Cyber Protection & Awareness For Females in Bangladesh

Conference Paper · November 2023

DOI: 10.1109/ICCCNT56998.2023.10306725

Md Abrar Hamim
University of Wollongong
8 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Israt Jahan Tasnova
Daffodil International University
2 PUBLICATIONS **8** CITATIONS
SEE PROFILE

Subrina Ferdous Khan
Daffodil International University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Sharmin Sultana Mim
Daffodil International University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Cyber Protection & Awareness For Females in Bangladesh

Md Abrar Hamim
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
abrar15-11821@diu.edu.bd

Israt Jahan Tasnova
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
israt15-12932@diu.edu.bd

Sharmin Sultana Mim
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
sharmin15-13639@diu.edu.bd

Subrina Ferdous Khan
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
subrina15-13751@diu.edu.bd

F.M. Tanmoy
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
tanmoy15-13672@diu.edu.bd

***Abstract*— Cybersecurity is the application of technologies to protect data from attack, damage, or unauthorized access, and is a major cyber threat for women due to the revolution in Information Technology. Women are facing a major cyber threat due to the revolution in Information Technology, which has caused them to lose their privacy. Alarmingly, young women and girls in Bangladesh have been victims of cybercrime. The privacy of young girls and women has been put at risk due to the accessibility of social media without knowledge of security measures. Bangladesh has fallen behind in raising youth awareness. The measurement of the present degree of cyber-security awareness is the main emphasis of this research. Moreover, the primary results are according to statistics. The authorities claim that 70% of women experience cyberbullying but do not report it. When the machine learning algorithms were applied to the cybersecurity dataset, the accuracy scores of the SVM, XGBoost, and Catboost methods were 93.6%, 93.7%, and 94.07%, respectively. Our CatBoost classifier produces the best outcome. The precision of CatBoost is 94.87%.**

Keywords*— *Cybersecurity, cyberbullying, cybercrime, XGBoost, Catboost.

I. Introduction

Cybercrime is any criminal conduct carried out by cybercriminals or cyberattacks that exploit or make use of a computer, computer network, or networked device. Women are more frequently the victims of cybercrimes, with 25% of 18 to 24-year-olds reporting being the target of online sexual harassment and 26% reporting being stalked. Cybercrime has escalated due to well-before social-physiological conditions and a lack of statutory protections, with women being the main targets. Social media trends such as spam, rape attacks, and suggestive messages are also on the rise. Women must be aware of the risks of using digital gadgets and sharing information online, which can lead to cybersecurity risks.

Increasing internet users' knowledge and educating them on internet dos and don'ts are key to protecting against these risks. Cybersecurity seeks to maintain the confidentiality, integrity, and availability of data and systems, so children and teenagers need to be taught the rules of the internet and that their social media account passwords are confidential.

II. Cyber Protection & Awareness Methodology

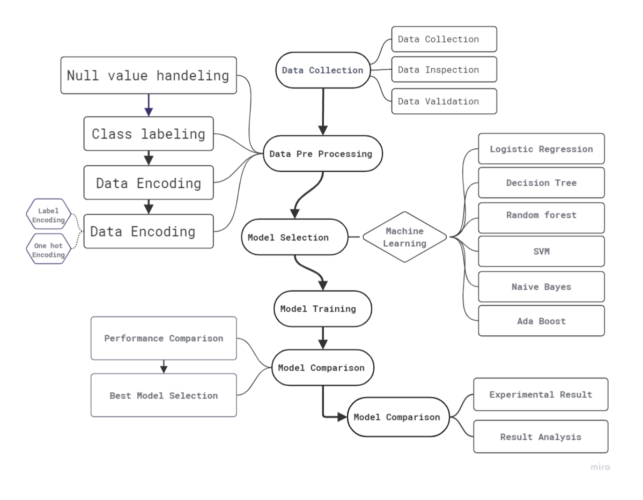

Fig. 1. Research Methodology

Here in this section We will Describe the Research methodology According to the Diagram and flow of the

A. Data Collection

This research recommends machine learning and deep learning for female cyber safety and awareness. Data collection can answer research questions, test theories, and evaluate findings ensures. Accurate data collection protects the study. Structured data collection clarity and relevance.

a. Collection

1. For our research, we manually collected data from schools, colleges, universities, offices, parks, and amusement locations. For this paper, we used employment and age categories to collect data. Cyber awareness and protection systems vary by gender, age, and occupation.

