International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Integrating Cybersecurity Awareness into Human Resource Management: A Framework for Organizational Resilience

Ripunjay Kumar
Research Scholar
Jabalpur
ripunjaykumar.bgp@gmail.com

***Abstract*—In the age of the digital revolution, human resource technology (HRTech) has emerged as a critical enabler for organizations to automate hiring, onboarding, payroll, employee management, performance management, and workforce analytics. However, there are significant cybersecurity risks associated with the growing application of cloud computing, digital platforms, and data-driven decision-making in HRM. This research paper examines the cybersecurity awareness policy in human resources (HR) management, its effectiveness, issues, and solutions. This paper introduces a hybrid deep learning method to improve cybersecurity awareness in human resource management using the Cybersecurity Risks Dataset. The proposed Hybrid GRU+BiLSTM model effectively captures long- and short-term dependencies in sequential data and outperforms traditional models such as RNN, SVM and KNN. The results show the best classification performance, with 97% accuracy (acc), 97% precision (pre), 98% recall (rec), and 98% F1-score (F1), indicating high reliability in identifying cybersecurity risk. The findings highlight the model's potential for supporting proactive decision-making and bolstering organizational resilience by augmenting threat identification and awareness in HR systems.**

***Keywords*—Human Resource Management (HRM), Cybersecurity Workforce, Digital Transformation, Workforce Development, Strategic Recruitment.**

I. INTRODUCTION

The digital age is making it imperative that anyone involved in a business or organisation understand Cyber security in order to recover. As more and more businesses transition to digital technology, they become more vulnerable to the many cyber threats that can disrupt their operations and put crucial data at risk [1][2][3][4]. Implementing cybersecurity awareness within the organization, particularly in HRM processes, is crucial for safeguarding company resources and employee information, particularly in scenarios involving remote and hybrid work. Human Resource Management has evolved into a strategic role with substantial influence on the culture and security behaviour of an organisation [5][6]. HR efforts such as recruitment, training, policy development, and performance management can help increase awareness of cybersecurity at all levels [7]. Integrating cybersecurity into onboarding can help build a culture of security awareness, continuous learning, and employee assessment [8][9][10]. Structured offboarding processes, such as revoking access and securely transferring knowledge, also make organizational defense mechanisms stronger and lower the risk of insider threats [11].

Organizations have a hard time putting cybersecurity awareness into practice, even though it is becoming more and more important. Poor readiness and low capacity for change due to limited resources and ever-evolving threat landscapes can leave people behind [12][13][14]. The HR policies are not linked to its cybersecurity policies, leading to reduced operational efficiency in the organization [15][16]. It is essential for organizations to build comprehensive security solutions that capable of addressing future cyber threats stemming from the cloud, AI and Internet of Things (IoT) applications.

AI, ML, and DL [17] are powerful cybersecurity tools that aid in the defence against hostile elements. The systems employ these technologies to identify sophisticated attacks and detect abnormal patterns and then automatically react to both phishing attacks and suspicious user actions [18][19][20]. The more data an ML model is trained on, the more accurate its predictions, and DL techniques can better discern patterns in complex data sets [21][22]. AI technology adds to these challenges with the need for robust security protocols capable of countering evolving security threats, alongside the risk of algorithmic bias and data poisoning, along with potential AI-driven cyber-attacks. The use of ML and DL technology within HR-integrated cybersecurity systems enables organizations to build stronger security defences while protecting their digital operations[23].

Organizations face increasing cybersecurity threats because their Human Resource Management systems do not effectively handle cybersecurity awareness training. The existing cybersecurity gap creates two problems because employees display unprotected behaviour and the organization becomes less capable of handling new cyber threats. Organizations should make human-centric solutions their primary focus because cyber threats have increased both in frequency and in complexity[24]. The integration of cybersecurity awareness training into human resource management systems leads to improved employee behaviour and reduced security risks while establishing a strong organizational culture. The study was developed to address the existing problem which occurs when human resources activities do not align with cybersecurity protection methods. The study has several important contributions which researchers have listed below:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- The Cybersecurity Risks Dataset provides necessary data to develop cybersecurity threat models which enable organizations to predict impending threats while protecting their human resource management systems.
- Cleaned dataset by filling in missing values, deleting duplicates, and filtering out noise.
- Data cleaning is performed by handling missing values, removing outliers, and eliminating duplicate or noisy records to ensure data quality.
- Feature transformation techniques such as one-hot encoding and normalization using StandardScaler are applied to prepare the data for effective model training.
- Proposes a novel Hybrid GRU+BiLSTM DL model for improving cybersecurity awareness in human resource management.
- To ensure a thorough and reliable study, the model's performance was evaluated using a battery of measures, including REC, ACC, PRE, F1, and ROC-AUC.

