Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 5s (2025)

Securing Future Learning in Education 5.0: An Ensemble Learning for Secure Smart Education System (SSEduS)

Sonal Shukla [1*], Anand Sharma [1]

[1*] sona.shukla91@gmail.com, [1] anand_glee@yahoo.co.in

[1] Mody University of Science and Technology, Sikar Rd, Lakshmangarh, Narodara Rural, Rajasthan 332311, India.

[1*]0000-0003-4242-244X, 10000-0002-9995-6226

Article History:

Received: *07-10-2024*

Revised: *27-11-2024*

Accepted: *06-12-2024*

Abstract:

Introduction: Education system is making its debut in the smart and intelligent system at a slow pace but the change seen in the system is an amazing shift. The learning system has developed and contributed to the disciples in many ways in Education using interactive tools and application of artificial intelligence i.e. Education 5.0. Integration of various technologies makes the Education 5.0 as the smart and intelligent education system which makes a more complex environment with unique security challenges. In this paper we attempt to analyse computer science, security and education to make a Secure Smart Education System (SSES) by using ensemble learning to address the security challenges. This paper addresses these challenges, associated risk and provides a basic analysis for cyber security..

Objectives: The objective of this work is to explore the transformative impact of Education 5.0, which represents a significant evolution in the educational landscape through the integration of advanced technologies, including artificial intelligence and interactive tools. As the education system gradually embraces these smart and intelligent frameworks, it encounters a myriad of unique security challenges that arise from the complexity of this new environment. This paper aims to analyse the intersection of computer science, security, and education to develop a Secure Smart Education System (SSES) that effectively addresses these security challenges.

Methods: This paper aims to analyse the intersection of computer science, security, and education to develop a Secure Smart Education System (SSES) that effectively addresses these security challenges. By employing ensemble learning techniques, we seek to enhance the robustness of security measures within educational platforms, thereby mitigating associated risks and vulnerabilities. Furthermore, this work provides a foundational analysis of cybersecurity issues pertinent to the educational sector, offering insights into how to create a safer and more secure learning environment in the context of rapidly evolving technological advancements.

Results: The proposed model is named the Secure Smart Education System (SSEduS), as it has shown promising results while using publicly available network data. This model consists of a stacked ensemble that uses three classifiers divided into two categories: traditional models and ensemble models for detecting malicious activity. Unlike other conventional models, our model is a perfect combination of base learners and strong learners. The proposed model has demonstrated good results, achieving nearly perfect accuracy of 99.99% and a false positive rate of 0.46%. The results have shown significant improvement over the existing models studied. The accuracy achieved is the best result so far using the stacked ensemble.

Conclusions: Our goal was to contribute to the ongoing discourse on the integration of security in smart education systems, ensuring that the benefits of Education 5.0 can be realized without compromising the safety and integrity of educational data and process.

Keywords: Smart Education, Education 5.0, Ensemble Learning, Cyber security, Secure Smart Education system (SSES).

1. Introduction

The education industry has adapted to new development and technological advancements in the sector. The digital transformation has now become an essential requirement of higher education to make it more robust, convenient and reachable. [1] This digital transformation has led to the fourth industrial revolution which aims to transform the ways of education by involving the use of artificial intelligence, machine learning, robotics and internet of things (IoT) [2]. This learning does not just focus on learning but also on skills of the disciples. With the rapid advancements in technology and the changing nature of work, individuals need a specific combination of skills to thrive.

Multiple technologies contributing to the era of smart education, each of these technologies have their merits and demerits. Privacy and security being the prominent issue in the all technologies poses the important issue in front of smart education [3]. There are many past incidents which show the need for security and privacy measures in the education sector. The victims in the education field are mostly students who have fresh identities in the society and are vulnerable as it can be easily targeted by the attacks. The cybercrime hits the education sector on a different level as the victims involved are either naive and have lack of knowledge of cyberspace, their identities are more prone to be used and they are more easier to be targeted [4]. It can be easily concluded that cyber attacks are a severe problem which should be addressed by any educational institutes or higher education bodies [5].

