Volume 11, Issue 2, February – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

Machine Learning-Based Password Vulnerability Detection and Strength Assessment System for Consumer Wi-Fi Routers

Amaka Eugenia Ngozi[1*]; Okpalla Chidimma Lilian[2]; Ezea Jonathan Ikechukwu[3]; Ibeneme-Sabinus Ifeoma Livina[4]; Nworuh Godwinner Emeka[5]; Atomatofa Emmanuel Oghenero[6]; Gloria Ngozi Ezeh[7]; Ugbor Ihechiluru Chinwe[8]; A. A. Galadima[9]

[1,4,5,6,8,9]Department of Cybersecurity, School of Information and Communication Technology, Federal University of Technology, Owerri, Imo State, Nigeria.
[2]Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Owerri, Imo State, Nigeria.
[3]Department of Information Technology, First Bank Nigeria Ltd, 35 Marina Lagos.
[7]Department of Information Technology, School of Information and Communication Technology, Federal University of Technology, Owerri, Imo State, Nigeria.

Corresponding Author: Amaka Eugenia Ngozi[1*]

Publication Date: 2026/03/02

Abstract: The improvement of consumer-grade Wi-fi routers greatly ascertained wide access to the global internet, though with numerous security challenges. Thus, existing research evidence confirmed that many users maintain weak passwords, while routers firmware were left outdated and lots of security misconfiguration settings. However, these security flaws were exploited by various attack mechanisms such as brute force attacks, phishing attacks among others, leading to invasion of user's privacy and campaign launch for distributed denial-of-service (DDoS). Notably, this research developed Secured Router Security Assessment System (SRSAS), applying a machine learning mechanism for evaluating Wi-Fi router password authentications. The system, however, classified the password authentication into three different categories such as Weak, Good and Strong. Similarly, the system used 60,000 datasets of labelled passwords to train the models. Hence, improving the reliability of the system incorporated entropy analysis, checking against known data breaches and generating suggestions to the users for stronger passwords. The results show that the system performs well in predicting password strength and in offering realistic advice for improving router security. The work therefore contributes both academically and practically: it demonstrates how machine learning can be applied to real-world network security and gives everyday users a tool for improving the safety of their home routers.

Keywords: *Router Security, Wi-Fi Vulnerability, Password Strength, Machine Learning, Entropy Analysis.*

How to Cite: Amaka Eugenia Ngozi; Okpalla Chidimma Lilian; Ezea Jonathan Ikechukwu; Ibeneme-Sabinus Ifeoma Livina; Nworuh Godwinner Emeka; Atomatofa Emmanuel Oghenero; Gloria Ngozi Ezeh; Ugbor Ihechiluru Chinwe; A. A. Galadima (2026) Machine Learning-Based Password Vulnerability Detection and Strength Assessment System for Consumer Wi-Fi Routers. *International Journal of Innovative Science and Research Technology,* 11(2), 2238-2245. https://doi.org/10.38124/ijisrt/26feb804

I. INTRODUCTION

Wi-Fi routers are ubiquitous gateways that enable internet access for households, small offices and a rapidly growing ecosystem of IoT devices and cloud services. As device diversity and online dependency increased between 2023–2025, routers assumed an ever-larger role in holding and forwarding sensitive personal and organisational data [3 & 25]. Concurrently, empirical studies show that consumer-grade routers continue to exhibit persistent weaknesses attributable to unchanged default credentials, weak user passwords, misconfiguration, delayed firmware updates and hidden firmware backdoors, noting conditions that adversaries routinely exploit with brute-force, dictionary and credential-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

stuffing attacks and, more recently, with AI-assisted cracking tools that significantly accelerate and tailor guessing strategies to user behaviour [4,10 & 24]. These vulnerabilities convert otherwise benign home routers into launching points for identity theft, network compromise and large-scale DDoS campaigns that can cascade into wider infrastructure impacts [15].

Basically, the major challenge is not limited to a static password validator satisfied by users to produce low password entropy with high prediction of vulnerabilities to modern attack workflows incorporating breach-corpus lookups [23]. Available research evidence claimed that a substantial fraction of router incidents was originated from weak credentials and user's behaviors to prioritize convenience over resilience[14]. Hence, the mitigative technicalities must adequately correspond with the user-cantered design for effective security measures [6 & 11]. Moreso, the vendor and policy shortfalls such as inconsistent defaults, slow patch cycles, and insufficient security guidance to users, systematically reduced the baseline security for consumer's routers [9 & 27]. Additionally, the routers have invariably been transformed from defensive gateways to persistent and scalable attack vectors with a wider indication of escalating the overall attack surface[1,8,17 & 28].