This study can be justified by the fact that there is an increasing need to enhance cybersecurity awareness in human resource management systems since traditional methods in most cases are not effective in detecting complex and dynamic cyber threats. The originality of the work is reflected by the fact that the hybrid GRU+BiLSTM DL architecture is integrated, which is the only architectural that integrates advantages of both designs to learn long-term and short-term dependencies in the data of the cybersecurity domain. Further, the use of advanced processing techniques and comprehensive assessment criteria enhances the model's validity, and the proposed approach can be regarded as a robust and innovative approach to bolstering organizational resilience and anticipating risks.

The paper is organized as follows: Section II describes related work on the topic of cybersecurity awareness in HRM, Section III presents the dataset, the pre-processing techniques, and the model implementation. The experimental results are discussed and compared in Section IV, and future research directions are summarized in Section V.

II. LITERATURE REVIEW

A wide-ranging review and analysis of previous research is performed to support and reinforce the development of this study. A summary of recent studies is provided in Table I, where models, datasets, important findings, and problems are identified. This review gives a useful overview of the state of the art and areas of knowledge that need to be developed.

R. Kumar *et al.* (2025) proposed the idea of giving safety recommendations and guidelines about phishing. It means the phishing detection system based on NLP is very accurate (92%) when compared with other conventional phishing detection systems. These values prove the effectiveness of the system in both correctly identifying phishing attacks and reducing false positives [25]. Similarly, Jonathan *et al.* (2025) used a comparison of the ACC and efficiency levels of each of the algorithms. The results of the experiments show that the SVM model has the highest ACC of 0.910 and is able to detect depression [26]. Z. Zhao *et al.* (2024) pointed out that this method has a high recognition rate of up to 98% in the field of communication threat events and can effectively identify the attacks of port scanning, illegal host login, and denial of service, which can provide technical support for protecting the security of the power information communication system. [27].

Likewise, A. Setiyaji *et al.* (2024) investigate the code that is used to detect and avoid SQL injection threats. When evaluating the model, many CNN models and SVM approaches are used. The proposed CNN model surpassed competing ML algorithms with an impressive 91% ACC rate [28]. M. Mouiti *et al.* (2023) proposed different models to improve performance and enhance efficiency. The experimental results were analyzed and compared in terms of pre, acc, F1, AUC, and rec. The results were competitive compared with existing works, with an ACC of 99%[29].

In another study, P. Thantharate and A. T (2023) developed a Federated learning architecture designed to identify intrusions while protecting privacy. Comparative analyses on the Bot-IoT dataset show that a centralized deep neural network gets 81.4% ACC while Cybria's federated model achieves 89.6%. For cyber protection applications, the ~10% increase demonstrates the advantages of collaborative learning from decentralized data [30]. B. Strickson et al. (2023) revealed a task increase of +14.0 points in REC and +9.19 ML persons had considerably better F1 overall ($p < 0.01$), with respect to points in ACC. A significant improvement in user ratings (66.7%), as well as a notable rise for ML persons ($p < 0.01$), was found in the second trial, cyber situational awareness (CSA) [31].

Research Gap: Although there has been progress in the prediction of cybersecurity risks, current models are most likely to fail to adequately capture both short- and long-term relationships on complex data sets, resulting in low prediction ACC. Numerous conventional methods are also incapable of addressing data imbalance and preprocessing issues, which affect overall model performance. Hence, an effective hybrid model that improves prediction ACC and reliability in cybersecurity risk assessment is required.

