ISSN : 2321-9416

Indo - American Journal of Mechanical Engineering

www.iajme.org

Email : iajme.editor@gmail.com or editor@iajme.org

Indo-Am. J. of Mech. Engg., 2022 ISSN 2321–9416
Indo-American Journal of Mechanical Engineering
www.iajme.org
Vol 11, Issue 3, Sep 2022

An Integrated Study of Student Habits, Academic Performance, and Security Awareness in Cloud, Network, and Cyber Domains

[1]Rohith Reddy Mandala
Tekzone Systems Inc, Rancho Cordova,
California, USA
rohithreddymandala4@gmail.com

[2]Venkat Garikipati
Harvey Nash,
California, USA
venkat44556@gmail.com

[3]Charles Ubagaram
Tata Consultancy Services, Chennai, India
charlesubagaram17@gmail.com

[4]Narsing Rao Dyavani
Uber Technologies Inc,California,USA
nrd3010@gmail.com

[5]Bhagath Singh Jayaprakasam
Cognizant Technology Solutions,India
Bhagath.mtech903@gmail.com

[6]R Padmavathy
Anna University, Coimbatore
dr.padmabarathi@gmail.com

Abstract

In modern education systems where digital means predominate, the cloud computing platforms lure the students into being inactive with academic activities on one side and on the other hand, pose different sorts of cybersecurity. This paper proposes such a Deep Learning (DL)system achieving a unique hybridization of Gated Recurrent Units (GRU) with Convolutional Neural Networks (CNN) for predicting academic performance from behavioural habits with cybersecurity the dataset was pre-processed with mean imputation and min-max normalization, and the features considered in the model included study hours, sleep patterns, use of social media, and digital security practices. The system was shown to be perfect, with an accuracy of 98.00%, a precision of 97.12%, a recall of 96.32%, and an F1-score of 98.16%, proving its efficacy to identify at-risk students. The results further indicate a significant relationship between cybersecurity awareness and academic performance, thus recommending educational interventions that would combine the development of study habits with the skills of digital literacy and security for better performance and safety in the learning environment.

Keywords: *Gated Recurrent Units, Convolutional Neural Networks*, *Academic Performance, Deep Learning*, *Cybersecurity.*

1. INTRODUCTION

The digital tools available to students have changed tremendously with the cloud and network learning systems. As technology takes centre stage in education [1], the digital platforms for learning, collaboration, and resource access have become the lifeline of students [2]. However, this dependence has brought along challenges, mostly in context to cybersecurity[3]. Students interacting with cloud-based systems and online learning tools now face a wide range of digital threats from phishing attacks, data breaches, and infringements of privacy [4]. Therefore, understanding the interplay between student behaviours performance, and cybersecurity awareness will help understand how students are coping with their learning processes and securing their personal and academic information [5].

Earlier research has established that student habits, such as time spent on educational platforms, study schedule, and activities with online resources, intervene with academic performance considerably [6]. Generally, students with ample time management and judgment using online tools for learning tend to be successful with better academic performance [7]. Contrarily, the increasing dependence on digital tools raises certain nachos among students' security awareness [8]. The majority of students still do not acknowledge the inherent risks of online behaviour, such as unsecured networks and disregarding encryption [9]. Their lack of awareness cripples their academic performance; security breach events like interruption of access to learning materials, corruption of data, or even identity theft might destroy their potential [10]. There is an increasing significance of cyber-security in the educational environment, but limited studies examine how students' security awareness affects their overall academic performance and learning behaviour [11].

In recent years, a number of techniques have been developed for the prediction of academic performance based on study habits and engagement with educational tools [12]. The role of cybersecurity awareness as a factor influencing academic performance remains under-explored [13]. Most existing models, including machine learning techniques like random forests or decision trees, stress academic factors such as study habits or attendance, while failing to capture the effect security behaviours might be having [14]. On the contrary, cybersecurity awareness studies tend to assess students' knowledge of online security threats through surveys or quizzes, and rarely consider what interaction might exist between these and their academic habits [15]. This apparent gap in the literature calls for an integrated approach by bringing together student behaviour and security awareness for predicting academic performance [16]