2. We utilized research-based, positive questions on a Google form to interview people.

3. Online data was also collected.

Verify that the information is complete, legal, and ethical. Thus, data must be carefully scrutinized after collection.

b. Data Inspection

Data inspection is necessary for validation and testing since it provides a comprehensive overview of all information. checks our data.

Data validation is a priority. The validation aim is data correctness in the ultimate result.

c. Data Validation

Data validation involves gathering or evaluating data. Validating the original data. Our research's top supervisor validates our data. One of the most crucial data quality checks. After confirmation, data is stored in.csv and in the cloud for security.

B. Data preprocessing

Sometimes some fields for some data, data records are left empty, null values are displayed. So now we talk about this type of problem

1. Null Value Handling

Random forest is used for classification and regression. Random Forest classifies and regresses. Sample averages for categorization and majority vote for regression produce decision trees. It parallelizes continuous and categorical data sets individually. The model's variance decreases but bias remains the same as the forest's trees.

2. Class labelling:

Class labeling is the classification labels for the original dataset's categories. Another name is target field. Data labeling is crucial for supervised ML preprocessing. Supervised learning uses categorize-tagged input and output data to set up future data collecting.

3. Data Encoding:

Processing requires encoding. Encryption secures documents. We must numerically encode independent variable categorical data. This aids algorithm interpretation.

Label Coding: Label encoding translates structured dataset categories into integers for supervised approaches. This article labelled data. Categorized data. Label encoding numerically encodes categories to apply algorithms.

Data was divided 70:30 because one class has a significant range of unique values. This splitter uses KNN and CNN.

C. Model Building:

Machine Learning (ML) including neural network-based deep learning is an important part of Artificial Intelligence (AI) that can be used to build a cyber protective model. For building the model we used

1. Logistic regression:

Logistic regression predicts categorical variables. It predicts discrete or categorical output. True, false, yes, no, 0 or 1, etc.

Logistic regression may use normalization to avoid overfitting in high-dimensional datasets. It forecasts discrete functions only if independent variables are linearly connected to log chances (log(p/(1-p)).

Fitting data to a logit function predicts event likelihood.[1].

2. *KNN*:

K-nearest neighbors (KNN) can be used for classification and regression prediction. It usually compares the data to the goal data. The KNN approach simplifies categorization of fresh data. Lazy learners store the training dataset before learning from it. The model classifies new data using the most similar old data. Distance determines the nearest neighbor.

3. Decision Tree:

DT methods are mainly classified according to their feature values. Each vertex denotes a feature and each edge denotes a value that can have in a sample to classify. Information gain is calculated by comparing the entropy of the dataset.

4. Random Forest:

Random forest is used for classification and regression. Random Forest classifies and regresses. Sample averages for categorization and majority vote for regression produce decision trees. It parallelizes continuous and categorical data sets individually. The model's variance decreases but bias remains the same as the forest's trees grow.

5. SVM:

Random forest is used for classification and regression. Random Forest classifies and regresses. Sample averages for categorization and majority vote for regression produce decision trees. It parallelizes continuous and categorical data sets individually. The model's bias and variance decrease with forest growth.

6. Gaussian Naïve Bayes:

Classification and regression problems use supervised machine learning methods like random forest. Classification and regression problems are solved with Random Forest. It creates decision trees using sample averages for classification and majority vote for regression. It handles continuous and categorical data sets independently and parallelizes. As the forest grows, the model's bias and variance decrease.

7. XGBoost (eXtreme Gradient Boosting)

XGBoost provides an ML-based power system assault detection model that can be trained utilising phasor monitoring sensor data and logs (PMUs). Gradient-boosted trees is open-source and popular. Supervised learning is used for massive dataset categorization and regression.

Memory, infinite dimensions, excellent recognition, and exact detection are needed. XG boost did well in this study. Darts and xgb work. Dart outperforms xgb.

8. K Means Clustering

Centroid-based K-Means clustering determines the dataset's K groupings. This study modelled transient and sustained cyberattacks. For more accurate bogus data identification, use multivariate Gaussian. Because it is unknown, the ideal number of clusters, k, that will maximise separation (distance) must be estimated. This method detected several impersonation assaults.