TABLE I. RECENT STUDIES ON CYBERSECURITY AWARENESS USING MACHINE LEARNING TECHNIQUES

Authors & Year	Objective	Techniques Used	Dataset/Domain	Performance Metrics	Key Results
R. Kumar *et al.* (2025)	Phishing detection with safety advice	NLP-based model	Phishing detection	Accuracy	Achieved 92% accuracy, outperforming conventional models and reducing false positives
Jonathan *et al.* (2025)	Depression detection	Support Vector Machine (SVM)	Mental health detection	Accuracy	SVM achieved 0.910 accuracy, best among compared models

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Z. Zhao *et al.* (2024)	Communication threat detection	ML-based threat recognition system	Cybersecurity (network threats)	Recognition Rate	Achieved 98% recognition rate for detecting attacks like port scanning and DoS
A. Setiyaji *et al.* (2024)	SQL injection detection	CNN + Supervised ML	Web security	Accuracy	CNN achieved 91% accuracy, outperforming other ML models
M. Mouiti *et al.* (2023)	Performance enhancement of detection models	Multiple ML models	Cybersecurity	Accuracy, Precision, Recall, F1, AUC	Achieved 99% accuracy, competitive with existing works
P. Thantharate & A. T. (2023)	Privacy-preserving intrusion detection	Federated Learning	Bot-IoT dataset	Accuracy	Achieved 89.6% accuracy, outperforming centralized model (81.4%)
B. Strickson *et al.* (2023)	Cybersecurity learning & awareness improvement	Machine Learning-based approach	Cyber situational awareness	Recall, Precision, F1-score	Improved +14% recall, +9.19% precision, 66.7% user score improvement

III. Research Methodology

The methodology starts by gathering and examining the Cybersecurity Risks Dataset. Then, Data pre-processing is applied by performing missing value imputation, outlier removal, categorical variable encoding, and normalization by using StandardScaler to enhance the quality of the data. An 80:20 stratified split is then used to divide the dataset into training and testing sets while maintaining the class distribution. A DL model that hybridizes GRU and BiLSTM is created to help capture short- and long-term dependencies in the data. Lastly, the accuracy, precision, rec, F1, and ROC curve metrics are used to compare the model, whereas Fig. 1 illustrates the suggested approach.

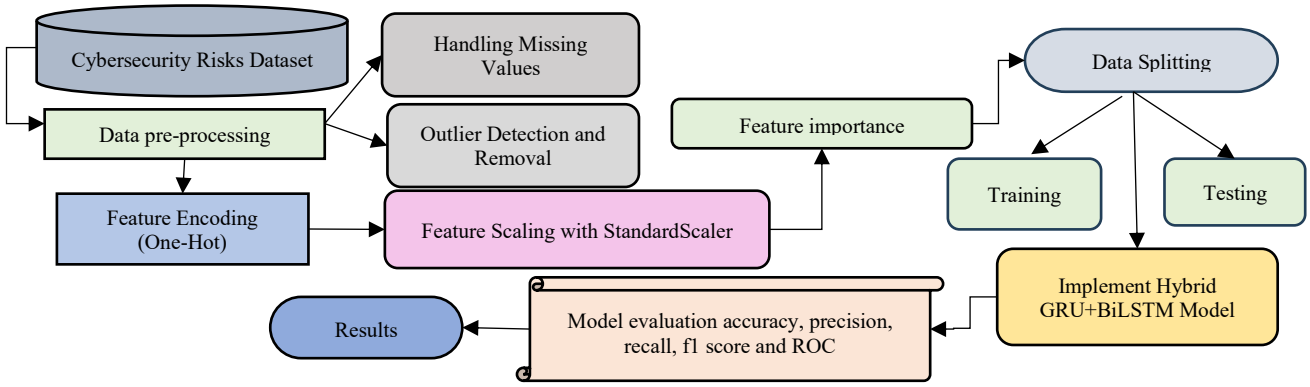

Fig. 1. Proposed Flowchart of Methodology

A detailed description of the suggested methodology's steps is provided in the following section:

A. Data Gathering and Analysis

The Threats to Cybersecurity There are 40,000 records in the Kaggle dataset, and each record has one of 25 attributes. These features include information on network traffic, signs of attacks, and system logs. Bar graphs and heatmaps are examples of data visualizations that are used to assess attack distribution and find feature connections:

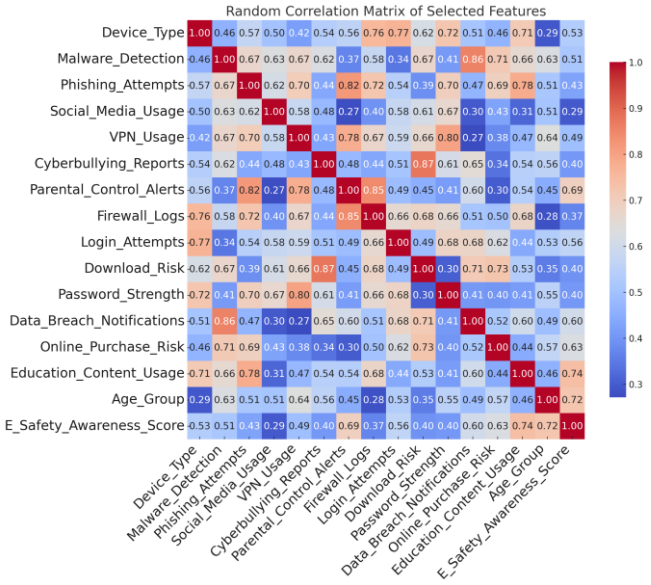

Fig. 2. Correlation of the Selected Features

A correlation matrix showing the direction and intensity of correlations between variables is shown in Fig. 2 for specific features. Stable positive and negative associations can be used

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

to identify key characteristics that contribute to cybersecurity risks, making it feasible to select features.

B. Data Pre-processing

The dataset is used for feature engineering, concatenation, and cleaning. There were several pre-processing steps such as the treatment of missing data, removal of duplication, removal of redundant data and noise and normalization. The major pre-processing steps are summarized below:

- **Pre-processing of Missing values:** Missing data are preprocessed to address missing or null values. Data quality and model reliability maintained by using correct methods including imputation and removal.
- **Outlier Detection and Removal:** To detect and remove outliers and extreme values that may bias the analysis, outlier detection and removal are carried out. This measure improved data consistency and overall model performance.

C. Feature Encoding (One-Hot Method)

The purpose of one-hot encoding is to transform categorical data into a numerical form that ML models can digest. The categories are converted to binary vectors, so that no ordinal relationship is created between values. This enhances model performance by facilitating the management of nominal data.

D. Feature Scaling with StandardScaler

The StandardScaler () technique is used to normalize the dataset by transforming it so that the distribution's mean is zero and its standard deviation is one. Equation (1) illustrates how to do this transformation by subtracting each observation's mean value and dividing by the standard deviation:

$$z = \frac{x-\mu}{\sigma} \quad (1)$$

in which x represents the starting point for every descriptor, z the transformed feature value, μ the mean of the dataset, and σ its standard deviation.

E. Feature importance

The most important factors that contributed to the cybersecurity risk forecast are identified using feature significance analysis. It also brings out the critical characteristics that produce on model performance and decision-making, the biggest influence. The process helps to select features leading to enhanced ACC and interpretability of models.

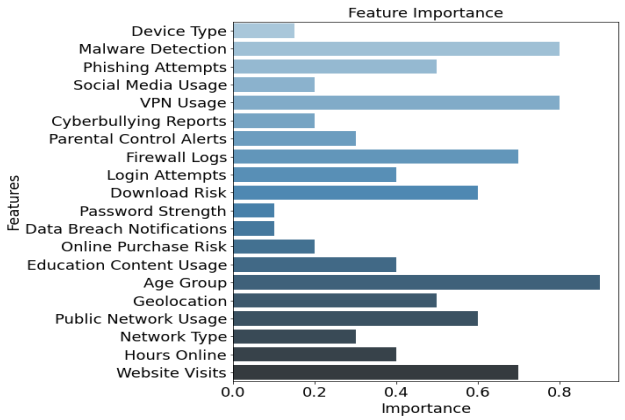

Fig. 3. Feature Importance of Features

Fig. 3 shows a bar chart indicating that various features have different significance in predicting cybersecurity risk, with higher values indicating a greater impact on the model. The age group, malware detection, and VPN usage are all important factors contributing to prediction performance.

F. Data Splitting

The dataset is split into 80% for training and 20% for testing to make an 80:20 stratified training-test split. Stratified sampling is used to partition the data into 80% training and 20% testing, ensuring that the class distribution is preserved.