An effective practical data-driven router using approaches presented by Machine Learning (ML) and hybrid ML-heuristic was adopted to close the identified gaps [3,11 & 12]. Hence, the ML models extracted structural features of the password strings and correlated them with the signals of the breached-password and heuristics crack-time, producing a real-time contextual and personalized recommendations, with the capabilities of outperforming simple rule-checks [5,7 &18]. Although, the recent experimental works of [17,22 & 24], demonstrated that classifiers such as random forest, gradient boosting among others combined with both entropy and breach-lookup modules to increase detection accuracy for weak credentials to quickly flag off rejection with a suggestion of automated stronger password [6,7 & 21]. Nevertheless, an enhanced system design like k-anonymity for privacy protection is required to avoid new vulnerability's introduction during telemetry, preserving usability for users' acceptance and adoption of stronger authentication practices [19,20 & 21].

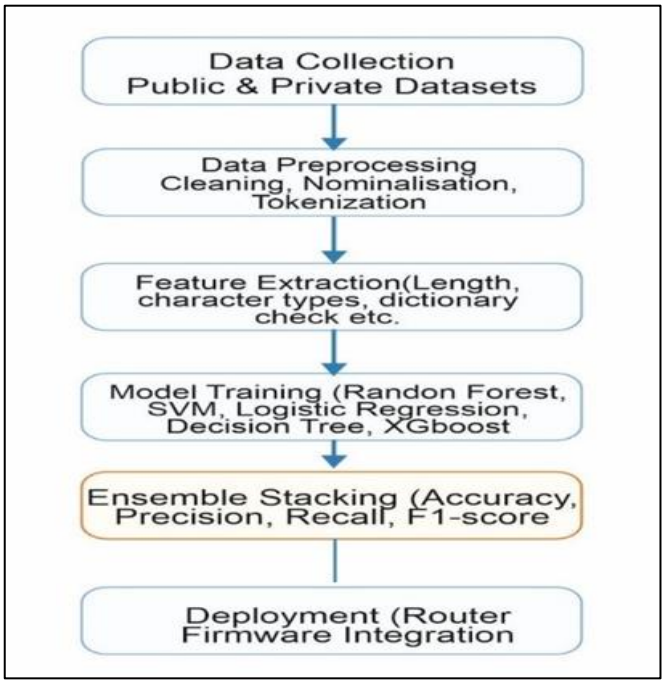
However, this research developed a Secured Router Security Assessment System (SRSAS), integrating an entropy analysis together with breach-database monitoring and a supervised ML classifier. The ML classifier was designed to perform three major roles not limited to password strength evaluation in a realistic router content. effectively surfaces the previously compromised credentials and provides very clear instructions for non-technical users to understand and act accordingly. Perhaps, the contribution of this research was to improve on low-entropy and exposing the breached passwords with rule-based validator's baseline. Though, the research further provided an embedded pathway for lightweight inference into a router setup flow to raise baseline security across for home deployment without the user's knowledge advancement.

Hence, the research's model was validated by assembling a diverse labelled dataset, extracting multi-level features and evaluating multiple classifiers with both stratified training, testing and maximizing generalization using ensemble stacking. Evaluation metrics include accuracy, precision/recall, F1, estimated crack-time distributions, and breach-detection rates; deployment scenarios consider on-device inference constraints, bandwidth/privacy trade-offs for remote breach checks, and human-factors aspects of recommendation phrasing and interruption timing. Empirical results and comparative analysis situate the proposed system within the rapidly evolving 2023–2025 threat landscape and provide concrete guidance for router vendors, ISPs and policymakers seeking to improve minimum security baselines for consumer devices [1,3,12,13 & 26]. Nonetheless, bridging adversary-aware threat modelling with user-centred, ML-driven detection and remediation, this study aims to reduce successful brute-force and credential-stuffing incidents, lower the prevalence of default/weak credentials in the field, and inform firmware and policy interventions that embed stronger, adaptive password practices into the consumer router lifecycle.

II. METHODOLOGY

➢ *Conceptual Framework*

Figure 1 presents the conceptual framework of the proposed Machine Learning-Based Password Vulnerability Detection and Strength Assessment System for Consumer Wi-Fi Routers. The framework illustrates how machine learning techniques are employed to identify, evaluate, and mitigate password-related vulnerabilities in consumer-grade Wi-Fi routers. Each component of the framework represents a critical stage in the end-to-end process of securing router authentication against modern cyber threats.



ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

Fig 1 Conceptual Framework for Password Vulnerability Detection and Strength Assessment System for Consumer Wi-Fi Routers

➢ *Data Collection*

The dataset collected for this research was from Kaggle password strength, available at https: www.mendeley.com/dataset/bhavikbb/password-strenght-classifier-dataset. However, RockYou and Have I Been Pwned (HIBP) password were included in the collected datasets. Similarly, we generated synthetic strong passwords used in balancing the datasets and this represented secure user practices. Furthermore, queries filtering was used to select a total number of 50,000 password entries, maintaining categorically the password length, frequency distribution and uniqueness to limit the over-representation of common weak passwords.

➢ *Data Preprocessing*

The collected data was pre-processed for quality improvement and consistency. The duplicated passwords were removed to avoid bias and missing values were also handled effectively by discarding incomplete rows. We further applied normalization techniques to adequately standardize password formats, with utmost assurance of a consistent treatment of both upper and lowercase entries. Then, characters were separated using tokenization into analysable units such as symbols, digits and alphabets.

➢ *Feature Extraction*

The transformation of raw passwords into measurable attributes was done by machine learning and extracted features were password length, diversity of character type, entropy and dictionary word checks, identifying predictable patterns. Thus, the input vectors for classification were formed using extracted features to enable the model to effectively distinguish between weak, medium and stronger passwords, noting the greater accuracy.

➢ *Ensemble Stacking*

Improving the classification accuracy demanded for the implementation of an ensemble stacking techniques. This approach combined the multiple models' predictions, regarded as base learners, passing them to meta-learners to produce the final classification. The strengths of the model as recorded were Random Forest and Decision Tree, while the weaknesses of the model recorded were Logistic Regression and XGBoost. Similarly, model's evaluation metrics were accuracy, precision, recall and F1-score, measuring the balance between weak password detection and false positive avoidance.

➢ *Deployment*

The deployment of the trained ensemble model was done within the environment of a simulated router firmware to evaluate the effectiveness of the model in a real-world application. Hence, deployment process involved the integration of the inference engine of the machine learning into the interface of the router's password configuration, evaluating the strengths of the password in real-time to provide the user with instant feedback. Moreso, the system performance, user trends and attack pattern evolvement were visualized through the model's connection to PowerBI dashboard.

III. RESULTS AND DISCUSSION

The password strength evaluation system implementation required both hardware and software resources not limited to a minimal capacity of an intel corei5 processor, with 8GB RAM and 500GB of hard disk storage. On the other hand, the hardware specifications handled dataset and the processes of the model training, achieving the optimal performance for accelerated computations with 16 Gb RAM, 1TB storage and a CUDA-enabled GPU. Additionally, the software specifications included Python programming language, Scikit-learn, Pandas, NumPy, Seaborn, matplotlib, and XGBoost. Though, the model's IDEs were jupyter notebook and visual studio code, while the backend integration was provided by FastAPI, ETL tool was Apache NiFi, visualization was handled by PowerBI with matplotlib and finally SQLite was used to store the model's results. The design of the model was cross-platform with a compatibility of Windows and Linux environments.

➢ *Pre-Test of the Existing Models*

The pre-test of the existing validation methods of the static password as shown on Table 1 was conducted for Logistic Regression, Decision Tree, Random Forest and Support Vector Machine. Obviously, among all existing models tested, it was Support Vector Machine that had a baseline performance metric of 23.95% for accuracy, 9% for precision, 23.95% for recall and 9.65% for F1-Score. This shows that the model has a very poor hyperparameter configuration due to its limited feature set. Contrarily, the K-Nearest Neighbours had the best performance with 86.30% accuracy, 86.34% precision, 86.30% recall and 86.05% F1-Score. This demonstrated a very high capability for password strength patterns to be captured even with basic features. However, these results demonstrated a severe limitation of machine learning models without ensuring the availability of sophisticated feature extraction and adequate data pre-processing. The findings gotten from this baseline evaluation formed the basis for the development of the enhanced models. This enhanced model incorporated an advanced feature extraction technique not limited to entropy calculation character distribution analysis for improvement of clarification accuracy and reliability.