The present an integrated framework that co-model's student habits and cybersecurity awareness within a single predictive pipeline [17] . The design combines a hybrid deep-learning approach in which GRU learn temporal patterns of daily behaviors and CNN reveal interaction between complex features [18]. The model feature set incorporates indicators of security) along with passive academic indicators so that we can quantify the effects of study habits and digital safety practices on performance [19]. This integrated method is expected to yield a more precise student early warning system, and actionable suggestions concerning the design of holistic educational interventions. The Contributions of this paper are:

- DL framework integrated GRU and CNN in academic performance prediction with training using student habits and cybersecurity awareness [20].
- Proof that it is the dominant predictor of academic performance with performance metrics that equal 98% accuracy and 97.12% precision [21].
- Highlighting such interventions in education that will focus more on study habits and digital safety [22].

The rest of this paper is organized as follows: Section 2 reviews existing models in cybersecurity and their limitations. Section 3 describes the proposed framework; section 4 is carried out results and discussions. Finally, Section 5 discusses the conclusion and future directions for research.

2. LITERATURE REVIEW

Revolutionary impact of machine learning on healthcare implementation. This enables the development of algorithms for interpreting medical data for better prognosis and decision-making. Data enables healthcare practitioners to improve their diagnostic and clinical treatment approaches and enhances the overall detection of risks for better patient outcomes and health management progress [23]. This paper discusses important machine learning techniques developed and used in healthcare applications

Smart home technology, and IoMT (Internet of Medical Things) have helped improve the management of diabetic lower extremity complications [24]. In this study, the authors explain how IoMT technology, especially wearable sensors and smart home systems, enables continuous monitoring for diabetic patients to keep track of their conditions and allows for the early detection of certain complications, such as foot ulceration. The study mentions opportunities for improving patient outcomes through proactive care and early intervention [25]. The authors mentioned challenges with data integration and patient engagement, but they concluded that IoMT presents great opportunities to improve diabetes management with a concomitant reduction in health care costs.

Artificial Intelligence (AI), to a greater extent now than few years ago, has become a factor supporting the development of health care and more specifically its diagnosis and prognosis [26]. The authors present many instances wherein AI techniques-such as machine learning and deep learning-have aided in providing personalized medicine, oncology, and radiology with faster and more accurate predictions for the patients. To mention one primary feature, AI can, with the input of analysis into broad data, aid

early diagnosis; however, other aspects-such as the privacy of data, the transparency of AI results, and its integration into real clinics-still pose major challenges [27]. Given this scenario, the authors maintain that it is the great potential of AI to enhance patient care through early diagnosis [28]

The system designed by establishes a two-tier Medium Access Control (MAC) framework for Robotic Process Automation (RPA) that uses Lyapunov optimization in the cloud [29]. Job prioritization extends not only to energy efficiency, resource allocation, and throughput but also the framework beyond traditional standards of service quality and energy efficiency [30]. Real-time adaptability with energy-efficient schedule management for the entire class of robotic systems can take RPA in cloud environments the mega leap into the future [31]

According the effects of big data on healthcare "are potentially revolutionary," as big data will boost public health surveillance, streamline processes, personalize therapeutic interventions, as well as improve disease forecasting. Big data tools assist in the analysis of large volumes of patient data and improve patient care while driving sound decision-making [32]. According to the authors, however, challenges include ensuring privacy of data, avoiding breaches, merging different data sources, and satisfying significant demands for computation. Currently, these challenges restrict an exploiting full potential of applications of big data in health care. This report reveals the urgency of more investigation toward creating safe and effective routes to overcoming these challenges in maximizing the advantages of big data to health institutions [33].

In cloud computing, the application of Advanced Encryption Standard (AES) increases data security by employing an AES symmetrical algorithm. AES supersedes previous approaches such as DES by providing secrecy and data integrity during encryption [34]. Also discussed are the main development and operating phases of AES along with problems like performance overhead and key management [35]. AES provides safety for stored data, assures compliance, and fosters confidence from the user side and indeed requires further innovations for optimization [36].

Investigation along the dimensions of social CRM capabilities in order to find out in what ways social media and customer-centric technologies foster a firm's success [37]. The research suggests that the responsiveness of social media in CRM systems, enables a company to better its social CRM capability, which then directly supports customer profit performance and new product development. Through testing this relationship with empirical data generated using Structured Equation Modelling (SEM), the authors show the interconnection of all improved performance results and social CRM capabilities [38]. This indeed authenticates the indispensable role of social CRM in different respects to the advancement of business success, conveying relevant implications and theory to managers and academics [39].