G. Proposed Hybrid Gated Recurrent Unit (GRU)+ Bidirectional Long Short-Term Memory(BiLSTM) Model

A DL-based Hybrid GRU + BiLSTM Model is proposed to solve the Portfolio Optimization problem in this work. The suggested hybrid model successfully captures both short-term and long-term dependencies in sequential data by combining the advantages of GRU and BiLSTM networks. GRUs are efficient in computation and can address vanishing gradient problem while still retaining the ability of BiLSTMs to learn from the context by analyzing the sequence in both directions. This blended approach is especially appropriate for modelling temporal patterns, such as in time-series forecasting and sequence modelling applications. The hybrid model is derived using equations (2-5):

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \quad (2)$$

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \quad (3)$$

$$\bar{h}_t = tanh(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \quad (4)$$

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \bar{h}_t \quad (5)$$

The GRU component enhances the learning speed without losing the critical memory, while the BiLSTM component captures the bidirectional dependency, achieving better forecasting performance.

H. Evaluation Metrics

The performance of proposed model is measured with help of various performance metrics[32]. To depict the outcome of classification, a confusion matrix is built with TP, FP, TN, and FN. According to these values, main metrics, including acc, prec, rec and F1, are calculated to measure overall performance of a model:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Accuracy: The proportion of accurately predicted instances by the trained model to all instances in dataset (input samples). It is given as Equation (6):

$$Accuracy = \frac{TP+TN}{TP+Fp+TN+FN} \quad (6)$$

Precision: The term "precision" refers to the percentage of positive cases that the model correctly predicts relative to the total number of positive outcomes. ACC shows... Equation (7) is its formal representation:

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

Recall: The ratio of positively expected occurrences to all instances that ought to have been positively impacted is this metric. It is expressed mathematically as equation (8):

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

F1 score: It aids in striking a balance between memory and PRE by combining the harmonic mean of the two. [0, 1] is its range. Mathematically, it is given as Equation (9):

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (9)$$

Receiver Operating Characteristic Curve (ROC): The ROC, a visual representation of multiple decisions, plots the proportion of instances correctly classified as positive versus those incorrectly classified as positive. While TPR is commonly referred to as sensitivity or REC, FPR is equal to 1-specificity.

IV. Results and Discussion

This experiment was executed on a GPU-enabled Google Colab platform using TensorFlow 2.9. The hardware used was a Dell Core i7 (12th Gen) machine with 32GB RAM and an NVIDIA RTX 3090 graphics card, which greatly improved the performance of DL operations. In Table II, the main metrics ACC, prec, rec, and F1 were evaluated on the Cybersecurity Risks Dataset. The findings indicate that the Hybrid GRU+BiLSTM model achieved 97% ACC and PRE, and 98% REC and F1, indicating strong predictive performance. In general, the model is effective in promoting cybersecurity awareness and risk management in human resource systems.

TABLE II. Classification Results of Proposed Model Using Cybersecurity Risks Dataset

Matrix	Hybrid GRU+BiLSTM
Accuracy	97
Precision	97
Recall	98
F1-score	98

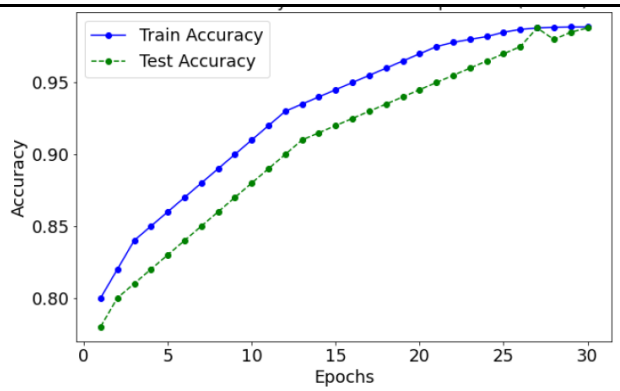

Fig. 4. Accuracy Curve for the Proposed Model

Fig. 4 shows the learning process of model, with Train and Test ACC (blue and green lines respectively) rising steadily to about 80 and then almost 100% respectively in 30 epochs. The tracking of the two lines, particularly when they merge at the end, is quite evident indicating a very stable training process with great generalization and no overfitting.