9. Gradient Boosting

Gradient boosting solves classification and regression issues. For huge and complicated datasets, it delivers forecast speed and accuracy.

Errors greatly impact all machine learning systems. Mistakes matter in machine learning. Bias and variance errors are the main types. Gradient boost reduces model bias. Gradient boost reduces model bias error. Decision Trees are meant to be gradient boosting's fixed base estimator.

10. LGBMC (Light gradient boosting machine classifier)

Decision tree algorithm underpins LGBM. Hence, the decision tree algorithm forms the framework. LGBM is quicker and more accurate than other algorithms. LGBM overfits minimum data easily due to its tendency to do so. LGBMC delivers 91.48% accuracy in this article.

11. Catboost Classifier:

CatBoost boosts categorically. CatBoost is popular because it is simple, reliable, and good with categorical data. Catboost is the latest and most effective categorization method. It solves categorization issues best. Automatic feature categorization uses statistics on categorical and numerical feature combinations to translate categories into numbers. Pre-processing-free CatBoost.

For this investigation, 94.87% accuracy is satisfactory. Depth dependent. CatBoost is the best classifier, whereas clustering is the worst.

D. Model training:

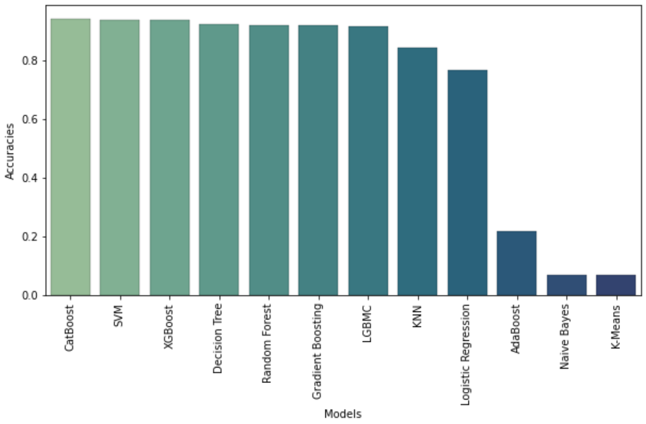

Fig. 2. Comparison of model in terms of accuracy

1. Model Selection:

World's most precious resource is data. Data security requires cyber defence. We protected cyberspace with ML and DL. This article covers cyberprotective ML and DL algorithms. ML is mostly AI and computational statistics. Mathematical optimisation ties this. ML prioritises classification and regression using training data features. DL research is new. Analytical neural networks motivate DL.

2. Model implementation:

ML/DL methods are useful. ML approaches are vital to cyber security's long-term growth. We used CatBoost, SVM, XGBoost, Decision Tree, Random Forest, Gradient Boosting, LGBMC, KNN, Logistic Regression, AdaBoost, NaiveBayes, and K-Means. SVM solves real-world issues. SVM is most accurate. The kernel approach fixes SVM's non-linear decision boundary. Kernel expressions are simple.

3. Model Training:

The Training outcome is visualized in the Fig: 2, it shows an accurate assessment of the accuracy in terms of accuracy, The training process was evaluated on the metric of accuracy. ML/DL approaches help. Cybersecurity's future depends on ML methods. CatBoost, SVM, XGBoost, Decision Tree, Random Forest, Gradient Boosting, LGBMC, KNN, Logistic Regression, AdaBoost, NaiveBayes, and K-Means. SVM handles problems accurately. Kernels fix SVM's non-linear decision boundary. Simple kernel expressions.

CatBoost model metrics were iteration = 100, learning rate = 0.1, depth = 9, eval metric = "AUC," and random speed = 42. Iterations slow learning. Iteration and dataset size effect learning rate. 9-depth training expedited. 94.07% correct CatBoost.

SVM used kernel = "rbf," gamma = "0.9," and C = "1.0" parameters. Gamma controls the model's support vector samples' low and high values. Gamma is distant when low and close when high. C balances training example categorization and decision function margin maximisation. Higher Cs narrow margins, whereas lower Cs widen them. RBF kernel. 93.6% SVM accuracy. Data is correct. XGBoost used booster='dart', learning rate=0.11, max depth=7, and n estimators=200. DART booster. Boosters give erroneous outcomes without training data. Learning rate optimises results. Learning rate 1.00 and 0.01 are better than the prior optimum. Hence, faster computation does not mean best. Slower calculation is ideal. XGBoost's 0.11 learning rate yields the greatest results. n estimators=200 and max depth=7 worked best. 93.7% correct XGBoost.