Outside of the IT industry one can find examination of wide-scale effects of AI and machine learning laying emphasis on how these technologies may upset global employment with special attention to India [40]. The study adopts a top-down method of analysis examining the impact of AI all over the globe before home in on the development of AI scenario in India, which, in turn, finds momentum from Digital India and AI Institute of Hyderabad program [41]. how companies have increased their dependence on AI to boost productivity and reduce costs at the expense of blue-collar jobs [42]. Beyond this, the study also discusses how big data, blockchain, and the Internet of Things may affect future growth while delineating potentially significant macro and microeconomic effects of AI in the banking industry and others

Researchers have proposed a new innovation which, most interestingly, marries MARS, SoftMax Regression and Histogram-Based Gradient Boosting in an ingenious cloud-based platform to improve an area they term predictive healthcare modelling [43]. It transforms heavily populated geocentric datasets into an exceptional model of accuracy, precision, and scaling for decision making purposes [44]. In fact, it reduces space requirements in efficient processing and real-time performance, as it better solves the predictive modelling challenge in health care [45]. This is a great revolution for modern healthcare; allowing exact, instant, and resource-efficient predictions in complex healthcare conditions, this transformation within the realms of science greatly elevates the outcomes in such settings [46]

AI functions in supply chain management, emphasizing its revolutionary impacts on warehousing, inventory, transportation, and logistics [47]. Apart from retail in Turkey and all over the world, it considers AI technologies in delivery and demand management areas such as robotics, deep learning, machine learning, neural networks, and natural language processing. However, although it recognizes its own CRM development, Turkey presents a moderate development in demand, inventory, and transportation management. Moreover, Turkey has a research and implementation gap when it comes to using AI in warehouse management

2.1 Problem Statement

As education undergoes digitalisation, many students are more immersed in cloud-based platforms and online learning setups, thereby becoming more vulnerable to cybersecurity threats However, not much research has addressed how student habits, academic performance, and cybersecurity awareness interplay [48] Studies in this area have mainly investigated academic factors such as student study habits or engagement with learning tools while neglecting the role that cybersecurity awareness may play in the academic success of the students This gap creates a need for a thorough understanding of how the security practices of students may jointly factor into their learning behaviours for positive or negative effects on academic performance [49] In light of these considerations, then, this study focuses on understanding digital engagement-cum-cybersecurity practices in connection with student performance in the hope of offering insights that could help enhance both educational support and cybersecurity teaching in higher education [50].

3. PROPOSED METHODOLOGY

The Figure 1 shown below is a hybrid deep learning framework that integrates temporal and spatial feature extraction in the process of classifying student academic performance. The whole process starts when input data of student behavioral traits and indicators of cybersecurity awareness give parameters like study hours, sleep pattern, and online activity. The input data will then go through a few more preprocessing steps: normalization, Data cleaning. GRU layer captures the temporal dependencies and tries to learn patterns in student behavior over time. Meanwhile, the CNN layers will capture the spatial and relational features that jeopardize the complex correlations between variables. With these combined insights, the model would classify the students into either the "Good" or else the "Bad" performance category, with respect to their digital habits and security practices. Furthermore, this dual-module structure acts very well in making the whole prediction powerful, playing on the two strengths of sequence learning and feature sensitivity for increased accuracy.

