ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

ENHANCING REGULATORY COMPLIANCE THROUGH TRAINING AND DEVELOPMENT PROGRAMS: CASE STUDIES AND RECOMMENDATION

Mitul Tilala[1], Abhip Dilip Chawda[2], Abhishek Pandurang Benke[3]

1Independent Researcher,USA.

2Independent Researcher,USA.

3Independent Researcher,USA.

Corresponding Author

Mitul Tilala

Independent Researcher,USA.

Email:tilalamitul@gmail.com

Abstract :

This article explores the significance of training and development in improving worker performance, particularly in the realm of Information Systems (IS) security. Recognizing that employees are crucial assets to any organization, the study focuses on the effectiveness of IS security training in fostering compliance and reducing security breaches. It employs two theoretical frameworks—the Elaboration Likelihood Model (ELM) and Universal Constructive Instructional Theory (UCIT)—to design a comprehensive training program aimed at enhancing cognitive processing and retention of security policies among employees.

The research adopts an action research methodology, characterized by a cyclical process of intervention and evaluation. This approach allows for the continuous refinement of the training program based on empirical evidence. The study is structured into four phases: identifying instructional tasks, diagnosing learner states, delivering instructional content, and evaluating training outcomes.

Results from the study reveal substantial improvements in employees' understanding and adherence to IS security policies, as well as heightened awareness of the risks associated with non-compliance. The findings underscore the effectiveness of theoretically grounded

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

training programs in achieving long-term behavioral change and enhancing organizational security.

Overall, the article provides valuable insights into the design and implementation of IS security training programs, demonstrating how the integration of ELM and UCIT can lead to more effective and sustainable training outcomes. It concludes with recommendations for further refining training approaches to better address the evolving security needs of organizations.

Keywords: Regulatory compliance,Training programs,Development programs,Case studies,Recommendations,Risk mitigation,Compliance culture,Regulatory excellence.

Introduction

Workers are the main asset of an organisation. The working process and working experience of the employees are the main subjects of worker performance. Hence, organisational managers need to identify the effectiveness of training and development workers' performance and also evaluate th

tion of the company's competitive advantages in the modern market. Research has been conducted in the training and development to enhance worker performance. The main purpose of this article is to provide effective information about the process of worker performance, training, development and evaluation. Worker's and user's noncompliance along with IS policies, and security is increasing IS security issues in organisations' security and computer crime [1]. At a time when users cannot comply with the policies of IS, this security deals huge loss in their efficiency. In order to address different types of approaches along with the uses of sanctions depending on deterrence theory, training, education and marketing campaigns. Sanction-dependent approaches argue with the fear of determines at the time of worker co only with different policies. The main aim of IS security education and training is the worker and active worker's thinking ability. Apart from punitive approaches, many countries adopted non-punitive activities which are focused on cognitive training and education. Sanction is an effective approach to providing security training [2]. However, IS security training and approaches largely remained anecdotal and atheoretical. Empirical evidence and underlying theories continue the princess of IS security training. Training programs can not follow any tools and theory which will be effective in working situations.

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

Background of study

This article focuses on security training is typically incorporated with upgrading used companies depending on IS security policies. These policies are associated with the instructor-led process which uses various web-related tutorials and videos. Hence, only two types of theoretical approaches are used in training programs.

Theoretical framework

In order to seek appropriate candidates based on the training program, this article has focused on two effective theories, these theories are mentioned below.

Elaboration Likelihood Model (ELM):

Dealing with different challenges, IS security training should focus on the use of effective training methods that enable the system's cognitive information process. Thus model is focused on highly motivated users who like to apply cognitive processing. On the other hand, personal relevance provides strong motivation for this theory [3]. The main aim of this motivation is to avoid superficial information processing. Thus security policy is against the use of learning tasks.