Cyber security in education system can be stated as the measure to protect the internet users which are students, faculties and managing bodies in our case, from the hazardous risks related to the modern technologies used in digital learning or use of internet [6]. After COVID-19, there was a rapid increase in the number of cyber-attacks all over the world. According to the Indian Cyber threat report 2023 [7] by Data Security Council of India, cyber security has become the top most priority for all the organizations. The education industry is in the top three industries after automobile [8] and government to keep its eyes open for cyber attacks especially malware attack along with phishing and ransomware attack. The lack of cyber awareness, frequent movement of staff and faculties and IoT vulnerabilities are the reason for cyber threats in the education system [9][10]. Therefore, in this paper we focus on core principles of Education 5.0, challenges and risks associated. In further sections we discussed the ensemble technique of machine learning contributing to cyber security which can also be leveraged in higher education and thus, we propose a secure model, Secure Smart Education System (SSEduS).

2. Education 5.0: Smart Education System

Education 5.0 came into existence as a response to the 4th industrial revolution which blurs the lines between technological advancements in physical, digital and biological fields. It was a new vision which helps the learners to acknowledge the sources which helps in building their skill sets as well as

knowledge base [11]. Contributing to self-paced learning by leveraging the benefits of artificial intelligence, it is also known as Smart Education, to personalize the learning experience, improve educational outcomes, and prepare students for the demands of the 21st century [2][12].

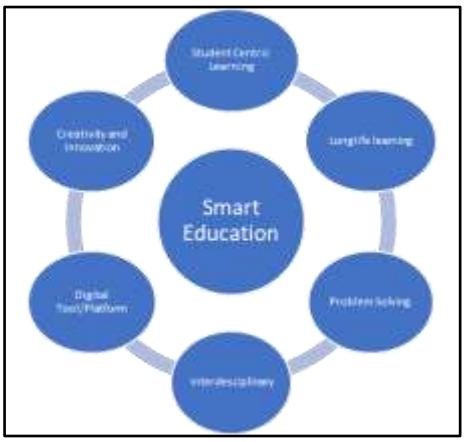

Figure 1. Key principles of Smart Education (Education 5.0)

The Core Principles of Education 5.0 can be categorized as student centric with technology integration. Education 5.0 not only helps the learners in skill development but as the overall development tool with respect to industry demands which further acts as a backbone in a job centric environment [13]. Students are the active entity in this learning environment with self-paced and personalized touch. Learning platforms provide speed-based content which can be selected by learners themselves [14]. Multiple technologies are contributing to make the pillars of Education 5.0, such as Big data, Internet of Things, Cloud services, Virtual reality and Augmented reality [15].

Unlike traditional teaching- learning methods which were teacher centric, this evolution goes beyond the classroom teaching and memorization [16], it focuses more on skill development like communication, personality development, critical thinking, problem solving, creativity etc. [17] [18].

With the ability to adapt and enhance the skill set, smart education is believed to inculcate a routine of lifelong learning in learners [19]. In this way, we will be giving our future generation the best possible education which will address a global skill gap problem and will give talented, upskilled leaders of society [20]. Although the potential of Education 5.0 is capturing the imagination of more and more people, implementation and the level of support is still in its infancy, with some small-scale attempts in some parts of the world, but still largely in a test phase [21]. It can be stated that smart education is a future vision of educational entities that will contribute in reforming education with respect to changes in technology and future demand of skill set in jobs. Making the use of a big umbrella "Artificial intelligence" [21][22], learners who need special attention can also be accommodated with better opportunities to learn and can be continuously monitored to improve their progress and educational achievements.

3. Challenges in Education 5.0

As moving towards the smart future, education has also evolved from past many years witnessing how much technological developments are contributing in making a new world. The development in education were categorised in stages Education 1.0 to 5.0 with respect to the transformation in internet

web [23]. Industrial revolution 5.0 targets to successfully integrate the artificial intelligence kits in the education system which positively contributes to the learning mechanism of an individual [24]. It is also important to identify solutions at the level of general education, including the humanities. This means that Education 5.0 should also be developed at the primary, secondary and higher education levels which include the humanities. Education 5.0 opens a new phase in which the humanist ideas are integrated into the digital world [25]