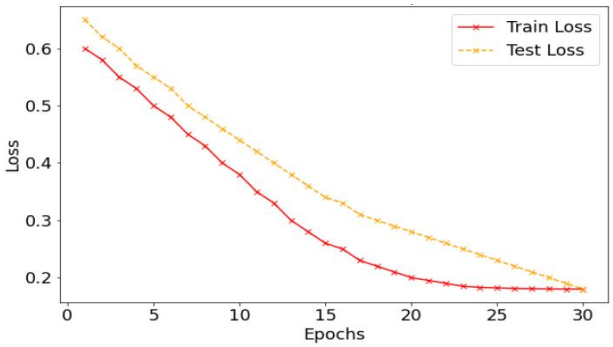

Fig. 5. Loss curve for the proposed model

Fig. 5 depicts an effective training process of an ML model in which both Train Loss (solid red line) and Test Loss (orange dashed line) decrease steadily in the first 30 epochs with a starting value of around 0.6 and a finishing value of roughly 0.2. The small distance between two curves suggests that model is extrapolating to unobservable data without overfitting or underfitting. Fig. 6 displays confusion matrix of Hybrid model performance with most of the predictions being correct along the diagonal under Safe (80), Neutral (53) and Risky (18) types. The total number of misclassifications per 156 samples is only five, which means that the model is especially useful in identification of safe and risky behaviour with minimal overlap.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

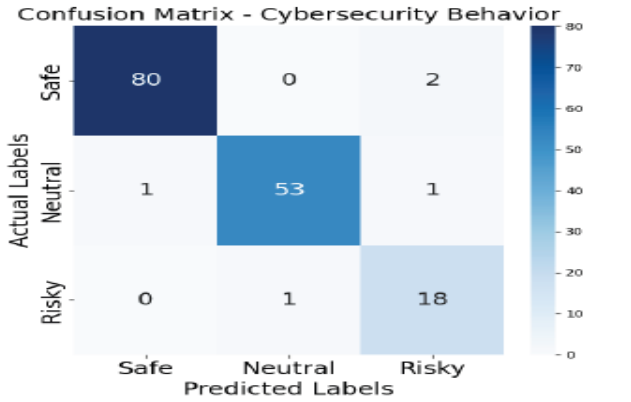

Fig. 6. Confusion Matrix for the Hybrid GRU+BiLSTM model

A. Comparative Analysis

Table III compares current ML and DL models for cybersecurity awareness to assess the efficacy of the suggested Hybrid GRU+BiLSTM model. As results show, the hybrid model has the highest performance with values of 97%, 97%, and 98% of ACC, prec, and rec and the F1, respectively. By comparison, the CNN-LSTM model achieves excellent performance, with 96.3% ACC. The RF and KNN models are comparable in ACC (93.1 and 93). In the meantime, the RNN model does the worst, having only 55% ACC and relatively low evaluation scores.

TABLE III. COMPARISON OF DIFFERENT MACHINE LEARNING AND DEEP LEARNING MODELS FOR CYBERSECURITY AWARENESS IN HR MANAGEMENT

Model	Accuracy	Precision	Recall	F1-score
RNN[33]	55	56	52	54
RF[34]	93.1	91.2	90.5	90.9
CNN-LSTM[34]	96.3	96.2	95.1	95.6
KNN[35]	93	90	87	88
Hybrid GRU+BiLSTM	**97**	**97**	**98**	**98**

The Hybrid GRU+BiLSTM model has great strengths, and ACC of model is high at 97, which makes the detection of cybersecurity threats reliable and accurate. It is able to capture sequential and contextual patterns effectively by integrating GRU and BiLSTM structures, resulting in better prediction. Also, the model can improve the quality of decision-making related to cybersecurity awareness by minimizing errors and improving the overall system robustness.

V. CONCLUSION AND FUTURE WORK

The accelerated process of digital revolution has generated an unprecedented need for professional cybersecurity. Human Resource Management (HRM) practices need to be modified to deal with this shortage of workforce particularly as cyber threats are becoming more advanced. In this paper, the objective is to discuss how HRM strategies can be optimized to effectively build a cybersecurity workforce. According to the outputs of the experiment, the experimental findings reveal that proposed Hybrid GRU+BiLSTM model is much better than classical models like RNN, RF, CNN-LSTM and KNN with the highest ACC on the Cybersecurity Risks Dataset. Consequently, the suggested model is a trustworthy and efficient solution to the improvement of cybersecurity awareness within human resource management systems, and it leads to better resilience of organizations and mitigation of risks. Future research can be devoted to possibility of incorporating real-time cybersecurity monitoring and large-scale and varied datasets to further improve the ACC and scalability of predictions.

REFERENCES

[1] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, Mar. 2014, doi: 10.1080/0144929X.2012.708787.

