

Adaptive Cryptography Key Management using Machine Learning Based Intrusion Detection

1st Prof. Ashish Dudhale

Department of Electronics and Telecommunication Engineering Army Institute of Technology Dighi, Pune, India

2nd Prof. Dr Rajashree Suryavanshi

Department of Electronics and Telecommunication Engineering Army Institute of Technology Dighi, Pune, India

Abstract - Modern communication systems use static cryptographic keys that are highly vulnerable to cyber-attacks, which can compromise sensitive data over time. To solve this problem, our project proposes an Adaptive Cryptography framework that integrates Machine Learning-based Intrusion Detection Systems (IDS) with dynamic key management. The system applies prescriptive modelling techniques to analyze the real-time and historical network traffic data to identify the anomalous patterns that may indicate the potential security threats. The model employs supervised machine learning algorithm Support Vector Machine (SVM) to classify traffic as normal or malicious with higher accuracy. When an intrusion is detected, the system automatically begins cryptographic key rotation using secure protocols such as Elliptic Curve Diffie-Hellman (ECDH) for key exchange and Advanced Encryption Standard (AES) for data encryption.[11] This adaptive mechanism helps to reduce the risk of compromising keys and provides continuous protection. Also, data science methods such as data preparation, feature selection and behavioral analysis improves the efficiency and decision making capability of the model.[6] The ultimate aim of this approach is to improve cyber security through real-time threat detection and dynamic encryption, ensuring secure and reliable communication in growing network environments.[5]

Keywords— Adaptive Cryptography, Intrusion Detection System (IDS), Machine Learning, Predictive Modelling, Dynamic Key Rotation, Cyber security.

I. INTRODUCTION

With the rise of cyber-attacks, it has become increasingly challenging and important to protect data and communication in today's digital world. Traditional security systems employ static cryptographic keys, which remain unchanged for extended periods and are thus susceptible to attacks. Once these keys are leaked or cracked, they could access sensitive data and create serious security risks. But frequent key changes are also inefficient and introduce complex overhead. This points to the need for smarter and more flexible security solutions. Adaptive Cryptography aims to tackle these limitations by combining machine learning with encryption techniques. Instead of using static keys, the system keeps an eye on network activity and responds to suspicious behaviour. When the system detects an intrusion, it automatically updates the encryption keys.[9] This measure prevents attackers from reusing any compromised keys. The

complexity of cyber threats is increasing and data-driven approaches are becoming more and more relevant. Network data is analysed at large to detect abnormal patterns and predict potential attacks using Machine Learning techniques. This allows the system to take preventive measures rather than reacting after damage has been done.[10]

The overall process is composed of several steps, each contributing to the construction of a secure and intelligent system:

- Data Preparation: Cleaning and structuring raw network data, removing irrelevant or inconsistent values.
- Pattern Modelling: Statistical and learning methods to understand normal vs abnormal behaviour.
- Decision Structures: Defining system responses to different threat scenarios using models such as decision trees.
- Anomaly Detection: Real-time detection of anomalous activities that could indicate a cyber-attack.
- Predictive Analysis: To foresee possible threats and take proactive measures like updating keys in advance.

A. Data Science/Analytics

The Data Science and Analytics deals with the analysis of a large amount of data in order to understand the behaviour of networks and the prediction of security risks. The analysis facilitates the identification of concealed patterns in network traffic and aids the system in making informed security decisions. The application of analytical techniques enables the system to detect potential risks within a network and respond appropriately.[1]

Five major types of the process:

- Data Collection: The process entails collecting real-time network data, including traffic logs, packet details, and intrusion alerts, from multiple sources.
- Data Storage: The collected data is systematically organized and securely stored, ensuring it remains clean, structured, and prepared for subsequent use.
- Data Processing: The data are analyzed employing

techniques such as classification and pattern recognition.

- **Data Analysis:** To calculate and evaluate how strong the threats are and predict the attacks, the advanced analytical methods are applied.
- **Data Presentation:** The final results are displayed using graphical representation, dashboards and reports, and results are shown.[2]

Machine Learning:

Machine learning is a key subject of Artificial Intelligence which allows the system, algorithm, tool to understand and learn from the given data sets. Here, it helps to understand and detect network activities which are more suspicious and then decide when to reset or update the cryptographic keys. By understanding previous data related to behaviour of the network, the model learns the network pattern and can take appropriate actions against cyber threats. Machine learning performs its operation based on major three components.[3]

- **Decision Mechanism:** This component analyses and understands the incoming datasets in the network and classifies as a dataset. It improves its efficiency without any programming. Triggering the rotation of cryptographic keys is mainly based on the features like login attempts i.e. how many times user have attempted login to the network, duration of the session and protocol type.
- **Optimization process:** To decrease the errors and glitches, the model runs continuously and adjusts all the parameters which are necessary. This behaviour of the model increases the reliability of detecting unusual, unseen and new cyber-attacks.
- **Evaluation Metrics:** There are few parameters like recall, F1 score, precision and accuracy to measure the performance of the model. This makes the model to understand the actual threat and attacks instead of unnecessary and unwanted alerts.[4]

II. PROBLEM STATEMENT

Design and develop a security algorithm which is smart and adaptive in nature to detect potential threats to the network at very early stage, detect channels which are compromised, which will prevent sensitive data from being accessed. Generally cryptographic systems have constant or static keys which do not change over the period of time, hence becomes easy for intruders to intercept the key and log in to the network easily. This situation creates difficulties in maintaining security of the network.