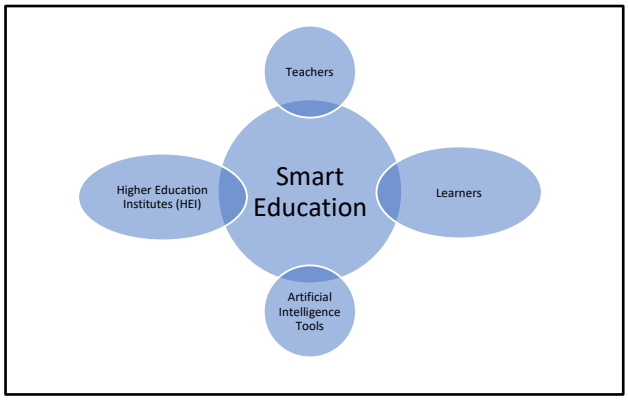

Figure 2. Key component of Smart Education

Taking India as an example, digital education is divided significantly into two areas: rural and urban. Few challenges faced by education while implementing the smart education in higher education [26]:

Digital Literacy: Rate of digital literacy varies from geographical region to region and this number is far from adequate with respect to the population in India [27]. Some developed countries are excelling in artificial intelligence and use of it in education as well whereas on the other hand more than half of the world comes under the category of developing or under developed countries who are still not fully aware of the benefits of AI in education and yet to implement it in education [28].

Internet Connectivity: In rural parts of the country, there is still need for network connectivity. Lack of this directly affects the growth of smart education in the country. [29] Digital India report of 2024 starting [30] reflected that approx. 52 percent of the population is internet users which is further divided into rural and urban areas.

Network Infrastructure: The network infrastructure refers to the combination of hardware as well as software components responsible for network connectivity and communication between parties. Many parts of developing countries like India are still struggling for internet connectivity and those who have this facility are suffering from bad infrastructure support for better connectivity [31].

Privacy Issue: Lots of data is stored digitally on servers and network storage to make it readily available to users and same goes for any education industry as well. Privacy of such data is an important issue which needs to be taken care of by educational institutions. Data breaches are the most common attack encountered by many sectors including education [32]. This issue can have hazardous effects if not taken care of at the right time. Most of the cyber attacks like phishing, ransome-ware, malwares etc are the result of poor privacy security management. Schools and universities are the most vulnerable as they consist of the students' records which are fresh identities in the cyber world and most targeted by attackers [33].

Smart education system has many benefits but it also comprises risks associated with these challenges. Data privacy and security have been the top most of all as artificial intelligence, the key component of education 5.0 [34], cannot be of use without a proper network with a secure mechanism to protect it from outside agents. Lack of cyber awareness and poor technology implementation attracts cyber-attacks, thus in our next section we discuss the machine learning based ensemble model which may help the education sector if implemented to detect the intrusion within their network.

4. Ensemble Learning in Security

Ensemble learning is a powerful machine learning technique that combines the predictions of multiple weaker models to create a single, more robust and accurate model. In the realm of security, ensemble learning is gaining traction due to its ability to address the ever-evolving landscape of cyber threats.

It can be used for a wider range of attacks in the cyber realm. The intrusion detection methods can be enhanced and made more accurate if the ensemble model is implemented. The models designed by implementing ensemble learning consist of various machine learning models which are trained on the same data set [35]. These types of models are more diverse in nature which helps in identifying different features and patterns in data, which make these models more robust in intrusion detection systems [36]. The final result is concluded by combining the prediction analysis done by various ML algorithms. The combining is done by various ensemble techniques:

Common Ensemble Techniques used in Security [37] [38]:

- **Bagging (Bootstrap aggregating):** Trains multiple models on different subsets of data with replacement, then aggregates their predictions through techniques like averaging or voting.
- **Boosting:** Trains models sequentially, where each subsequent model focuses on the errors made by the previous one, ultimately leading to a more robust ensemble.
- **Stacking:** Trains a meta-learner model that combines the predictions of several base-learner models to generate the final prediction.