Table 1 Pre-Test Result

Pretest Results (intentionally low):

	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.7555	0.774882	0.7555	0.713147
Decision Tree	0.8490	0.850710	0.8490	0.845088
Random Forest	0.8435	0.845919	0.8435	0.838720
SVM	0.2395	0.099971	0.2395	0.096516
KNN	0.8630	0.863399	0.8630	0.860523

PS C:\Users\USER\Desktop\ofodum>

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

➢ *Post-test Evaluation of the Enhanced Model*

A post-test conducted assessed the model's performance to ascertain the reliability of the model's effectiveness. The results obtained clearly highlighted the performances of 99.70%, 99.70% precision, 99.70% for recall, and 99,67% F1-Score for Logistic Regression analysis. This, perhaps, shows that the model can effectively handle complex classification tasks distinguishing between weak and strong passwords. The model's consistency of high precision, recall and F1-Score, indicated correctly that the model classified a very vast majority instances, maintaining both false positive and false negatives imbalances.

Nevertheless, the exceptional results obtained from the Decision Tree and Random Forest emerged the best model's performance with 99.95% across all metrics such as accuracy, precision, recall and F1-Score, Similarly, the SVM and K-Nearest Neighbours performance of 99.55% across all metrics such as accuracy, precision, recall and F1-Score. Similarly, the SVM and K-Nearest Neighbour's performance of 99.55% and 99.55% respectively for accuracy, while 99.55% was obtained for other metrics of SVM, and 99.75% was also obtained for other metrics of K-Nearest Neighbours as the case maybe. However, when these results are compared to the results of both Random Forest and Decision Tree, this indicates that

F1-Score is slightly lower, showing a marginal decrease in precision and recall balances.

Thus, the confusion matrix as presented in Fig 1 provided a deeper insight in the performance classification of each model. Notably, Logistic Regression obtained correctly 600 classified instances of class 0 with 191 misclassifications and identified 625 instances of class1 with 124 misclassifications. Thus, the Decision Tree ascertained an improved performance of the model with 646 predictions for class 0 and 105 miscalculations, 665 predictions for class 1 and 84 miscalculations. The Random Forest had 710 predictions for class 0 and 41 miscalculations, 700 predictions for class 1 and 49 miscalculations. Moreso, the SVM and KNN had classification patterns of 710 and 702 predictions respectively for class 0, and 699 prediction each for class 1.

However, the indication of the overall model evaluation shows that RF and DT were optimally the choices for evaluating password strength. The combination of these models is robust and could leverage the strengths of multiple model's high performance to create a reliable and accurate password security assessment system. This, however, shows that the improvement of pre-test analysis necessitated a comprehensive feature extraction in addition to a sophisticated approach for machine learning in building an effective security model. Thus, Wi-Fi Security Analyzer interface was used to evaluate the real-time strength for the password model simulated. The testing was focused on different strength categories assessing the ability of the model with accurate classification in real-world scenarios, providing the users with suitable feedback. Fig 2 presented the three distinct test cases that demonstrated the model's ability to effectively differentiate between the three parameters such as weak, medium, and strong passwords with the aid of an advanced feature analysis and machine classifications.