[2] H. Wang, W. Ma, F. Deng, H. Zheng, and Q. Wu, "Dynamic threshold ECDSA signature and application to asset custody in blockchain," *J. Inf. Secur. Appl.*, vol. 61, p. 102805, Sept. 2021, doi: 10.1016/j.jisa.2021.102805.

[3] S. T. S. Tarakampet, "Architecting Resilient HR Automation Systems: Lessons from Enterprise-Scale Deployments," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 14, no. 1, pp. 1723–1729, 2026, doi: 10.22214/ijraset.2026.77214.

[4] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, "Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability," *Comput. Sci. IT Res. J.*, vol. 5, no. 1, pp. 100–119, Jan. 2024, doi: 10.51594/csitrj.v5i1.708.

[5] M. Alshaikh, "Developing cybersecurity culture to influence employee behaviour: A practice perspective," *Comput. Secur.*, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.

[6] B. Madupati, M. M. Mohammed, L. Upadhyay, D. P. Guda, K. Kaushik, and M. Soni, "Integrating Artificial Intelligence with Cybersecurity for Resilient Wireless Communication Against Advanced Threats," in *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, IEEE, Aug. 2025, pp. 1–5. doi: 10.1109/AIMV66517.2025.11203666.

[7] B. Singh, M. A. Augie, H. Singh, and T. Banerjee, "Strengthening Modern IAM Authentication with Quantum Cryptography and Anti-Phishing Techniques," *Sarcouncil J. Eng. Comput. Sci.*, vol. 04, no. 10, pp. 17–31, October, 2025, doi: 10.5281/zenodo.17260292.

[8] I. Barreto, "Dynamic Capabilities: A Review of Past Research and an Agenda for the Future," *J. Manage.*, vol. 36, no. 1, pp. 256–280, Jan. 2010, doi: 10.1177/0149206309350776.

[9] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[10] V. K. R. K. Koppireddy, "AI-driven cybersecurity integration: a comprehensive framework for enterprise security automation and threat management," *Int. J. Adv. Res. Eng. Technol*, vol. 16, no. 1, pp. 189–200, 2025.

[11] D. P. Guda and C. Appani, "Graph Neural Networks for Dynamic Malware Behaviour Analysis and Classification in Advanced Persistent Threats (APT)," *Int. J. Commun. Networks Inf. Secur.*, vol. 14, no. 3, 2022.

[12] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, no. 10, pp. 13–21, Oct. 2014, doi: 10.22215/timreview/835.

[13] S. Duchek, "Organizational resilience: a capability-based conceptualisation," *Bus. Res.*, vol. 13, no. 1, pp. 215–246, 2020, doi: 10.1007/s40685-019-0085-7.

[14] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER – Int. Res. JOURNAL*, vol. 9, no. 10, pp. 49–55, 2022.

[15] D. Ussher-Eke, "The Human Firewall: How HR Shapes cybersecurity culture," *Int. J. Sci. Res. Arch.*, vol. 16, no. 2, pp. 505–514, Aug. 2025, doi: 10.30574/ijsra.2025.16.2.2349.

[16] P. Kumar, "A Zero Trust-Based Approach to Modern

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Cybersecurity Challenges in Software Development," *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 9, pp. 113–122, September, 2025.

[17] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, Mohali, Punjab, India: IEEE, 2025, pp. 1–6, December. doi: 10.1109/ISAECT68904.2025.11318752.

[18] S. A. Gramitto Ricci and C. M. Sautter, "The Educated Retail Investor: A Response to 'Regulating Democratized Investing,'" *Ohio State Law J. Online*, 2022.

[19] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.

[20] S. P.Sivashanmugam, S. Kumara, A. Mohile, and D. R. Suram, "Improving Detection Accuracy of Phishing Attacks with Feature Selection and Machine Learning Techniques in Cybersecurity," in *2026 1st International Conference on Emerging Trends in Advancements and Applications of Computational Intelligence Techniques (ETAACT)*, Bhubaneswar, India: IEEE, Apr. 2026, pp. 1–6. doi: 10.1109/ETAACT69135.2026.11542138.

[21] S. Priyadarshi and M. A. Hashmi, "Cybersecurity data science and threats: an overview from machine learning perspective," *Accent. Trans. Inf. Secur.*, vol. 7, no. 25, Jan. 2022, doi: 10.19101/TIS.2021.621013.

