison based on specific strength and density of in-situ Ti/Al and Ti/Ni metal intermetallic laminates. Journal of Materials Research and Technology, 14, 1126-1136. https://doi.org/10.1016/j.jmrt.2021.06.102

[34] Minervini G, Franco R, Marrapodi MM, Di Blasio M, Ronsivalle V, Cicciù M. Children oral health and parents education status: a cross sectional study. BMC Oral Health. 2023 Oct 24;23(1):787. doi: 10.1186/s12903-023-03424-x. PMID: 37875845; PMCID: PMC10594879.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85174817824&origin=resultslist

[35] Minervini G, Franco R, Marrapodi MM, Almeida LE, Ronsivalle V, Cicciù M. Prevalence of temporomandibular disorders (TMD) in obesity patients: A systematic review and meta-analysis. J Oral Rehabil. 2023 Dec;50(12):1544-1553. doi: 10.1111/joor.13573. Epub 2023 Aug 27. PMID: 37635375.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85168909924&origin=resultslist

[36] Minervini G, Franco R, Marrapodi MM, Di Blasio M, Isola G, Cicciù M. Conservative treatment of temporomandibular joint condylar fractures: A systematic review conducted according to PRISMA guidelines and the Cochrane Handbook for Systematic Reviews of Interventions. J Oral Rehabil. 2023 Sep;50(9):886-893. doi: 10.1111/joor.13497. Epub 2023 May 24. PMID: 37191365.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85160102823&origin=resultslist

[37] Minervini G, Franco R, Marrapodi MM, Fiorillo L, Cervino G, Cicciù M. The association between parent education level, oral health, and oral-related sleep disturbance. An observational crosssectional study. Eur J Paediatr Dent. 2023 Sep 1;24(3):218-223. doi: 10.23804/ejpd.2023.1910. PMID: 37668455.

https://www.scopus.com/record/display.uri?eid=2-s2.0-85169847956&origin=resultslist

[38] Minervini G, Franco R, Marrapodi MM, Fiorillo L, Cervino G, Cicciù M. Post-traumatic stress, prevalence of temporomandibular disorders in war veterans: Systematic review with meta-analysis. J Oral Rehabil. 2023 Oct;50(10):1101-1109. doi: 10.1111/joor.13535. Epub 2023 Jun 23. PMID: 37300526.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85169847956&origin=resultslist

[39] Di Stasio D, Romano A, Paparella RS, Gentile C, Serpico R, Minervini G, Candotto V, Laino L. How social media meet patients' questions: YouTube™ review for mouth sores in children. J Biol Regul Homeost Agents. 2018 Jan-Feb;32(2 Suppl. 1):117-121. PMID: 29460528.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85042328325&origin=resultslist

[40] Di Stasio D, Lauritano D, Romano A, Salerno C, Minervini G, Minervini G, Gentile E, Serpico R, Lucchese A. IN VIVO CHARACTERIZATION OF ORAL PEMPHIGUS VULGARIS BY OPTICAL COHERENCE TOMOGRAPHY. J Biol Regul Homeost Agents. 2015 Jul-Sep;29(3 Suppl 1):39-41. PMID: 26511179.
https://www.scopus.com/record/display.uri?eid=2-s2.0-84992222066&origin=resultslist

[41] Di Stasio D, Lauritano D, Gritti P, Migliozzi R, Maio C, Minervini G, Petruzzi M, Serpico R, Candotto V, Lucchese A. Psychiatric disorders in oral lichen planus: a preliminary case control study. J Biol Regul Homeost Agents. 2018 Jan-Feb;32(2 Suppl. 1):97-100. PMID: 29460524.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85042256369&origin=resultslist

[42] Lucchese A, Dolci A, Minervini G, Salerno C, DI Stasio D, Minervini G, Laino L, Silvestre F, Serpico R. Vulvovaginal gingival lichen planus: report of two cases and review of literature. Oral Implantol (Rome). 2016 Nov 13;9(2):54-60. doi: 10.11138/orl/2016.9.2.054. PMID: 28042431; PMCID: PMC5159910.
https://www.scopus.com/record/display.uri?eid=2-s2.0-84995923599&origin=resultslist

[43] Di Stasio D, Romano A, Gentile C, Maio C, Lucchese A, Serpico R, Paparella R, Minervini G, Candotto V, Laino L. Systemic and topical photodynamic therapy (PDT) on oral mucosa lesions: an overview. J Biol Regul Homeost Agents. 2018 Jan-Feb;32(2 Suppl. 1):123-126. PMID: 29460529.
https://www.scopus.com/record/display.uri?eid=2-s2.0-85042255902&origin=resultslist

[44] Trasca, T. I., Ocnean, M., Gherman, R., Lile, R. A., Balan, I. M., Brad, I., ... & Firu Negoescu, G. A. (2024). Synergy between the Waste of Natural Resources and Food Waste Related to Meat Consumption in Romania. Agriculture, 14(4), 644.

[45] Balan, I. M., Gherman, E. D., Gherman, R., Brad, I., Pascalau, R., Popescu, G., & Trasca, T. I. (2022). Sustainable nutrition for increased food security related to romanian consumers' behavior. Nutrients, 14(22), 4892.

[46] Balan, I. M., Gherman, E. D., Brad, I., Gherman, R., Horablaga, A., & Trasca, T. I. (2022). Metabolic Food Waste as Food Insecurity Factor—Causes and Preventions. Foods, 11(15), 2179.

[47] Balan, I. M., Popescu, A. C., Iancu, T., Popescu, G., & Tulcan, C. (2020). Food safety versus food security in a world of famine. Food Safety Versus Food Security in a World of Famine. Journal of Advanced Research in Social Sciences and Humanities, 5(1), 20-30.

[48] Salasan, C., & Balan, I. M. (2022). The environmentally acceptable damage and the future of the EU's rural development policy. In Economics and Engineering of Unpredictable Events (pp. 49-56). Routledge.

[49] Lile, R., Constantinescu, S. C., Durau, C. C., Ocnean, M., & Balan, I. M. (2016). RESEARCH ON AQUACULTURE IN ROMANIA OVER THE PAST DECADE-QUALITY AND DYNAMICS. In 3rd International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2016 (pp. 1005-1012).

[50] Balan, I. M., Chis, S. S., Constantinescu, S. C., Ciolac, R. M., Sicoe-Murg, O. M., & Chis, S. (2016). Romanian imports evolution of fish and fish products according to quality classes. Journal of Biotechnology, (231), S101.

[51] Cornelia, P., Ioana, B., Petroman, I., DORA, O. M., Băneș, A., Trifu, C., & Diana, M. (2009). Național grading of quality of beef and veal carcasses in Romania acconrding to EUROP sistem. Food Journal of Agriculture & Enviroment science and technology, 7(3&), 4.

[52] Sălășan, C., & Bălan, I. (2014). Suitability of a quality management approach within the public agricultural advisory services. Quality-Access to Success, 15(140), 81-84.

[53] BALANCE OF RED MEAT IN ROMANIA - ACHIEVEMENTS AND PERSPECTIVES https://www.webofscience.com/wos/woscc/full-record/WOS:000385997200048
Nicoleta MATEOC SIRB, Paun Ion OTIMAN, Teodor MATEOC, Cosmin SALASAN, Ioana ...
FROM MANAGEMENT OF CRISIS TO MANAGEMENT IN A TIME OF CRISIS