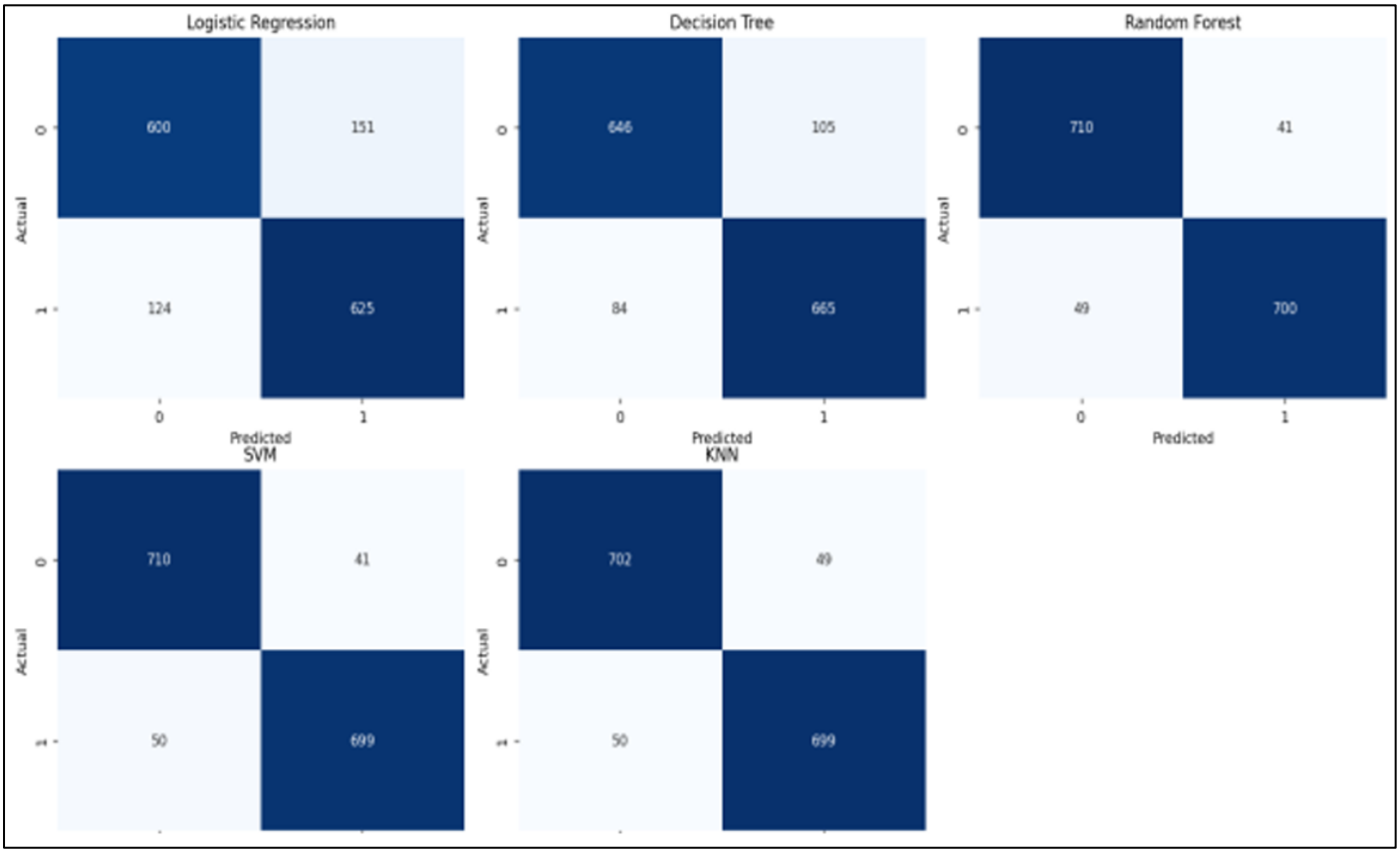


Fig 2 Model's Confusion Metrics

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

A weak password was examined at the first phase as shown on Figure 3 where a four-character password consisting of four dots was evaluated. Hence, a warning of red progress ring, accompanied by a prominent high risk and an incomplete notification was displayed. A critical security metrics, exhibiting an entropy of 24.35 bits, with an indication of a low randomness and predictability was revealed by the detailed analysis panel. This had only 0.02 seconds for estimated crack time and instantly demonstrated a compromised password through a brute force attack. However, the composition of the character analysis showed four-character length, consisting of one-uppercase letter, one digit and two symbols were insufficient to enhance the security measure due to the limited length. A speedy recommendation was provided to increase the password length to a minimum of 12 characters, incorporating lowercase letters to the existing character composition for improved diversity.