[22] S. Tarakampet and S. B. S. Ali, "Integrating Custom Enterprise Applications with Legacy Systems for Risk Management: A Modern Enterprise Approach," *Int. J. Trend Sci. Res. Dev.*, vol. 10, no. 1, 2026.

[23] S. Somula, "Legacy system modernization: Strategic imperatives and transformation metrics in digital evolution," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 1, pp. 2597–2606, Feb, 2025, doi: 10.32628/CSEIT251112278.

[24] A. T. Swati Tyagi, "Evaluating the Performance with Deep Learning Techniques in Cybersecurity for Effective Threat Detection," in *Proceedings of International Conference on Information Technology and Artificial Intelligence*, 2025, pp. 437–452, October. doi: https://doi.org/10.1007/978-981-96-8687-2_31.

[25] R. Kumar, K. Srujana, P. Sampath, J. C. Patni, P. Agrawal, and S. R. Mallick, "Detecting Phishing Emails with Artificial Intelligence: A Hybrid Machine Learning Approach," in *2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, IEEE, Aug. 2025, pp. 132–136. doi: 10.1109/ETNCC66224.2025.11299563.

[26] Jonathan, A. D. Novika, and D. Suhartono, "Leveraging Machine Learning for Early Detection of Depression Based on Social Media Behaviour," in *2025 IEEE 2nd International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, IEEE, Oct. 2025, pp. 138–142. doi: 10.1109/ICoCICs68032.2025.11384019.

[27] Z. Zhao, C. Yuan, and X. Jiang, "Research on Risk Perception in Power Information Communication Based on Machine Learning," in *2024 7th International Conference on Mechatronics and Computer Technology Engineering (MCTE)*, IEEE, Aug. 2024, pp. 1090–1093. doi: 10.1109/MCTE62870.2024.11118050.

[28] A. Setiyaji, K. Ramli, Z. Y. Hidayatulloh, and G. S. Budhi Dharmawan, "A technique utilizing Machine Learning and Convolutional Neural Networks (CNN) for the identification of SQL Injection Attacks," in *2024 4th International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, IEEE, Jul. 2024, pp. 1–6. doi: 10.1109/ICSINTESA62455.2024.10748116.

[29] M. Mouiti, A. Elhariri, O. Habibi, and M. Lazaar, "Toward Improving Internet of Things (IoT) Networks Security Using Machine Learning Based Intrusion Detection System," in *Proceedings - 2023 International Conference on Digital Age and Technological Advances for Sustainable Development, ICDATA 2023*, 2023. doi: 10.1109/ICDATA58816.2023.00018.

[30] P. Thantharate and A. T, "CYBRIA - Pioneering Federated Learning for Privacy-Aware Cybersecurity with Brilliance," in *2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET)*, IEEE, Dec. 2023, pp. 56–61. doi: 10.1109/HONET59747.2023.10374608.

[31] B. Strickson, C. Worsley, and S. Bertram, "Human-centred Assessment of Automated Tools for Improved Cyber Situational Awareness," in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, IEEE, May 2023, pp. 273–286. doi: 10.23919/CyCon58705.2023.10181567.

[32] P. Srivastava and K. Kirti, "Cyber security challenges in human resource technology: protecting employee data in the digital age," in *Strategic Blueprint for Viksit Bharat 2047*, Maharashtra: Dzarc Publications, May 2025, pp. 114–121. doi: 10.64171/JSRD.4.S1.114-121.

[33] M. G. Rubina, Kureshi, and D. R. K. Dhuware, "A Deep Learning Framework for Cyber Security Attacks Detection Using CNN-RNN-Bi-LSTM Algorithms Using Jupyter Notebook," *Int. J. Nov. Res. Dev.*, vol. 10, no. 6, pp. 779–794, 2025.

[34] O. M. Nwakeze, N. U. Mohammed, and N. P. Oboti, "Enhancing Risk Management with Human Factors in Cybersecurity Using Behavioural Analysis and Machine Learning Technique," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 51, pp. 101–118, Jun. 2025, doi: 10.37745/ejcsit.2013/vol13n51101118.

[35] W. N. Mike Nkongolo and M. Tokmak, "Evaluating Cybersecurity Awareness in Employees Using Gameplay: Data and Machine Learning Models," *Eur. Conf. Games Based Learn.*, vol. 19, no. 2, pp. 648–657, 2025, doi: 10.34190/ecgbl.19.2.3978.