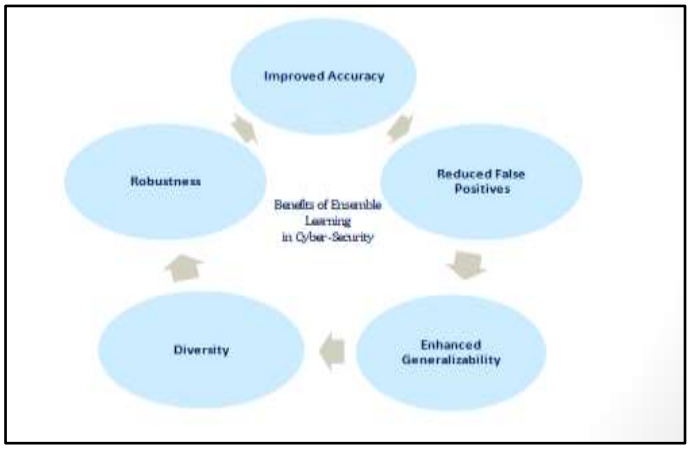

Figure 3. Benefits of Ensemble Learning models in Cyber security

5. Secure Smart Education System (SSEduS)

In our research we intended to combine ensemble learning for network security in smart education due to the high dependency of internet networks in it. Our proposed model emphasizes the security issue

acknowledged earlier. Our model uses the hybrid model which combines the traditional machine learning (ML) algorithms with the ensemble model to enhance the overall performance of the proposed SSEduS model. The traditional ML algorithms are also known as classical learning algorithms, the foundation of machine learning [39]. In our proposed methodology, we have used decision tree and random forest traditional machine learning algorithms and XGBoost (Gradient boosting algorithm) for ensemble methods.

Decision tree algorithms are selected for effective handling of labeled, categorised and numerical data but since it comes with a problem of overfitting [40], we have combined it with random forest as an improvement on it. Random forest creates multiple trees and combines their predictions, often resulting in better accuracy than individual trees. Random forest is also used as an ensemble method in the SSEduS model. We have done bootstrap aggregation by random forest and applied a decision tree on each sample generated by bootstrap aggregation. Voting mechanism is done at each node for the prediction and prediction with majority vote is the final verdict.

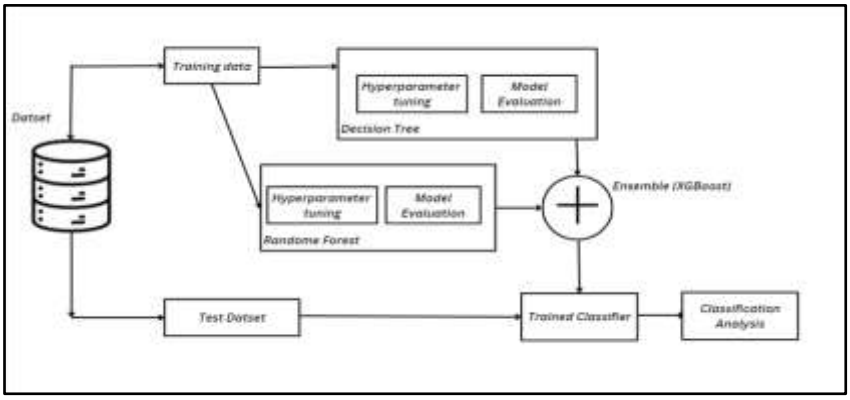

Figure 4. Block diagram of Proposed SSEduS Model.

Along with the traditional method, gradient boosting technique is also used to create a stronger predictive model by combining various weak learners. The evaluation phase consists of evaluation of performance of each model and later on conducting the classification analysis of the combined model using evaluation techniques. A confusion matrix is used for performance evaluation of classification algorithms [41], showing positive and negative predictions. Another evaluation method implemented was cross- validation by dividing the dataset into multiple folds for training and testing. The performance metrics used are [42]:

- **Accuracy:** The overall proportion of correct predictions (both true positives and true negatives).
- **Precision:** The proportion of positive predictions that are actually correct (true positives out of all positive predictions).
- **Recall (Sensitivity):** The proportion of actual positives that are correctly identified (true positives out of all actual positives).
- **F1-score:** The harmonic mean of precision and recall, providing a balance between the two.
- **False Positive Rate (FPR):** The proportion of negative instances incorrectly classified as positive.

- **True Positive Rate (TPR):** The proportion of positive instances correctly classified as positive (same as recall).