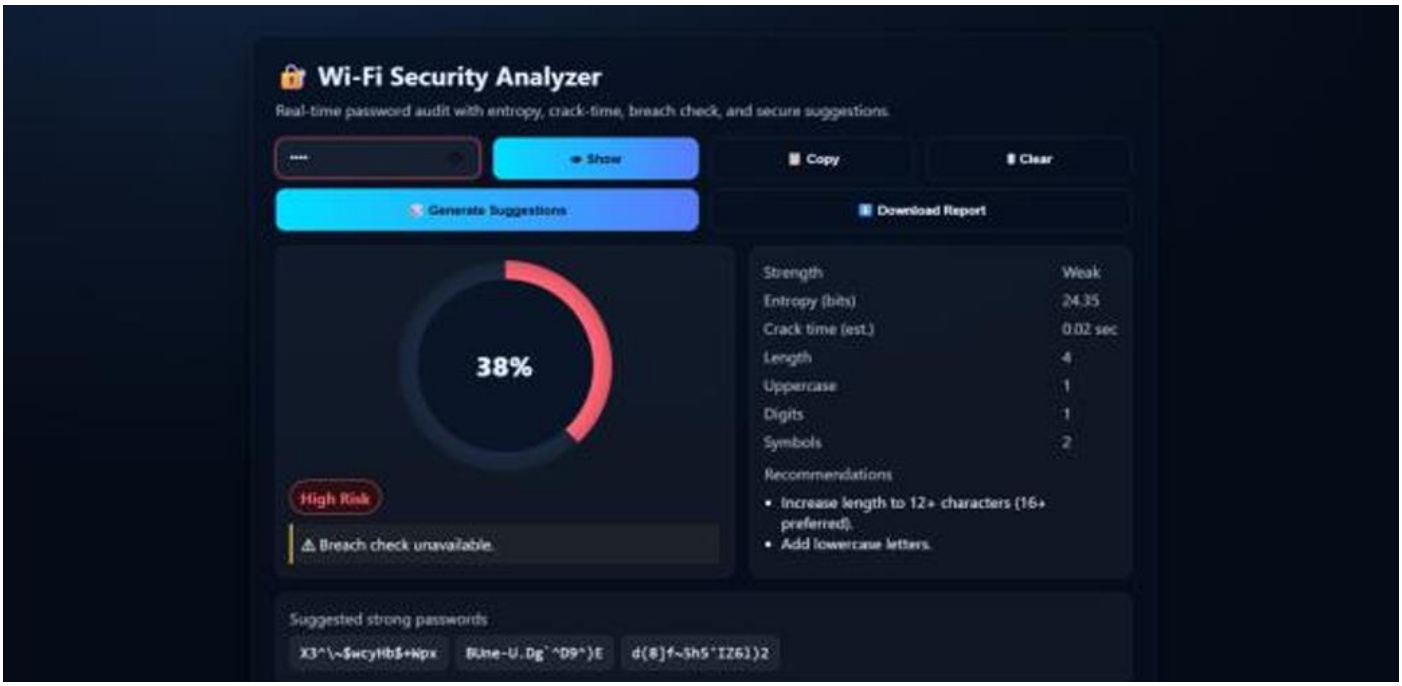


Fig 3 Weak Password

Meanwhile, the second test as displayed on Figure 4 demonstrated a strong password from the model's evaluation. Though, this had a longer sequence of dots at the interface. The results as displayed by the circular strength indicator showed a complete green ring of 100% strength, accompanied with assurances of low-risk classification.

Fig 4 Strong Password

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

The comprehensive analysis also revealed an exceptional security characteristic of an adequate achievement with an entropy of 91.76 bits. This indicates an extremely high randomness and unpredictability, with high resistance to various attack mechanisms. Notably, the estimated crack time extension was approximately 133547028846.36 years, invariably, minimized the password attack scenarios. The character composition maintained a length of 14 characters, incorporating three-uppercase letters, one-digit and six-symbols to create a complex pattern that would not be easy to crack or guess. The model's recommendation was that the password creation was very good with a suggestion to be stored in a trusted password manager.

Furthermore, the third case scenario was a medium-strength password as depicted on Figure 5. In this case, an orange progress ring of 71% was displayed by circular strength indicator, with a medium risk warning classification. Similarly, the detailed metrics of 45.88 bits were displayed, a moderate security range with vulnerabilities,

The estimated crack time of 18,01 hours suggests a potential compromise by more sophisticated or persistent adversaries. The character composition analysis of seven-character lengths, consisting of one-upper letter, one-digit and four-symbols chosen demonstrated a failure in optimal security standards. The same recommendation of twelve-characters minimum was made available as in the first test scenarios.

Fig 5 Medium-Strength Password

However, these three test case scenarios collectively demonstrated the model's sophisticated abilities, performing nuanced password strength classifications in real-time. Moreso, the successful interface translation of complex analysis of the machine learning into intuitive visual feedback using color-coded circular indicators, risk-warning labels, and a comprehensive metrics display was achieved. The model, also, provided actionable recommendations regarding the password challenges, and possible mitigate measures, enhancing the character compositions. Most importantly, the real-time analysis ensured timely feedback to users at the processes of password creation. The entropy calculation integration, estimation of crack-time, analysis of character composition and breach checking created multiple dimensions for a holistic security assessment of password vulnerabilities. This approach however, ascertained the readiness of the model for deployment in router firmware environments for users' access and consumption.