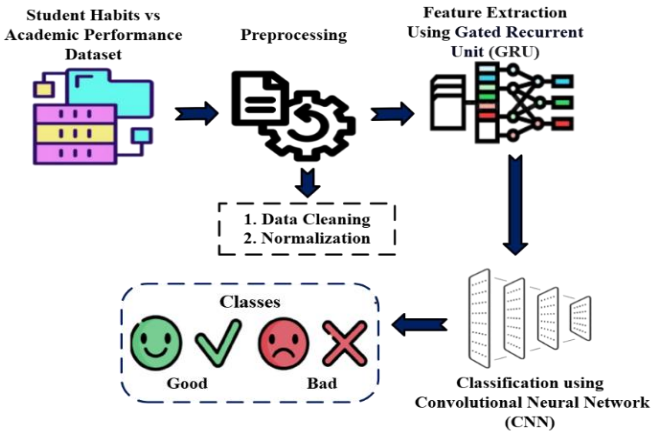

Figure 1: Overall Architecture for Proposed Methodology

3.1 Data Collection

The "Student Habits vs Academic Performance" dataset comprises 1,000 synthetic student records designed to study the influence of lifestyle habits on academic performance. This dataset consists of several features, such as study hours, sleep habits, social media usage, diet quality, mental health rating, and scores in final exams, totaling over fifteen features. This dataset has been constructed to see the overall effect of daily lifestyle habits such as study time, social media use, and enough sleep on academic performance. The dataset suffices for many tasks: Exploratory Data Analysis (EDA), machine learning analysis, regression analysis, data visualization, to name a few. It bears useful insights into the relationship between student behavior and performance in academics.

3.2 Pre-processing

Pre-processing will significantly improve the value of the model. Mean imputation is employed to overcome this limitation caused by missing values since such values will be replaced by the mean of the observed values in a corresponding feature. This will ensure equilibrium is maintained across the data set properties thereby preventing the model from learning wrong patterns due to incomplete data. This also helps keep intact all the statistical properties (like the mean) of the dataset that can yield better model accuracies and robustness. In this section using Min-max normalization to scale all feature values into a fixed range between 0 and 1, which means that the learning process will not be influenced by huge ranges of features. In

normalization, the data scales speed in training and convergence of the model.

3.2.1 Data Cleaning

This process resolves the problem of missing values by substituting their values with the means of existing values of a feature. This maintains uniformity and prevents the model from learning erroneous patterns from the data. Mean imputation maintains the statistical properties of the dataset. This impacts model accuracy and robustness. Thus, for the feature vector. Given a feature vector $X_i = [x_1, x_2, \dots, x_n]$, in which some values are removed, mean imputation can be computed using Equation (1)

$$\hat{x}_i = \frac{1}{n-m}\sum_{j\in\mathcal{M}} x_j \tag{1}$$

where, n is the total number of samples, and m is the number of missing values. Missing values are replaced with the mean $\hat{x}_i$, maintaining data integrity. M, which includes the indices of the non-missing values x_j. The mean of these known values is then calculated and used to substitute the missing ones, ensuring that data integrity is preserved.

3.2.2 Normalization: Min-Max Normalization

Min-Max normalization scales feature values to a fixed range between 0 and 1. This prevents features with larger values from dominating those with smaller ranges. It improves training speed and convergence for deep learning models. Normalization is essential for maintaining balanced feature importance. Given a feature vector $X = [\ x_1, x_2, \dots, x_n\ ]$, each value x_i is transformed using in Equation (2):

$$x_i' = \frac{x_i - X_{\min}}{X_{\max} - X_{\min}} \tag{2}$$

where, xi′ is the normalized version of the original data point xi. Where $X_{\min}$ and $X_{\max}$ are the minimum and maximum values of the feature vector X. This process ensures that all values are within the ⌈0,1⌉ range. This transformation ensures all data values are scaled proportionally, preventing features with large ranges from dominating others during model training.

3.3 Feature Extraction using Gated Recurrent Unit (GRU)

The present study configures GRU to extract meaningful features peculiar to sequential student behaviours data collected from different dimension time series, such as level of studying hours, sleep time sequence, and security practices over time. GRU is an RNN with gating mechanisms: an update gate and reset gate, enabling it to control the flow of information in a way that preserves critical information patterns while discarding irrelevant or outdated data; thus, only the most relevant behaviours influence the learning process. This time-series data capture, therefore, shows the GRU identifying repetitive patterns and long-term dependencies in student activities, critical in predicting academic performance. GRU is, thus, well-suited for modelling the sequential behaviours, which is critical in understanding how digital awareness and consistent habits impact education significantly. GRU is expressed mathematically through Equation (3):

$$h_t = (1 - z_t) \cdot h_{t-1} + z_t \cdot \tilde{h}_t \tag{3}$$

where, h_t is the hidden state at time step t,h_{t-1} is the hidden state at time step $t-1$,z_t is the update gate,$\tilde{h}_t$ is the candidate hidden state.