6. Result and Conclusion:

In this study, we used our university network traffic data but it was not sufficient to provide any conclusive results. And due to the data confidentiality clause of universities, real time data could not be used. Hence, we have used the CICIDS 2017 dataset which is a static publicly available dataset for intrusion detection. The dataset is further divided into 80:20 ratio for training and testing.

This section discusses the complete experimental results that have been carried out in our study. The selection features for traditional machine learning and ensemble methods are presented in Table 1 and Table 2.

Table 1. Features selected for Decision Tree

No.	Feat. ID	Feature Names
1	41	Packet Length Std
2	13	Total Length of Bwd Packets
3	65	Subflow Bwd Bytes
4	8	Destination Port
5	42	Packet Length Variance
6	20	Bwd Packet Length Mean
7	54	Avg Bwd Segment Size
8	18	Bwd Packet Length Max
9	67	Init_Win_bytes_backward
10	12	Total Length of Fwd Packets
11	63	Subflow Fwd Bytes
12	66	Init_Win_bytes_forward
13	52	Average Packet Size
14	40	Packet Length Mean
15	39	Max Packet Length
16	14	Fwd Packet Length Max
17	22	Flow IAT Max
18	36	Bwd Header Length
19	9	Flow Duration
20	26	Fwd IAT Max
21	55	Fwd Header Length
22	24	Fwd IAT Total

Table 2. Features selected for Random Forest

No.	Weigth	Feat. ID	Feat. Names
1	0.7521	41	Packet Length Std
2	0.7197	13	Total Length of Bwd Packets
3	0.7197	65	Subflow Bwd Bytes
4	0.6937	66	Init_Win_bytes_forward
5	0.6916	63	Subflow Fwd Bytes
6	0.6916	12	Total Length of Fwd Packets
7	0.6823	42	Packet Length Variance
8	0.6694	40	Packet Length Mean
9	0.6571	18	Bwd Packet Length Max
10	0.6511	39	Max Packet Length
11	0.6472	67	Init_Win_bytes_backward
12	0.6401	52	Average Packet Size
13	0.64	20	Bwd Packet Length Mean
14	0.64	54	Avg Bwd Segment Size
15	0.6313	14	Fwd Packet Length Max
16	0.6096	8	Destination Port
17	0.6089	22	Flow IAT Max
18	0.5835	9	Flow Duration
19	0.5769	55	Fwd Header Length
20	0.5707	26	Fwd IAT Max
21	0.5485	36	Bwd Header Length
22	0.5438	24	Fwd IAT Total
23	0.5051	25	Fwd IAT Mean
24	0.4752	21	Flow IAT Mean
25	0.4718	53	Avg Fwd Segment Size
26	0.4718	16	Fwd Packet Length Mean
27	0.4673	1	Bwd Packet Length Std
28	0.4604	2	Flow Bytes/s

To build the strong ensemble model using stacking techniques, we have trained three classifiers, decision tree, random forest (both as base learners) and combiner XGBoost (meta learner) in parallel fashion. While conducting our experiment, we used a random forest with 50 trees and XGBoost with 200 trees. In SSEduS proposed model, we have implemented the proposed approach on dataset using multiple folds i.e 5 folds and 10 folds and variety of splits ranging from 10 to 90 on traditional models.

Table 3. Validation Results traditional stacked ensemble model

	Total Instances		Accuracy	
Test Mode	**Training**	**Testing**	**Training**	**Testing**
Use Training Set	594456	254767	99.989	99.994
10-Fold	594456	254767	99.847	99.829
5-Fold	594456	254767	99.844	99.831
Split 10	535010	229290	99.762	99.829
Split 20	475565	203814	99.803	99.745
Split 30	416119	178337	99.817	99.772
Split 40	356674	152860	99.833	99.779
Split 50	297228	127383	99.831	99.821
Split 60	237782	101907	99.831	99.825
Split 70	178337	76430	99.844	99.837
Split 80	118891	50953	99.847	99.835
Split 90	59446	25477	99.860	99.859
	Average		**99.842**	**99.830**

The individual performance of the traditional model was measured using a confusion matrix. A confusion matrix is most commonly used and an efficient, two dimensional matrix presenting the information regarding actual class and prediction class. According to our observation, the confusion

matrix of each traditional method (model 1: decision tree classifier and model 3: random forest) is presented in figure 5.