IV. CONCLUSION

The research's goal was achieved by developing a hybrid pipeline with a combination of a supervised machine learning classifiers, entropy-based heuristics and privacy-preserving breach lookups to effectively produce an adversary-awareness and credential context-sensitivity assessment. Hence, this great achievement was done through feature engineering, incorporating length metrics, diversity of character-class, patterns of n-gram, dictionary checks and signals of breach-frequency. Notably, this achievement was also credited to the following models trained: Logistic Regression, Random Forest, and Support Vector Machines on a curated, and labelled corpus for effective predictive performance.

Interestingly, the Logistic Regression accuracy score of 95% demonstrated that a relatively lightweight and well-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

tuned model could reliably discriminate between these passwords (weak, moderate, and strong). Nonetheless, the combination of this research is beyond raw classification accuracy, rather it demonstrated a more realistic real-world assessment by the combination of heuristic measures with predictions of the machine learning and breach of intelligence. Contrarily, the research has its limitations such as constraints posed to both training and evaluation to only available leaked datasets. The deployment data was also limited, making it difficult for generalizability across other features (cultures, languages and real-world user behaviour) for evaluation. The scope of the research was limited to authentication weakness without considering firmware vulnerabilities, misconfigurations beyond passwords and detection of traffic-based anomaly, addressing the activities of post-compromise.

REFERENCES

[1]. Alturki, B., & Alsulami, A. A. (2025). Semi-Supervised Learning with Entropy Filtering for Intrusion Detection in Asymmetrical IoT Systems. *Symmetry*, *17*(6). https://doi.org/10.3390/sym17060973

[2]. Ammu, E., & Devanathan, B. (n.d.). A Comparison study of various Wireless Intrusion Detection Systems. *International Journal on Science and Technology (IJSAT) IJSAT25049500*, *16*(4). Retrieved www.ijsat.org•

[3]. Bhardwaj, A., Bharany, S., Abulfaraj, A. W., Osman Ibrahim, A., & Nagmeldin, W. (2024). Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities. *Egyptian Informatics Journal*, *25*. https://doi.org/10.1016/j.eij.2024.100443

[4]. Chatzisofroniou, G., & Kotzanikolaou, P. (2025). Security analysis of the Wi-Fi Easy Connect. *International Journal of Information Security*, *24*(2). https://doi.org/10.1007/s10207-025-00988-3

[5]. Farhan, M., Waheed ud din, H., Ullah, S., Hussain, M. S., Khan, M. A., Mazhar, T., Khattak, U. F., & Jaghdam, I. H. (2025). Network-based intrusion detection using deep learning technique. *Scientific Reports*, *15*(1), 1–15. https://doi.org/10.1038/s41598-025-08770-0

[6]. Gambo, A. Y., Gambo, F. L., Abdullahi, A. A., Ibrahim, N., Maitama, Y. I., & Zakari, Z. A. (2024a). Improving intrusion detection system accuracy using deep neural network. *Dutse Journal of Pure and Applied Sciences*, *10*(2c), 68–74. https://doi.org/10.4314/dujopas.v10i2c.7

[7]. Gambo, A. Y., Gambo, F. L., Abdullahi, A. A., Ibrahim, N., Maitama, Y. I., & Zakari, Z. A. (2024b). Improving intrusion detection system accuracy using deep neural network. *Dutse Journal of Pure and Applied Sciences*, *10*(2c), 68–74. https://doi.org/10.4314/dujopas.v10i2c.7

[8]. Hu, H., Myers, S., Colizza, V., & Vespignani, A. (2009). *WiFi networks and malware epidemiology*. www.pnas.org/cgi/content/full/

[9]. Karmous, N., Aoueileyine, M. O. E., Abdelkader, M., Romdhani, L., & Youssef, N. (2024). Software-Defined-Networking-Based One-versus-Rest Strategy for Detecting and Mitigating Distributed Denial-of-Service Attacks in Smart Home Internet of Things Devices. *Sensors*, *24*(15). https://doi.org/10.3390/s24155022

[10]. Kaushik, K., Bhardwaj, A., & Dahiya, S. (2025). Framework to analyze and exploit the smart home IoT firmware. *Measurement: Sensors*, *37*. https://doi.org/10.1016/j.measen.2024.101406

[11]. Liu, J. (2024). Enhancing Network Security Through Router-Based Firewalls: An Investigation into Design, Effectiveness, and Human Factors. In *Highlights in Science, Engineering and Technology CSIC* (Vol. 2023).