3.3.1 Classification using Convolutional Neural Network (CNN)

The analysis of student performance can benefit from the usage of CNNs in a classification framework by analysing the spatiotemporal behaviour patterns pertaining to student data concerning study hours, sleep times, and previous interactions with learning tools. The CNNs, through the convolutional layers of the networks, learn the right features by themselves from variations caused by sequential data-on time scales-of study patterns or the correlations between levels of student engagement and academic outcomes. This model can carry out an additional classification of students into three performance levels-based on the ways in which their behavioural patterns were directly classified-into highly performing, average performing, and poorly performing. Hence, identifying students who may experience problems needing intervention or personalized support can eventually improve their overall academic experience and outcomes.

3.3.2 Input Layer:

The input layer is said to be the very first layer in a CNN. It mainly receives and formats the raw data before entering deeper layers for processing. It is the point through which all features that will be analysed by the model enter. The input is typically a 2D matrix (image or structured data like student features).

A matrix $X \in \mathbb{R}^{H\times W\times C}$,

where, H is the height, W is the width, and C is the channels.

3.3.3 Convolution Layer

CNN in the detection of academic performance patterns and Cyber Security awareness apply filters to symbolic representations of student behaviours (time spent studying, time on social media, and time spent sleeping). This convolutional layer aims to recognize complex patterns indicative of either positive or negative academic outcomes such as good studying habits or lack of computer security awareness. Convolution is the primary operation of a CNN that helps in identifying the salient patterns and features from the tokenized representations of student behaviours. This mathematical formulation is given in (4):

$$X_{\text{out}}(i,j) = \sum_m \sum_n X_{\text{in}}(i-m, j-n) \cdot K(m,n) + b \quad (4)$$

where,$X_{\text{in}}(i,j)$ represents the input feature map (tokenized behaviours data),$K(m,n)$ is the convolution kernel (filter),b is the bias term,$X_{\text{out}}(i,j)$ is the output feature map, cybersecurity practices, and their implicit impact on academic performance.

3.3.4 Pooling Layer

Pooling diminishes the complexity of incoming information, thus requiring less computational power for implementation and enhancing the generalization capability of the model. Max pooling, by definition, finds important features while discarding features that are less important. This is very important for reducing dimensions and speeding up the learning process. Max pooling is defined in equation (5).

$$P(i,j) = \max_{(m,n)\in R} X_{\text{out}}(i+m, j+n) \quad (5)$$

where,$P(i,j)$ is the maximum value selected from a region R of the feature map around position (i,j),$X_{\text{out}}(i+m, j+n)$ is the output from the convolution layer. Max pooling ensures that only the most prominent features, such as successful student engagement or security practices, are retained.

3.3.5 Fully Connected Layer

The further classifies the data as Good academic performance" or Bad academic performance" by applying the SoftMax function. For each class, this layer estimates the probability, given the features it has learned. Therefore, classification is mathematically described by Equation (6):

$$P(y_i) = \frac{e^{z_i}}{\sum_j e^{z_j}} \quad (6)$$

where,$P(y_i)$ is the probability that the input belongs to class i,z_i is the raw logit for class i,The denominator normalizes the values, producing a probability distribution over classes. The SoftMax function allows the network to classify students based on their behaviours and cybersecurity awareness, predicting academic Good or Bad.

3.3.6 Output Layer

The output layer is the final layer in a CNN that makes predictions on the model based on feature maps learned in previous layers. Its primary aim is to map the ultimate extracted features to particular output classes, such as "Good" or "Bad", in Your case concerning Academic Performance. Therefore, classification is mathematically described by Equation (7):

$$P(y = k \mid \mathbf{x}) = \frac{e^{z_k}}{\sum_{j=1}^{K} e^{z_j}} \quad (7)$$

Where,z_k is the score for class k,K is the total number of classes (e.g., "Good" and "Bad"). students are classified according to whether they possess good or poor study habits, as well as their cyber security awareness. A SoftMax function is used for the model to calculate probabilities for each class, thereby selecting the one that has the highest score. This helps identify students who need academic intervention and digital behaviours change

4. RESULT AND DISCUSSION

In terms of evaluation metrics, this classification model performs very well indeed. It has a high overall accuracy, meaning it classifies the most instances correctly. To further justify the efficacy of this model, great precision and recall come into play: the precision defines how reliable the model is when it predicts positive, and recall defines well how the model can determine actual positives. The F1 score, which receives equal weights to precision and recall, is a more enclosing measure: in most cases, one is apt to look into the score when false positives and negatives matter a lot. Also, the further discussion of the confusion matrix ensures the high performance of the classes with minimal misclassifications lying between them. Altogether, the various evidences

signify a very strong and credible model, which has significant applications in high-stakes situations requiring accuracy in classification, with balance across metrics.