94.07% was CatBoost's best.

4. Model Comparison:

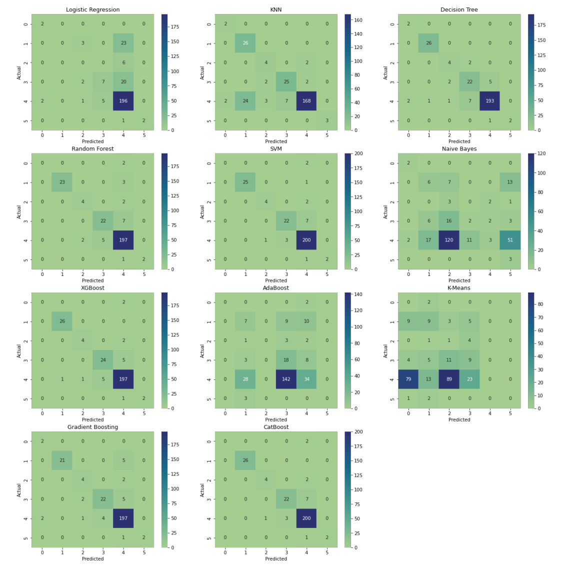

Fig: 3 All Confusion matrix Ascending order

Here shown in 4 as a grid of heatmaps, The top model performance of ML algorithms in the dataset is CatBoost, SVM, and XGBoost, The Figure further shows the rate of prediction to further back up our view. while Naive Bayes and K-means give the worst performance. The confusion matrix is used to visualize the performance of algorithms, with four results being true positives, false negatives, false positives, and true negatives. The highest value for CatBoost and SVM is 200, while the worst result is K-Means.

1. Catboost:

CatBoost is an ensemble method that helps to reduce overfitting and improve accuracy. It is an alternative to XGBoost, with an accuracy of 94.07%. It handles categorical features and has a simpler hyperparameter tuning process. The learning rate is in every iteration, and the true positive value is 200. It also has a higher mutation rate.

2. SVM:

SVM is a supervised algorithm used for classification and regression. It uses the hyperparameter C to create the best line or decision boundary for n-dimensional classification. The SVM kernel is used as the Kernel converts non-linear to linear. Gamma values are used to increase the efficiency of the model and reduce the point around it. The true positive value is 200, which is correctly classified by the model. However, 4 negative class data is incorrectly classified.

3. XGBoost:

Extreme Gradient Boosting (xgboost) is a more structured algorithm that can compute parallel computation in a single machine. It has both linear model solver and tree learning algorithms and is best for learning_rate=0.11, maxim_depth=7, and n_estimators=200 parameters. The learning rate must be set as low as possible to achieve the best optimum result. The true positive value of the model is 197, and 7 negative class data is incorrectly classified. However, nAdaboost, naive Bayes, and k-means are not capable of achieving a high level of accuracy due to their clustering algorithms. Clustering is unsupervised learning and only works with one set of input data.

E. Result Analysis:

TABLE I. THE BEST PERFORMING ALGORITHMS (SORTED BY ACCURACY)

Algorithm	Accuracy	F1 Score
CatBoost	94.07%	94%
SVM	93.71%	94%
XGBoost	93.70%	93%
Decision tree	92.2%	93%
Random forest	91.85%	92%
Gradient boosting	91.85%	92%
LGBMC	91.48%	91%
KNN	84.44%	84%
Logistic regression	76.66%	77%
Adaboost	21.12%	22%
Naive Bayes	7.3%	7%
K Means	7.3%	7%

The accuracy scores of SVM, XGBoost, and Catboost algorithms were 93.6%, 93.7%, and 94.07%, respectively when applied to the cybersecurity dataset. As summarized in the Table 1. These algorithms have been successful due to their capacity to deal with high-dimensional and non-linear data, their ability to manage large volumes of data, and their use of "RBF" kernels and "dart" boosters. The AdaBoost, Naive Bayes, and K-means algorithms had the worst performance on the counterterrorism dataset. AdaBoost is an example of ensemble learning, while Naïve Bayes classifier is a probabilistic method that clusters data into groups, while K-Means is an unsupervised learning method. In-depth study of the findings in their entirety can help guide decision-making for the foreseeable future.