Universal Constructive Instructional Theory (UCIT)

This model is effective for guiding the training approaches depending on the phase framework. These phases are mentioned below.

a. Knowing the industrial task
b. Diagnostics of learner and present state
c. Delivering and constructing proper instructions
d. Diaginisis the high rate of success

Depending on UCI's effective process, identify, and determine the instructional job present in the first task [4]. The main focus of this article is to provide guidance to the instructional job by following IS security policy. The second phase is associated with diagnosing the present mindset of the learner who is going to explore the instructional job. Some guidance and knowledge are essential for the learner. There is a huge difference between requirement and knowledge helps to define what the learner needs to learn. This approach is known as a learning task. In the third phase, delivering and constructing instruction which is related to the learning task are conducted and delivered. In the next stage, the main aim of IS security training is provided to the instructor. The instructor has to consider different aspects of IS security policy in particular target groups [5]. The principle of cognitive processing of information provide guidance on providing instruction whose aim is to provide long-lasting

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

effective changes in users. In the last phase, the success of instruction, and diagnosis of success are properly accessed by identifying the user's degree. This model highlights vital and crucial elements for delivery and design as per the instruction. The instruction depends on functions, and components of the effective instructions and pointed out the constraints and possibilities for effective learning in some organisations. The approaches of UCIT are dependent on knowledge which provides an effective impact on IS security learning users. The functions of this model are, accepting the knowledge and keeping the knowledge in proper storage [6]. The last function is the use of this knowledge. The components of this model are associated with learning and understanding the environment (teaching methods instructor and media). Second is the effective learning job which is associated with the policies of IS security. The third function is the user or learners and the fourth function is the place in which the instruction is provided. The basic function and components of this model are the user and his modern and effective knowledge of learning. Delivery and design of the training program and IS security policy are focused on the user's efficiency of using effective modern knowledge. UCIT model suggests what the user should learn and is influenced by constraints and possibilities to arise user's previous knowledge[7]. IS security policy provides compliance against leverage training of the learner depending on the knowledge of IS security policy.

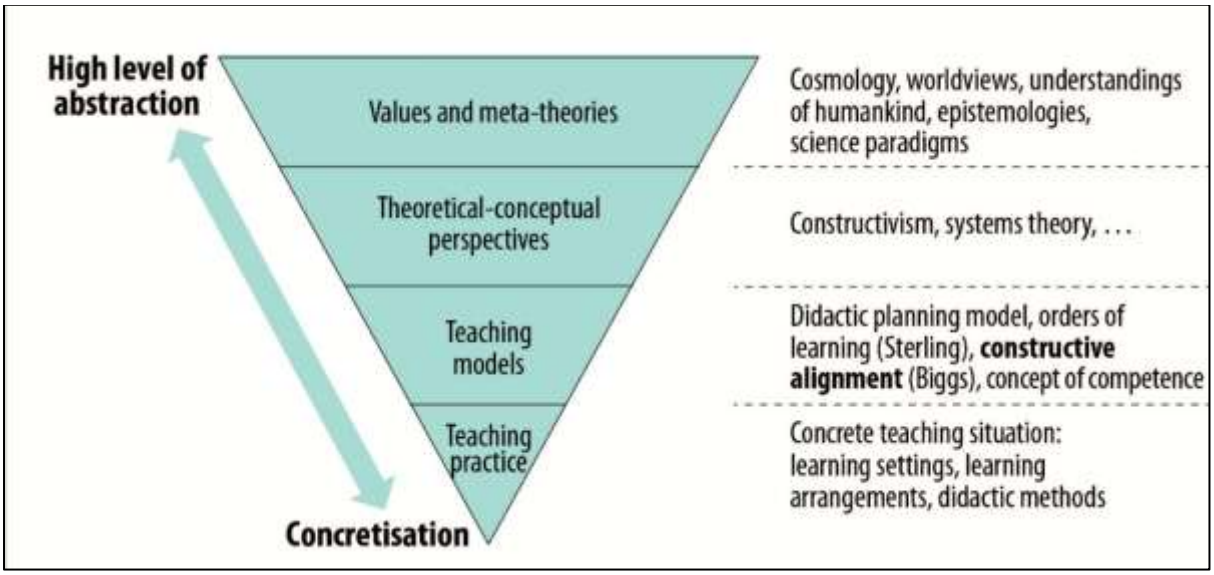

Figure 1: Universal Constructive Instructional Theory

Source: [11]