Training Decision Tree Classifier			
		Actual	
		Normal	Attack
Predicted	Normal	542973	436
	Attack	432	106701

(a)

Training Random Forest			
		Actual	
		Normal	Attack
Predicted	Normal	542861	389
	Attack	239	106900

(b)

Figure 5: Presents the evaluation metrics of Traditional method using decision tree in (a) and using random forest in (b).

In the ensemble method as a combiner, gradient boosting based XGBoost classifier is used in this study. Gradient boosting is focused on finding the optimal solution for a variety of problems. This optimization algorithm works on fine tuning the learning parameters to reduce the cost function. This ensemble model was selected to reduce probability of overfitting and provide better performance. Therefore, we have used XGBoost as a combiner to handle complex interaction and non-linearities. Along with the stated benefits, XGBoost also provides better processor utilization, better speed and memory utilization. Figure 6 represents the confusion matrix at combiner level, representing the values of matrices used for evaluation.

Training XGBoost			
		Actual	
		Normal	Attack
Predicted	Normal	543041	368
	Attack	110	107023

Figure 6: Confusion matrix presentation of Ensemble classifier XGBoost.

Testing Proposed model			
		Actual	
		Normal	Attack
Predicted	Normal	33526	0
	Attack	2	431

Figure 7. Presentation of confusion matrix of proposed SSEduS model on 20% test data

The performance result can easily be calculated using the evaluation metrics presented in Figure 7. The two class confusion matrix of testing dataset of proposed SSEduS model is calculated by accuracy and false positive rate, as following

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP+FN} \quad (2)$$

The model proposed is considerably robust with the dataset and handles the imbalance problem very well. The ratio of “normal” and “attack” on the test dataset is 33,536 to 431, which is highly imbalanced. In our result, all “normal” samples were correctly detected as normal whereas 2 samples under the “attack” category were incorrectly classified as normal. The two-performance metrics, accuracy and FPR are evaluated based on this result. These metrics were also further compared with the few existing work in an unbiased manner in Table 4.

Table 4. Comparative evaluation with some existing work (our result indicated in bold)

S.no	Technique	Feature selection	Validation method	Accuracy (%)	FPR(%)	Significance test
1	Proposed	No	Hold-out 80/20	99.99	0.46	Two step statistical test
2	Deep neural network [41]	No	Hold-out	99.92	0.05	No
3	Ensemble method [40]	Yes	10cv	99.88	0.002	No
4	k-NN [42]	Yes	Hold out 70/30	99.46	Not reported	No
5	Random forest [24]	Yes	Not reported	99.4	0.01	No
6	GRU-RNN [41]	Yes	Hold-out	89	Not reported	No
7	Adaboost [28]	Yes	5x10cv	81.83	Not reported	No
8	Local outlier factor [36]	No	Hold-out	68	Not reported	No

The proposed model has shown good results with near perfect 99.99% accuracy and false positive rate as 0.46%. The results has shown significant improvement over the existing models studied. The accuracy achieved is the best result so far using the stacked ensemble.

7. Conclusion

This study has explored the evolution of smart education, education 5.0 and challenges in the area to achieve a state of art infrastructure of smart education. In this work, we have specifically focused on making smart education more reliable for all the four components associated with it. This study aims to detect the intrusion in the educational institutions network infrastructure and prevent cyber threats. The proposed model is named as Secure Smart Education System (SSEduS), as it has shown promising results while using the publicly available network data. This model consists of a stacked ensemble using three classifiers divided into two categories: traditional model and ensemble model for detecting the malicious activity. Unlike other conventional models, our model is a perfect combination of base learners and strong learners. Considering future aspects, there are many possibilities to improve this secure model.

Refrences

[1] Zhiting, Z.; Hongwei, L.; Chengqian, W.; Jiao, H. Digital Transformation and Integrative Innovations of Foreign Language Education. Technol. Enhanc. Foreign Lang. 2022, 4, 7.

[2] Hussin, Anealka Aziz. "Education 4.0 made simple: Ideas for teaching." International Journal of Education and Literacy Studies 6.3 (2018): 92-98.