III. LITERATURE REVIEW

It explores deep autoencoders, constrained Boltzmann machines, recurrent neural networks, generative adversarial networks, and other DL methods for cybersecurity, including spam, insider threats, network breaches, and fake data injection. [1].

This article presents a collaborative deep-learning technique for recognizing malware-infected files and counterfeit software in IoT networks, using tokenization and weighting characteristics and deep neural networks to detect software theft through source code copying with a 97.46% success rate. [2]

Article covers federated deep learning techniques for IoT apps, including security and privacy systems, experimental examination of three deep learning algorithms, federated learning with blockchain, and malware/intrusion detection systems achieving 99.20% accuracy, with the goal of sharing knowledge on networked deep learning approaches using cybersecurity tools.[3].

Paper proposes cyber analytics using ML and DM methods for intrusion detection, providing an overview of each method and utilizing well-known cyber datasets, addressing the complexity and challenges of using these techniques for cybersecurity.[4]

It analyzes security weaknesses, risks, and implications in the automation industry, including unintentional and malicious attacks resulting in economic and financial losses, and discusses ways to increase robotic system security, including adding security measures. [5].

This paper develops a neural network-reinforcement learning system to detect online phishing attacks by automatically adding fresh emails to the offline dataset. A novel strategy is proposed to find new phishing methods in the dataset. The method handles zero-day attacks with 98.63% accuracy, 98.19% TNR, and 99.07% TPR. FNR and FPR are also low at 0.93% and 1.81%.[7]

The paper uses a multi-layer generative model to identify adware as "opcode sequences" and shows that deep belief networks (DBN) are better at malware detection than decision trees, support vector machines, and baseline models using the k-nearest neighbor technique as classifiers. [8].

Study examines how artificial intelligence (AI) applications and technologies affect social media, highlighting their benefits for user and proprietor privacy and showing that businesses using AI-based social media marketing platforms see a 10% increase in profits, decreased expenditures, and improved productivity and logistical networks.[9].

A revolutionary client-side data machine learning-based anti-phishing technology that recognizes 19 unique features directly from website URLs and raw code achieves an overall detection accuracy of 99.09% and a high true positive rate of 99.39% for phishing websites compared to older methods. [10].

This study's machine-learning anti-phishing approach exclusively collects client-side data. It detected 19 unique features taken from URLs and raw code of various webpages. The document focused on intrusion monitoring. [11].

In this paper, basically, they apply neural network-based DL approaches to cyber security applications to detect new and different types of malware and zero-day attacks , which also included spam, insider threats, network intrusions, false data injection, and malicious domain names used by botnets[12].

The paper explores the potential threats posed by AI applications and examines various AI strategies for combating cyberattacks in light of the rapid evolution of information and communication technologies and emerging cybersecurity threats. [13].

The IntruDTree machine-learning security model provides accurate forecasting with lower computational complexity compared to other established techniques like k-nearest neighbor algorithm, logistic regression, support vector machines, and naïve Bayes classifier. [14].

AI techniques, including support vector machines (SVM) and random forests (RF), were used to detect cybersecurity intrusions in IoT environments due to their high detection accuracy, with a focus on researching popular AI trends in defense and innovative solutions. [15].

This paper examines the benefits and drawbacks of using AI in the evolving landscape of cyber security, as the number of applications and risks increase. The focus is on exploring the potential uses of AI to address related problems and risks.[16].

With IoT and linked devices, cyber security experts face new hurdles.Measurement of cybersecurity threats in IoT is superior to state-of-the-art techniques, with an accuracy rate of 97.46%.[17].

The result of this study offers a comprehensive and in-depth examination of "AI-driven Cybersecurity," which may make computing processes more automatic and intelligent than current security measures. [18].

Centralized digital groups make it possible for people, services, and devices to communicate safely, but the digital transformation is risky. With the aid of AI tools and data-driven solutions, certain hacking problems can be resolved[19].

IoT is one of the fastest-growing disciplines in technology, with an expected 50 billion devices by 2020. ML/DL approaches are essential for converting IoT system security from device-to-device communication to intelligence-based security mechanisms [20].

It covers a survey of smart grid technologies, power industry practices, and standards, solutions that address cyber security issues, a review of existing CPS testbeds for cyber security research, and unsolved cyber security problems[21].