[12]. M. M., Y., K. G., F., M., C., & L. C., O. (2024). An Efficient Security Routing Protocol for Cloud-Based Networks Using Cisco Packet Tracer. *British Journal of Computer, Networking and Information Technology*, *7*(2), 49–67. https://doi.org/10.52589/bjcnit-oyirlauk

[13]. Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of Smart Homes: Privacy and Security. *Journal of Electrical and Computer Engineering*, *2024*. https://doi.org/10.1155/2024/7716956

[14]. Oughton, E., Geraci, G., Polese, M., Shah, V., Bubley, D., & Blue, S. (2024). Reviewing wireless broadband technologies in the peak smartphone era: 6G versus Wi-Fi 7 and 8. *Telecommunications Policy*, *48*(6). https://doi.org/10.1016/j.telpol.2024.102766

[15]. Quach, S., Dang, S., Thaichon, P., Le, D., & Le, T. H. H. (2025). Data vulnerability: does privacy protection behaviour improve digital well-being? *European Journal of Marketing*. https://doi.org/10.1108/EJM-12-2022-0953

[16]. Radha, M. C., Midunkumar, M. R., Muralibabu, M. S., Partheeban, M. V, & Mani, M. C. (n.d.). Enhancement of Security in Wireless Network. In *International Journal of Scientific Research & Engineering Trends* (Vol. 10, Number 6).

[17]. Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. In *Computers* (Vol. 14, Number 2). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/computers14020061

[18]. Sivagaminathan, V., Sharma, M., & Henge, S. K. (2023). Intrusion detection systems for wireless sensor networks using computational intelligence techniques. *Cybersecurity*, *6*(1). https://doi.org/10.1186/s42400-023-00161-0

[19]. Su, B., Huang, J., Miao, K., Wang, Z., Zhang, X., & Chen, Y. (2023). K-Anonymity Privacy Protection Algorithm for Multi-Dimensional Data against Skewness and Similarity Attacks. *Sensors*, *23*(3). https://doi.org/10.3390/s23031554

[20]. Sugai, R., Sei, Y., Tahara, Y., & Ohsuga, A. (2023). A k-Anonymization Method for Social Network Data with Link Prediction. *International Conference on*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb804

Information Systems Security and Privacy, 493–500. https://doi.org/10.5220/0011676800003405

[21]. Sweeney, L. (2002). L. Sweeney. k-anonymity: a model for k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY 1. In *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* (Vol. 10, Number 5).

[22]. Torra, V., & Navarro-Arribas, G. (2023). Attribute disclosure risk for k-anonymity: the case of numerical data. *International Journal of Information Security*, *22*(6), 2015–2024. https://doi.org/10.1007/s10207-023-00730-x

[23]. Ussipov, N., Akhtanov, S., Turlykozhayeva, D., Temesheva, S., Akhmetali, A., Zaidyn, M., Namazbayev, T., Bolysbay, A., Akniyazova, A., & Tang, X. (2024). MEGA: Maximum-Entropy Genetic Algorithm for Router Nodes Placement in Wireless Mesh Networks. *Sensors*, *24*(20). https://doi.org/10.3390/s24206735

[24]. Valvi, H., Mohan, A., & Nair, S. S. (2025). Analyzing Router Firmware for Potential Security Weaknesses. *International Research Journal of Engineering and Technology*. www.irjet.net

[25]. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. In *Electronics (Switzerland)* (Vol. 13, Number 16). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13163343

[26]. Vehkjärvi, P. (n.d.). *Understanding the Risks of Home Wi-Fi Router Breaches on Corporate Off-Site*.

[27]. Xing, L., Zhang, D., Wu, H., Ma, H., & Zhang, X. (2023). Distributed K-Anonymous Location Privacy Protection Algorithm Based on Interest Points and User Social Behavior. *Electronics (Switzerland)*, *12*(11). https://doi.org/10.3390/electronics12112446

[28]. Ye, J., de Carné de Carnavalet, X., Zhao, L., Zhang, M., Wu, L., & Zhang, W. (2024). Exposed by Default: A Security Analysis of Home Router Default Settings. *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 63–79. https://doi.org/10.1145/3634737.3637671

[29]. Ye, J., De Carne De Carnavalet, X., Zhao, L., Zhang, M., Wu, L., & Zhang, W. (2025). Exposed by Default: A Security Analysis of Home Router Default Settings and Beyond. *IEEE Internet of Things Journal*, *12*(2), 1182–1199. https://doi.org/10.1109/JIOT.2024.3502405