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

Methodology

The research action has stood out as the ideal method of research for possibly refining and validating the IS policy of safety. It has owned the intervention of the cyclical field in terms of theory testing. Action research is a clinical method, aimed at creating change in the organisation. This study has also discussed how this programme has been used to transmit the behaviour of the employees by using the method of action research. It has discussed the four stages of UCIT instruction. Thee phase 1 has depicted the instructional task and its determination. Phase 2 has diagnosed the current position of the researcher and these two phases have been considered as the learning task[8]. Phase 3 has discussed delivering and constructing the construction. In this phase, the ELM principles have been been utilised to provide the guidance on this instruction design that is aimed at long-lasting change. The final phase has discussed the diagnosis of the success. All the methods of collecting the information at the time of interviews have been recorded[9]. The utilisation of the audio recorder has been abandoned as it has been stated that the use of tape recorders has been less open and less truthful.

Result and Discussion

This paper has discussed the enhancement of the “IS security policy” training programme of regulatory compliance. The enhancement of the programme has been built on two essential theories named ELM and UCIT. There are four key sessions and the first session has been designed for all users. The first session has three parts, and the first part has been designed as a collaborative discussion about the issues regarding the utilisation of email. The main aim of the design has been to activate the existing knowledge of the learners. This has been expected to develop learning in regulatory compliance. One of the main tasks has been to improve the activities of the learners to enhance their knowledge of new information. It has been essential for long-lasting change. The next part has been designed to utilise the email papers which had been given to the customers and partners. This design aimed to utilise the learner's own document that is authentic, although the task was created to assess the documents and identify confidential information.

First Phase

The next part was designed to assess the potential consequences of regulatory compliance among the learners and the team. The information has been confidential and it has been included product development cost and product pricing, the profit and the details of the

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

company in a different way. The information of the company has come out in front of the public and its competitors could result in a losing ground for the company. It would be an essential economic loss for the company and its main task was to make it significant. This task was created to make a "cost-effective mental model" and it has been considered to be the key factor of long-lasting change in regulatory compliance.

Second phase

The second session has been designed for nontechnical users and the main aim of this session has been to enable the users so that they can utilise the encryption software named "7Zip". In the time of using this software, there has been a password that can protect these encrypted files and these have been shared among the communicating parties. This is a new process and the instructor has expected a greater number of users to be unaware of this software. The first part task was designed to get the skills and knowledge needed to use the software to find email.

The next session has been designed to take a review of this problem covered in its first sessions. Classification principles of the information, the cause of encrypting the electronic information and the utilisation of the 7zip software for the process of encryption. It has been planned as a discussion that is instructor-led involving all employees.

Third phase

The next phase has been considered as delivering the training and it was seen as the intervention of action research. This phase has been included in the delivery process of the learning task in the environment of learning [10]. The IS security model of the company was changed from the document of MS Word to the HTML document. An abstract has been added at the start of each manual section.

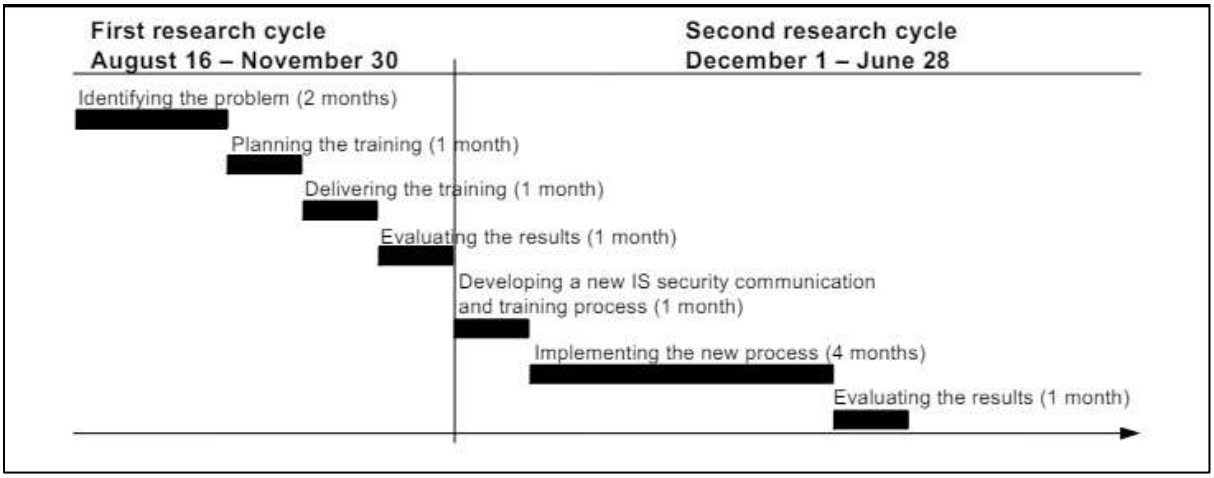

Figure 2: Research Timeline

Source: [10]