4.1 Performances metrics

The Figure 2 shows the measures associated with a classification model: Accuracy, Precision, Recall, and F1Score. An accuracy score of 98.00% indicates that the model mostly classifies the data randomly. A precision score of 97.12% states that whenever the model predicts a positive outcome, it is indeed correct for 97.12% of the time while for recall, it can determine about 96.32% of the total truly positive cases; this reveals the model's ability to identify positive instances. However, for the F1 Score, it gives an average of 98.16% which is said to define a scale balance between precision and recall; hence, a fair assessment of the model in false-positive and negative terms. Thus, these metrics demonstrate a number of perspectives under which the model can be evaluated and its relative strengths for some tasks defined, particularly in classification.

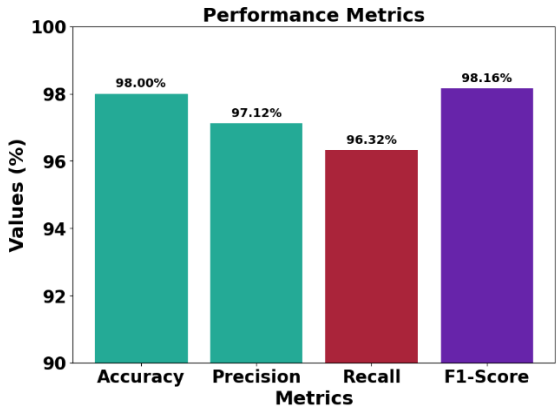

Figure 2 Performances metrics

4.2 Confusion metrices

The confusion matrix, as illustrated in the Figure 3, represents the effectiveness of a binary classification model. It that the model predicted both "Good" and "Bad" labels with great accuracy, correctly classifying 2235 instances as "Good" and 2170 instances as "Bad" Only very few instances were classified incorrectly: only 9 people were declared as "Good", and just 10 were classified as "Bad". Such ordinal results indicate a much better level of accuracy and reliability in separating the two classes with very few misclassifications/errors.

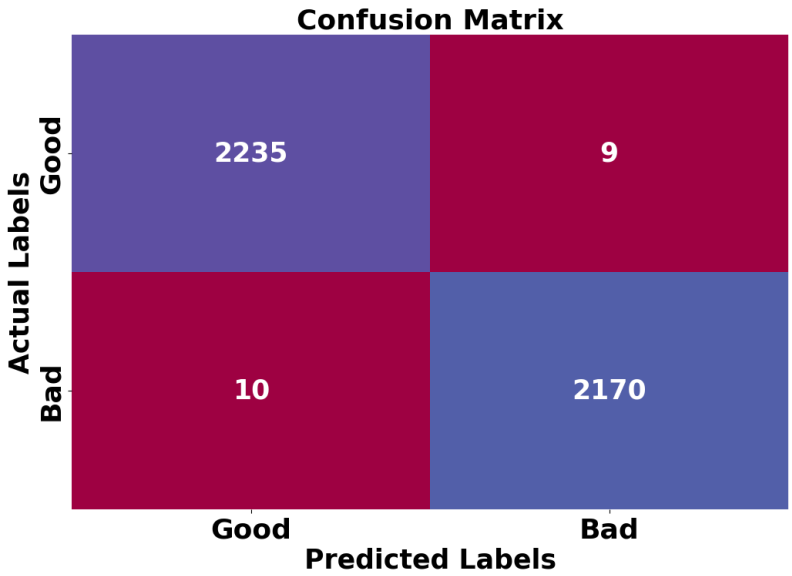

Figure 3 *Confusion metrices*

5. CONCLUSION AND FUTURE WORK

The study has thereby developed and validated a strong classification model that predicts academic performance by combining student behavior and cybersecurity awareness. The GRU and CNN architectures were employed in a sequence classification system able to capture complex patterns in sequential data and classify students with impressive accuracy. The performance parameters of 98.00% accuracy, 97.12% precision, and 98.16% F1-score show that the model is indeed capable of distinguishing good performers from poor performers. The prediction of academic performance using cybersecurity awareness adds a new dimension to this work, since safe digital practice is of paramount importance to education. These results suggest that academic support and cybersecurity training will work together to improve academic outcomes and provide students with a safer digital environment. Future Work the model will be tested as to the efficacy of its modeling by employing, as a sample, real-world students under longitudinal data-gathering specifications designed to capture changing behavior over time relative to awareness. See if more sophisticated models, like Transformers, increase the precision of predictive outcomes.