[3] J.C. Augusto, Ambient intelligence: Opportunities and consequences of its use in smart classrooms, Innovation in Teaching and Learning in Information and Computer Sciences 8: (2) ((2009)), 53–63. doi:10.11120/ital.2009.08020053.
[4] Alexei, Arina & Alexei, Anatolie. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. International Journal of Scientific & Technology Research. Volume 10. 128-133.
[5] Bandara, I., Ioras, F. and Maher, K., 2014. Cyber security concerns in e-learning education. In ICERI2014 Proceedings (pp. 728-734). IATED.
[6] Singar, A.V., Akhilesh, K.B. (2020). Role of Cyber-security in Higher Education. In: Akhilesh, K., Möller, D. (eds) Smart Technologies . Springer, Singapore. https://doi.org/10.1007/978-981-13-7139-4_19
[7] Accessed on 15.07.2024, "Annual Report on Ransom-Ware in India 202, "https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2023.pdf
[8] Elkhail, A.A., Refat, R.U.D., Habre, R., Hafeez, A., Bacha, A. and Malik, H., 2021. Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses. IEEE Access, 9, pp.162401-162437.
[9] Cheng, E.C.K.; Wang, T. Institutional Strategies for Cybersecurity in Higher Education Institutions. Information 2022, 13, 192. https://doi.org/10.3390/info13040192
[10] Corradini, I. and Nardelli, E., 2020. Developing digital awareness at school: a fundamental step for cybersecurity education. In Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, July 16–20, 2020, USA (pp. 102-110). Springer International Publishing.
[11] Fisk, P. (2017). Education 4.0 … the future of learning will be dramatically different, in school and throughout life. Retrieved from https://www.peterfisk.com/2017/01/future-education-young-everyone-taught-together/
[12] Demir, K.A., 2021. Smart education framework. Smart Learning Environments, 8(1), p.29.
[13] Chen, X., Zou, D., Xie, H. and Wang, F.L., 2021. Past, present, and future of smart learning: a topic-based bibliometric analysis. International Journal of Educational Technology in Higher Education, 18(1), p.2.
[14] Jamaludin, R., McKAY, E. and Ledger, S. (2020), "Are we ready for Education 4.0 within ASEAN higher education institutions? Thriving for knowledge, industry and humanity in a dynamic higher education ecosystem?", Journal of Applied Research in Higher Education, Vol. 12 No. 5, pp. 1161-1173. https://doi.org/10.1108/JARHE-06-2019-0144
[15] Papadakis, S., Kravtsov, H.M., Osadchyi, V.V., Marienko, M.V., Pinchuk, O.P., Shyshkina, M.P., Sokolyuk, O.M., Vakaliuk, T.A. and Striuk, A.M., 2023. Revolutionizing education: using computer simulation and cloud-based smart technology to facilitate successful open learning.
[16] Lovett, M.C., Bridges, M.W., DiPietro, M., Ambrose, S.A. and Norman, M.K., 2023. How learning works: Eight research-based principles for smart teaching. John Wiley & Sons.
[17] González-Pérez, Laura Icela, and María Soledad Ramírez-Montoya. "Components of Education 4.0 in 21st century skills frameworks: systematic review." Sustainability 14.3 (2022): 1493.
[18] Cui, Q., 2023. Multimedia teaching for applied linguistic smart education system. International Journal of Human–Computer Interaction, 39(1), pp.272-281.
[19] Nguyen, A., Ngo, H.N., Hong, Y., Dang, B. and Nguyen, B.P.T., 2023. Ethical principles for artificial intelligence in education. Education and Information Technologies, 28(4), pp.4221-4241.
[20] Chatterjee, R., Bandyopadhyay, A., Chakraborty, S. and Dutta, S., 2023. Digital education: the basics with slant to digital pedagogy-an overview. Digital learning based education: transcending physical barriers, pp.63-80.
[21] J. Udvaros, N. Forman (2023) ARTIFICIAL INTELLIGENCE AND EDUCATION 4.0, INTED2023 Proceedings, pp. 6309-6317.doi: 10.21125/inted.2023.1670
[22] Lin, C.C., Huang, A.Y. and Lu, O.H., 2023. Artificial intelligence in intelligent tutoring systems toward sustainable education: a systematic review. Smart Learning Environments, 10(1), p.41.
[23] Sarowski, Ł. 2017). Od Internetu Web 1.0 do Internetu Web 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci. [From Web 1.0 to Web 4.0 – Evolution of Communication Space Forms in the Global Network.] Rozprawy Społeczne [Social Considerations], 11, 32-39.
[24] Dimitriadou, E. and Lanitis, A., 2023. A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms. Smart Learning Environments, 10(1), p.12.