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

Fourth Phase

The fourth part of this research has evaluated the training results and it has been included in the fourth part of the UCIT. All the users were interviewed a minimum of two times following group interviews and personal interviews. Overall, the outcomes of this research cycle have been positive and the manager of IS security has been positive regarding the training. In this result, more than 9 people have claimed that this programme has made them assess the consequences of giving the unencrypted email.

The second cycle of research at the SC

The cycle has focused on testing the impact of the intervention built on the theory of UCIT and ELM. The second part of the cycle has focused on refining this intervention by implementing an IS security process to communicate. This cycle has some phases such as enhancing the new process of IS security training and communication.

Result	Method
New solutions of encryption to mitigate the technical problems	Interviews
Developed the usability of the policy of e-mail	Interviews
Enhanced consciousness of the probable consequences	Interviews
Enhance the utilisation of e-mail	Interviews
Increase in the utilisation of encrypted e-mail	Observation

Table 1: Result summary

This paper has discussed the enhancement of the IS policy regarding the security training programme. The enhancement of this training is based on the theories of ELM and UCIT. This has been refined and tested at the software organisation through the intervention of action research. The first section of this supported the theories of UCIT and ELM. The second part focused on the refinement of theory by expanding the training programme of IS security.

Conclusion

Workers who cannot be related to proper security policies which are effective for serious risks in their companies, use effective models to enhance this policy. Different types of IS security policy define advanced approaches which are effective for ranking from campaigns and sanctions to providing education and training. Different approaches of education and

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

training are provided effective approaches in this article. This article focuses on the training approaches of IS security and

education which follow anecdotal and atheoretical an.In order to find out deficiencies in the policy of IS security research, this article created a theory-oriented training program which provides effective IS security training. This effective training program is dependent on the global constructive instructional theory which is effective for the model. This article tested training and practical experience which is given through the training program. This is the innovative approach of the research section of this article.

Reference List

[1] Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, p.102267.

[2] Alkhazi, B., Alshaikh, M., Alkhezi, S. and Labbaci, H., 2022. Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. *IEEE access*, *10*, pp.132132-132143.

[3] Alassaf, M. and Alkhalifah, A., 2021. Exploring the influence of direct and indirect factors on information security policy compliance: a systematic literature review. *IEEE Access*, *9*, pp.162687-162705.

[4] Hwang, I., Wakefield, R., Kim, S. and Kim, T., 2021. Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), pp.345-356.

[5] Ali, R.F., Dominic, P. and Karunakaran, P.K., 2020. Information security policy and compliance in oil and gas organizations—A pilot study. *Solid State Technol*, *63*(1s), pp.1275-1282.

[6] Onumo, A., Ullah-Awan, I. and Cullen, A., 2021. Assessing the moderating effect of security technologies on employees' compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems (TMIS)*, *12*(2), pp.1-29.

[7]Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, pp.85701-85719.

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

[8]Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, pp.85701-85719.

[9]Wu, H., Han, H., Wang, X. and Sun, S., 2020. Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, pp.153826-153848.

[10]AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F. and Choo, K.K.R., 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, p.102754.

[11]Wilhelm, S., Förster, R. and Zimmermann, A. (2019). Implementing Competence Orientation: Towards Constructively Aligned Education for Sustainable Development in University-Level Teaching-And-Learning. Sustainability, 11(7), p.1891.