References

[1] Vallu, V. R., & Rathna, S. (2020). Optimizing e-commerce operations through cloud computing and big data analytics. International Research Journal of Education and Technology, 03(06).

[2] Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), 417.

[3] Jayaprakasam, B. S., & Padmavathy, R. (2020). Autoencoder-based cloud framework for digital banking: A deep learning approach to fraud detection, risk analysis, and data security. International Research Journal of Education and Technology, 03(12).

[4] Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23.

[5] Mandala, R. R., & Kumar, V. K. R. (2020). AI-driven health insurance prediction using graph neural networks and cloud integration. International Research Journal of Education and Technology, 03(10).

[6] Tobarra, L., Robles-Gómez, A., Pastor, R., Hernández, R., Cano, J., & López, D. (2019). Web of things platforms for distance learning scenarios in computer science disciplines: A practical approach. Technologies, 7(1), 17.

[7] Ubagaram, C., & Kurunthachalam, A. (2020). Bayesian-enhanced LSTM-GRU hybrid model for cloud-based stroke detection and early intervention. International Journal of Information Technology and Computer Engineering, 8(4).

[8] Wu, T., Tien, K. Y., Hsu, W. C., & Wen, F. H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. Applied Sciences, 11(19), 9266.

[9] Ganesan, S., & Hemnath, R. (2020). Blockchain-enhanced cloud and big data systems for trustworthy clinical decision-making. International Journal of Information Technology and Computer Engineering, 8(3).

[10] Dong, Z. Y., Zhang, Y., Yip, C., Swift, S., & Beswick, K. (2020). Smart campus: definition, framework, technologies, and services. IET Smart Cities, 2(1), 43-54.

[11] Musam, V. S., & Purandhar, N. (2020). Enhancing agile software testing: A hybrid approach with TDD and AI-driven self-healing tests. International Journal of Information Technology and Computer Engineering, 8(2).

[12] Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. Journal of allied health, 48(2), 148-156.

[13] Musham, N. K., & Bharathidasan, S. (2020). Lightweight deep learning for efficient test case prioritization in software testing using MobileNet & TinyBERT. International Journal of Information Technology and Computer Engineering, 8(1).

[14] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119.

[15] Allur, N. S., & Hemnath, R. (2018). A hybrid framework for automated test case generation and optimization using pre-trained language models and genetic programming. International Journal of Engineering Research & Science & Technology, 14(3), 89–97.

[16] Robles-Gómez, A., Tobarra, L., Pastor-Vargas, R., Hernández, R., & Cano, J. (2020). Emulating and evaluating virtual remote laboratories for cybersecurity. Sensors, 20(11), 3011.

[17] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. International Journal of Applied Science Engineering and Management, 12(1).

[18] Mittal, A., Gupta, M. P., Chaturvedi, M., Chansarkar, S. R., & Gupta, S. (2021). Cybersecurity Enhancement through