[25] do Rosário Cabrita, M., Safari, H. and Dueñas, M.D.P.M., 2020. Preparing for education 4.0: Skills facing economic, social and environmental challenges. International Journal of Innovation, Management and Technology, 11(1), pp.33-37.
[26] Singh, H. and Miah, S.J., 2020. Smart education literature: A theoretical analysis. Education and Information Technologies, 25(4), pp.3299-3328., Jabbar, M.A. and Aluvalu, R., 2017, August. Smart cities in India: Are we smart enough?. In 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon) (pp. 1023-1026). IEEE., Sharma, P. and Rajput, S. eds., 2017. Sustainable smart cities in India: Challenges and future perspectives. Springer.
[27] Lee, S.H., 2014. Digital literacy education for the development of digital literacy. International Journal of Digital Literacy and Digital Competence (IJDLDC), 5(3), pp.29-43.]. Teachers and students are also not aware about the smart education methods, platforms and techniques [Spante, M., Hashemi, S.S., Lundin, M. and Algers, A., 2018. Digital competence and digital literacy in higher education research: Systematic review of concept use. Cogent education, 5(1), p.1519143.
[28] Sharma, Y., Suri, A., Sijariya, R. and Jindal, L., 2023. Role of education 4.0 in innovative curriculum practices and digital literacy–A bibliometric approach. E-Learning and Digital Media, p.20427530231221073.
[29] Audrin, C. and Audrin, B., 2022. Key factors in digital literacy in learning and education: a systematic literature review using text mining. Education and Information Technologies, 27(6), pp.7395-7419.
[30] Accessed on 06-07-2024: https://datareportal.com/reports/digital-2024-india by Digital 2024: India
[31] Hota, S.P., 2023. Education infrastructure, expenditure, enrollment & economic development in Odisha, India. International Journal of Educational Development, 103, p.102903.
[32] Geeta Dharmavaram, V. (2023). DATA PRIVACY IN EDUCATION SECTOR – ISSUES AND MEASURES. EDPACS, 68(2), 1–12. https://doi.org/10.1080/07366981.2023.2242130
[33] Kaur, M. and Saini, M., 2023. Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. Education and Information Technologies, 28(1), pp.581-615.
[34] Alharbi, A.M., 2023. Implementation of Education 5.0 in developed and developing countries: A comparative study. Creative Education, 14(5), pp.914-942.
[35] Alotaibi Y, Ilyas M. Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security. Sensors. 2023; 23(12):5568. https://doi.org/10.3390/s23125568
[36] Thockchom, N., Singh, M.M. & Nandi, U. A novel ensemble learning-based model for network intrusion detection. Complex Intell. Syst. 9, 5693–5714 (2023). https://doi.org/10.1007/s40747-023-01013-7
[37] Chakir, O., Rehaimi, A., Sadqi, Y., Krichen, M., Gaba, G.S. and Gurtov, A., 2023. An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 4.0. Journal of King Saud University-Computer and Information Sciences, 35(3), pp.103-119.
[38] Hossain, M.A. and Islam, M.S., 2023. Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array, 19, p.100306.
[39] Wang, P., Fan, E. and Wang, P., 2021. Comparative analysis of image classification algorithms based on traditional machine learning and deep learning. Pattern recognition letters, 141, pp.61-67.
[40] Azam, Z., Islam, M.M. and Huda, M.N., 2023. Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree. IEEE Access
[41] Alotaibi, Y. and Ilyas, M., 2023. Ensemble-learning framework for intrusion detection to enhance internet of things' devices security. Sensors, 23(12), p.5568.
[42] Naidu, G., Zuva, T. and Sibanda, E.M., 2023, April. A review of evaluation metrics in machine learning algorithms. In Computer Science On-line Conference (pp. 15-25). Cham: Springer International Publishing.