[12] Kanungo, Satyanarayan. "Cross-Border Data Governance and Privacy Laws." International Journal of Open Publication and Exploration (IJOPE), vol. 11, no. 1, January-June 2023, pp. 44-46. Available online at: https://ijope.com

[13] Kanungo, Satyanarayan. "Security Challenges and Solutions in Multi-Cloud Environments." Stochastic Modelling and Computational Sciences, vol. 3, no. 2 (I), July - December 2023, p. 139. Roman Science Publications. ISSN: 2752-3829.https://romanpub.com/resources/smc-v3-2-i-2023-14.pdf

[14] Kanungo, Satyanarayan. "Blockchain-Based Approaches for Enhancing Trust and Security in Cloud Environments." International Journal of Applied Engineering & Technology, vol. 5, no. 4, December 2023, pp. 2104-2111.

[15]Kanungo, Satyanarayan. "Edge Computing: Enhancing Performance and Efficiency in IoT Applications." International Journal on Recent and Innovation Trends in Computing and Communication 10, no. 12 (December 2022): 242. Available at: http://www.ijritcc.org

[16] Kanungo, Satyanarayan. "Hybrid Cloud Integration: Best Practices and Use Cases." International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 9, no. 5, May 2021, pp. 62-70. Available at: http://www.ijritcc.org

[17] Kanungo, Satyanarayan. "Decoding AI: Transparent Models for Understandable Decision-Making." Tuijin Jishu/Journal of Propulsion Technology 41, no. 4 (2020): 54-61.

[18] Kanungo, Satyanarayan, and Pradeep Kumar. "Machine Learning Fraud Detection System in the Financial Section." Webology, vol. 16, no. 2, 2019, p. 490-497. Available at: http://www.webology.org

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

[19] Kaur, Jagbir. "Streaming Data Analytics: Challenges and Opportunities." International Journal of Applied Engineering & Technology, vol. 5, no. S4, July-August 2023, pp. 10-16.https://romanpub.com/resources/ijaetv5-s4-july-aug-2023-2.pdf

[20] Kaur, Jagbir, et al. "AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization." Tuijin Jishu/Journal of Propulsion Technology 40, no. 4 (2019): 50. (Google scholar indexed)

[21] Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service . (2019). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98

[22] Ashok Choppadandi, Jagbir Kaur, Pradeep Kumar Chenchala, Akshay Agarwal, Varun Nakra, Pandi Kirupa Gopalakrishna Pandian, 2021. "Anomaly Detection in Cybersecurity: Leveraging Machine Learning Algorithms" ESP Journal of Engineering & Technology Advancements 1(2): 34-41.

[23] Ashok Choppadandi et al, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.12, December- 2020, pg. 103-112. (Google scholar indexed)

[24] AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

[25] Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. (2020). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127

[26] Rahman, Md. Rezowanur, Diponkor Kumar Shill, Uttom Kumar, A.S.M. Monjur Al Hossain, Sitesh Chandra Bachar, and Abu Shara Shamsur Rouf. "Formulation and Evaluation of Ledipasvir Nano-suspension Through QbD Approach." Journal of Pharmaceutical Technology 19, no. 3 (2023): 127-135.

[27] Chintala, S. (2023). Improving Healthcare Accessibility with AI-Enabled Telemedicine Solutions. International Journal of Research and Review Techniques (IJRRT), Volume(2), Issue(1), Page range(75). Retrieved from https://ijrrt.com

[28]Chintala, S. (2022). Data Privacy and Security Challenges in AI-Driven Healthcare Systems in India. Journal of Data Acquisition and Processing, 37(5), 2769-2778. https://sjcjycl.cn/18. DOI: 10.5281/zenodo.7766

[29]Chintala, S. K., et al. (2022). AI in public health: Modeling disease spread and management strategies. NeuroQuantology, 20(8), 10830-10838. doi:10.48047/nq.2022.20.8.nq221111

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

[30]Chintala, S. (2022). Data Privacy and Security Challenges in AI-Driven Healthcare Systems in India. Journal of Data Acquisition and Processing, 37(5), 2769-2778. https://sjcjycl.cn/DOI: 10.5281/zenodo.7766

[31]Chintala, S. K., et al. (2021). Explore the impact of emerging technologies such as AI, machine learning, and blockchain on transforming retail marketing strategies. Webology, 18(1), 2361-2375.http://www.webology.org

[32]Chintala, S. K., et al. (2022). AI in public health: Modeling disease spread and management strategies. NeuroQuantology, 20(8), 10830-10838. doi:10.48047/nq.2022.20.8.nq221111