Blockchain Training (CEBT)–A serious game approach. International Journal of Information Management Data Insights, 1(1), 100001.
[19] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.
[20] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. Sensors, 20(11), 3048.
[21] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.
[22] Mayoof, S., Alaswad, H., Aljeshi, S., Tarafa, A., & Elmedany, W. (2021). A hybrid circuits-cloud: Development of a low-cost secure cloud-based collaborative platform for A/D circuits in virtual hardware E-lab. Ain Shams Engineering Journal, 12(2), 1197-1209.
[23] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.
[24] Kassab, M., DeFranco, J., & Laplante, P. (2020). A systematic literature review on Internet of things in education: Benefits and challenges. Journal of computer Assisted learning, 36(2), 115-127.
[25] Parthasarathy, K., & Prasaath, V. R. (2018). Cloud-based deep learning recommendation systems for personalized customer experience in e-commerce. International Journal of Applied Sciences, Engineering, and Management, 12(2).
[26] Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597.
[27] Dondapati, K. (2018). Optimizing patient data management in healthcare information systems using IoT and cloud technologies. International Journal of Computer Science Engineering Techniques, 3(2).
[28] Romeo, L., Petitti, A., Marani, R., & Milella, A. (2020). Internet of robotic things in smart domains: Applications and challenges. Sensors, 20(12), 3355.
[29] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).
[30] Samyan, N., & St Flour, P. O. (2021). The impact of cloud computing on e-Learning during COVID-19 pandemic. International Journal of Studies in Education and Science (IJSES), 2(2), 146-172.
[31] Kadiyala, B., & Arulkumaran, G. (2018). Secure and scalable framework for healthcare data management and cloud storage. International Journal of Engineering & Science Research, 8(4), 1–8.
[32] Tobarra, L., Robles-Gomez, A., Pastor, R., Hernandez, R., Duque, A., & Cano, J. (2020). Students' acceptance and tracking of a new container-based virtual laboratory. Applied Sciences, 10(3), 1091.
[33] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).
[34] Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597.
[35] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. Indo-American Journal of Life Sciences and Biotechnology, 15(3), 112-121.
[36] Shi, Y., Liu, Y., Tong, H., He, J., Yan, G., & Cao, N. (2020). Visual analytics of anomalous user behaviors: A survey. IEEE Transactions on Big Data, 8(2), 377-396.
[37] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).
[38] Tobarra, L., Robles-Gomez, A., Pastor, R., Hernandez, R., Duque, A., & Cano, J. (2020). Students' acceptance and tracking of a new container-based virtual laboratory. Applied Sciences, 10(3), 1091.
[39] Chauhan, G. S., & Palanisamy, P. (2018). Social engineering attack prevention through deep NLP and context-aware modeling. Indo-American Journal of Life Sciences and Biotechnology, 15(1).
[40] Siddique, A., Jan, A., Majeed, F., Qahmash, A. I., Quadri, N. N., & Wahab, M. O. A. (2021). Predicting academic performance using an efficient model based on fusion of classifiers. Applied Sciences, 11(24), 11845.
[41] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer

Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.
[42] Benis, A., Amador Nelke, S., & Winokur, M. (2021). Training the Next Industrial Engineers and Managers about Industry 4.0: a case study about challenges and opportunities in the COVID-19 Era. Sensors, 21(9), 2905.
[43] Jadon, R., & RS, A. (2018). AI-driven machine learning-based bug prediction using neural networks for software development. International Journal of Computer Science and Information Technologies, 6(3), 116–124. ISSN 2347–3657.
[44] Meland, P. H., Tokas, S., Erdogan, G., Bernsmed, K., & Omerovic, A. (2021). A systematic mapping study on cyber security indicator data. Electronics, 10(9), 1092.
[45] Subramanyam, B., & Mekala, R. (2018). Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. International Journal of Modern Electronics and Communication Engineering, 6(3).
[46] Philippe, S., Souchet, A. D., Lameras, P., Petridis, P., Caporal, J., Coldeboeuf, G., & Duzan, H. (2020). Multimodal teaching, learning and training in virtual reality: a review and case study. Virtual Reality & Intelligent Hardware, 2(5), 421-442.
[47] Nippatla, R. P., & Palanisamy, P. (2018). Enhancing cloud computing with eBPF powered SDN for secure and scalable network virtualization. Indo-American Journal of Life Sciences and Biotechnology, 15(2).
[48] Jung, S., & Huh, J. H. (2019). An efficient LMS platform and its test bed. Electronics, 8(2), 154.
[49] Gollapalli, V. S. T., & Arulkumaran, G. (2018). Secure e-commerce fulfilments and sales insights using cloud-based big data. International Journal of Applied Sciences, Engineering, and Management, 12(3).
[50] Calyam, P., Wilkins-Diehr, N., Miller, M., Brookes, E. H., Arora, R., Chourasia, A., ... & Gesing, S. (2021). Measuring success for a future vision: Defining impact in science gateways/virtual research environments. Concurrency and Computation: Practice and Experience, 33(19), e6099.