This paper reviews that cyber security and information security do not totally correlate. cyber security is more secure than information security. Because cyber security secure not only information but also other assets [22].

Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from misaligning de jure from de facto property rights.[23]

This paper focused on the importance of standards in cyber defense, the architecture of cyber security framework, standardization challenges, national strategies to secure cyberspace. [24].

The three major applications discussed in this paper are cyber-physical security, communication security, and privacy. The article examines current game-theoretic approaches for cyber security and privacy problems.[25].

This paper covers cybercrimes including privacy, e-chats, online grooming, sexual misbehavior, bullying, hacking, spoofing, cyberstalking, online abuse, obscene materials and sexual defamation, blackmailing, misrepresentation, financial gain, and espionage, with women and girls being the main victims. [26].

The primary goal of the research in this paper is to use smartphone technology to look into people's levels of knowledge and behavior regarding cyber security. level of awareness and behavior in cyber security, using smartphones were discovered and discussed[27].

A first phishing attack, a knowledge transfer using a mixed approach, and a second phishing attack with different content made up the study's three phases. Only Thai employees working in the financial services industry in Thailand were the focus of this study [28].

The current study state and practices in cybersecurity knowledge for kids are examined in this review article, with a particular emphasis on privacy, cyberbullying, and exposure to inappropriate material and erotica [29].

In order to promote cyber-security practices, level of awareness, and incident reporting, this paper examines the current state of cyber-security awareness in Saudi Arabia. [30].

IV. CONCLUSION AND FUTURE WORK:

In conclusion, it is abundantly clear that women are the primary targets of cyberbullying, and the general public awareness of cyber-security needs to also be vastly increased in order to effectively defend against the rapidly rising incidence of cyberbullying. Data Collection is a process where information is gathered and evaluated on a particular area of interest. Basically, We collect our data manually, online form based, and from online sources. After collecting data it goes through data collection, data inspection, and data validation phase, and then in the pre-processing process, it again goes through null value handling, class labeling, and data encoding phase. For the model building process we used logistic relations, knn, decision tree, random forest, SVM, gaussian naive bayes, xG boost, k means clustering, gradient boosting, LGBMC, and lastly Cat boost classifier. After model selection, we train the model and also used model comparison for showing results in a clear and understandable way.

The best result gives us a Cat boost classifier. Which accuracy is 94.87%. Because this is sufficient for this study. Depending on the depth. If we compare catboost to other classifiers, it comes in first, and k means clustering comes in worst. k means is not clustering data. In future study, we want to work with large datasets and works on the proposed data so that it goes up to the future.

V. References

vol. 21, no. 1, pp. 115–158, Feb. 2022, doi: 10.1007/S10207-021-00545-8.

[6] M. Alazab, V. Ravi, S. Srinivasan, S. Venkatraman, and Q.-V. Pham, "Deep Learning for Cyber Security Applications: A Comprehensive Survey," 2021, doi: 10.36227/techrxiv.16748161.

[7] S. Smadi, N. Aslam, L. Z.-D. S. Systems, and undefined 2018, "Detection of online phishing email using dynamic evolving neural network based on reinforcement learning," *Elsevier*, 2018, doi: 10.1016/j.dss.2018.01.001.

[8] D. Yuxin and Z. Siyi, "Malware detection based on deep learning algorithm," *Neural Comput Appl*, vol. 31, no. 2, pp. 461–472, Feb. 2019, doi: 10.1007/S00521-017-3077-6.

[9] L. A.-G.-S. E. and Innovation and undefined 2021, "Towards adopting AI techniques for monitoring social media activities," *search.proquest.com*, Accessed: Jan. 10, 2023. [Online]. Available: https://search.proquest.com/openview/4be50c31fab811a682bcd9fc6ffb4a34/1?pq-origsite=gscholar&cbl=5567716

[10] A. K. Jain and B. B. Gupta, "Towards detection of phishing websites on client-side using machine learning based approach," *Telecommun Syst*, vol. 68, no. 4, pp. 687–700, Aug. 2018, doi: 10.1007/S11235-017-0414-0.

[11] Y. Xin *et al.*, "Machine learning and deep learning methods for cybersecurity," *ieeexplore.ieee.org*, Accessed: Jan. 10, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8359287/

[12] D. Berman, A. Buczak, J. Chavis, C. C.-Information, and undefined 2019, "A survey of deep learning methods for cyber security," *mdpi.com*, doi: 10.3390/info10040122.