[33] Sathish Kumar Chintala. (2023). Evaluating the Impact of AI on Mental Health Assessments and Therapies. Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal, 7(2), 120–128. Retrieved from https://eduzonejournal.com/index.php/eiprmj/article/view/488

[34] Chintala, S. (2022). AI in Personalized Medicine: Tailoring Treatment Based on Genetic Information. Community Practitioner, 21(1), 141-149. ISSN 1462-2815.www.commprac.com

[35] Machine Learning Algorithms and Predictive Task Allocation in Software Project Management". (2023). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 11(1), 34-43. https://ijope.com/index.php/home/article/view/107

Chintala, S. (2023). AI-Driven Personalised Treatment Plans: The Future of Precision Medicine. Machine Intelligence Research, 17(02), 9718-9728. ISSN: 2153-182X, E-ISSN: 2153-1838.

[36] Chintala, S. (2019). IoT and Cloud Computing: Enhancing Connectivity. International Journal of New Media Studies (IJNMS), 6(1), 18-25. ISSN: 2394-4331. https://ijnms.com/index.php/ijnms/article/view/208/172

[37] Chintala, S. (2018). Evaluating the Impact of AI on Mental Health Assessments and Therapies. EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), 7(2), 120-128. ISSN: 2319-5045. Available online at: www.eduzonejournal.com

[38] Sathishkumar Chintala. (2021). Evaluating the Impact of AI and ML on Diagnostic Accuracy in Radiology. Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal, 10(1), 68–75. Retrieved from https://eduzonejournal.com/index.php/eiprmj/article/view/502

ISSN:0975-3583,0976-2833 VOL14, ISSUE11,2023

[39] Chintala, S. (2023). Artificial Intelligence-Based Device for Managing Patient Privacy and Data Security. Patent No. 6335758. Retrieved from https://www.registered-design.service.gov.uk/find/6335758/

[40] Tilala, Mitul, Saigurudatta Pamulaparthyvenkata, Abhip Dilip Chawda, and Abhishek Pandurang Benke. "Explore the Technologies and Architectures Enabling Real-Time Data Processing within Healthcare Data Lakes, and How They Facilitate Immediate Clinical Decision-Making and Patient Care Interventions." European Chemical Bulletin 11, no. 12 (2022): 4537-4542. https://doi.org/10.53555/ecb/2022.11.12.425.

[41] Mitul Tilala. (2024). Real-Time Data Processing in Healthcare: Architectures and Applications for Immediate Clinical Insights. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 1119–1125. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10629

[42] Tilala, Mitul, and Abhip Dilip Chawda. "Evaluation of Compliance Requirements for Annual Reports in Pharmaceutical Industries." NeuroQuantology 18, no. 11 (November 2020): 138-145. https://doi.org/10.48047/nq.2020.18.11.NQ20244.

[43] Dodda, Suresh, Navin Kamuni, Venkata Sai Mahesh Vuppalapati, Jyothi Swaroop Arlagadda Narasimharaju, and Preetham Vemasani. "AI-driven Personalized Recommendations: Algorithms and Evaluation." Propulsion Tech Journal 44, no. 6 (December1,2023).https://propulsiontechjournal.com/index.php/journal/article/view/5587.

[44] Kamuni, Navin, Suresh Dodda, Venkata Sai Mahesh Vuppalapati, Jyothi Swaroop Arlagadda, and Preetham Vemasani. "Advancements in Reinforcement Learning Techniques for Robotics." Journal of Basic Science and Engineering 19, no. 1 (2022): 101-111. ISSN: 1005-0930.

[45]Dodda, Suresh, Navin Kamuni, Jyothi Swaroop Arlagadda, Venkata Sai Mahesh Vuppalapati, and Preetham Vemasani. "A Survey of Deep Learning Approaches for Natural Language Processing Tasks." International Journal on Recent and Innovation Trends in Computing and Communication 9, no. 12 (December 2021): 27-36. ISSN: 2321-8169. http://www.ijritcc.org.

[46] Mitul Tilala. (2023). Real-Time Data Processing in Healthcare: Architectures and Applications for Immediate Clinical Insights. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 1119–1125. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10629