[13] T. Truong, Q. Diep, I. Z.- Symmetry, and undefined 2020, "Artificial intelligence in the cyber domain: Offense and defense," *mdpi.com*, doi: 10.3390/sym12030410.

[14] I. Sarker, Y. Abushark, F. Alsolami, A. K.-Symmetry, and undefined 2020, "Intrudtree: a machine learning based cyber security intrusion detection model," *mdpi.com*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.mdpi.com/708786

[15] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *mdpi.com*, 2022, doi: 10.3390/electronics11020198.

[16] "Artificial Intelligence in Cyber Security - A Review... - Google Scholar." https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Artificial+Intelligence+in+Cyber+Security+-+A+Review++Jenis+Nilkanth+Welukar%2C+Gagan+Prashant+Bajoria&btnG= (accessed Jan. 10, 2023).

[17] "ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY - Google Scholar." https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=+ARTIFICIAL+INTELLIGENCE+TECHNIQUES+FOR+CYBER+SECURITY+&btnG= (accessed Jan. 10, 2023).

[18] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Comput Sci*, vol. 2, no. 3, May 2021, doi: 10.1007/S42979-021-00557-0.

[19] I. M.-I. J. O. INNOVATIONS and undefined 2020, "ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE," *researchgate.net*, vol. 7, 2020, Accessed: Jan. 10, 2023. [Online]. Available: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887583_ARTIFICIAL_INTELLIGENCE_FOR_CYBERSECURITY_A_SYSTEMATIC_MAPPING_OF_LITERATURE/links/61169e870c2bfa282a41f607/ARTIFICIAL-INTELLIGENCE-FOR-CYBERSECURITY-A-SYSTEMATIC-MAPPING-OF-LITERATURE.pdf

[20] M. Al-Garadi, A. Mohamed, A. A.-A.-… S. & Tutorials, and undefined 2020, "A survey of machine and deep learning methods for internet of things (IoT) security," *ieeexplore.ieee.org*, Accessed: Jan. 10, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9072101/

[21] C. Sun, A. Hahn, & C. L.-I. J. of E. P., and undefined 2018, "Cyber security of a power grid: State-of-the-art," *Elsevier*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061517328946

[22] R. von Solms, J. V. N. & security, and undefined 2013, "From information security to cyber security," *Elsevier*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404813000801

[23] D. Craigen, N. Diakun-Thibault, R. P.-T. Innovation, and undefined 2014, "Defining cybersecurity," *timreview.ca*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.timreview.ca/article/835

[24] J. Srinivas, A. Das, N. K.-F. generation computer systems, and undefined 2019, "Government regulations in cyber security: Framework, standards and recommendations," *Elsevier*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18316753

[25] C. T. Do *et al.*, "Game theory for cyber security and privacy," *ACM Comput Surv*, vol. 50, no. 2, pp. 30–37, May 2017, doi: 10.1145/3057268.

[26] D. Verma, V. Verma, A. Pal, and D. Verma, "Identification and Mitigation of Cyber Crimes against Women in India," *researchgate.net*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.researchgate.net/profile/Deepak-Verma-19/publication/360306507_Identification_and_Mitigation_of_Cyber_Crimes_against_Women_in_India/links/626ed94ac42af62fe2e545f9/Identification-and-Mitigation-of-Cyber-Crimes-against-Women-in-India.pdf

[27] P. Mai, A. T.-A. Polytech. Hung, and undefined 2021, "Cyber Security Awareness and behavior of youth in

smartphone usage: A comparative study between university students in Hungary and Vietnam," *researchgate.net*, vol. 18, no. 8, pp. 2021–67, doi: 10.12700/APH.18.8.2021.8.4.

[28] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks," *Educ Inf Technol (Dordr)*, vol. 27, no. 4, pp. 4729–4752, May 2022, doi: 10.1007/S10639-021-10806-7.

[29] F. Quayyum, D. Cruzes, L. J.-I. J. of Child, and undefined 2021, "Cybersecurity awareness for children: A systematic literature review," *Elsevier*, Accessed: Jan. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212868921000581

[30] A. A.- Heliyon and undefined 2021, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Elsevier*, Accessed: Jan. 10, 2023. [Online].