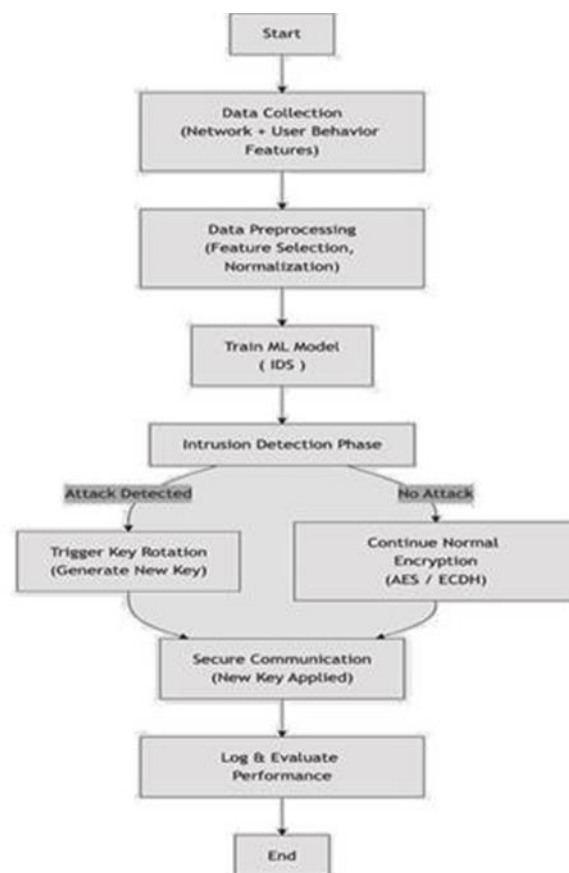


Fig. 1. Flowchart of security algorithm design

III. METHODOLOGY

A. Data Collection

There are standard data sets available like NSL – KDD from which user behaviour parameters and data of network traffic is collected for manipulation. These data sets have information about multi-level connection features including types of protocol, traffic flags. This gives clear idea about network activity.

session_id	network_ip	protocol_type	login_attempt	session_duration	encryption_used	ip_reputation_score	failed_login	browser_type	unusual_time_access	attack_detected
SID_00001	598	TCP	4	492.9832934	DES	0.60681808	1	Edge	0	1
SID_00002	472	TCP	3	1557.996461	DES	0.301568968	0	Firefox	0	0
SID_00003	629	TCP	3	75.04426166	DES	0.739164328	2	Chrome	0	1
SID_00004	804	UDP	4	601.2488352	DES	0.123267176	0	Unknown	0	1
SID_00005	453	TCP	5	532.5408884	AES	0.054873857	1	Firefox	0	0
SID_00006	453	UDP	5	380.4715502	AES	0.422465061	2	Chrome	1	0
SID_00007	815	ICMP	4	728.1071647	AES	0.413771929	1	Chrome	0	1
SID_00008	653	TCP	3	12.58896011	DES	0.097719366	3	Chrome	1	1
SID_00009	406	TCP	2	542.5588952	None	0.284579688	0	Chrome	1	0
SID_00010	608	UDP	6	531.9441066	None	0.424116564	1	Chrome	0	0
SID_00011	407	UDP	6	560.7219254	DES	0.122893709	3	Firefox	0	1
SID_00012	406	UDP	9	191.0528389	DES	0.338711271	1	Edge	0	1
SID_00013	548	TCP	2	186.1476383	None	0.408898633	2	Safari	1	0
SID_00014	117	TCP	4	833.4889648	DES	0.472291905	2	Unknown	0	1
SID_00015	155	TCP	3	77.8495157	None	0.352475575	3	Chrome	0	1
SID_00016	387	ICMP	6	292.1361196	DES	0.254912451	3	Chrome	0	1
SID_00017	297	TCP	8	1421.414371	AES	0.345367552	3	Firefox	0	1
SID_00018	562	UDP	1	87.64100189	None	0.13672919	2	Firefox	0	0
SID_00019	318	TCP	5	504.98087	AES	0.394231457	1	Unknown	0	1
SID_00020	217	ICMP	2	863.6279678	DES	0.310113157	0	Chrome	0	0

Fig. 2. Dataset 1: cybersecurity_intrusion_data.csv

B. Data Cleansing

Pre-processing of the data is performed in Jupiter notebook environment by using Python libraries like

pandas. This process helps to remove null values data sets, duplicate data sets to improve data consistency. This leads to generate hassle free and clean data sets which is then used for further analysis and to train the model.

```
plt.figure(figsize=(15,8))
df[numerical_features].boxplot()
plt.xticks(rotation = 15)
plt.title("Boxplot of Numerical
Features (Outlier Detection)")
plt.ylabel("Values")
plt.show()
```

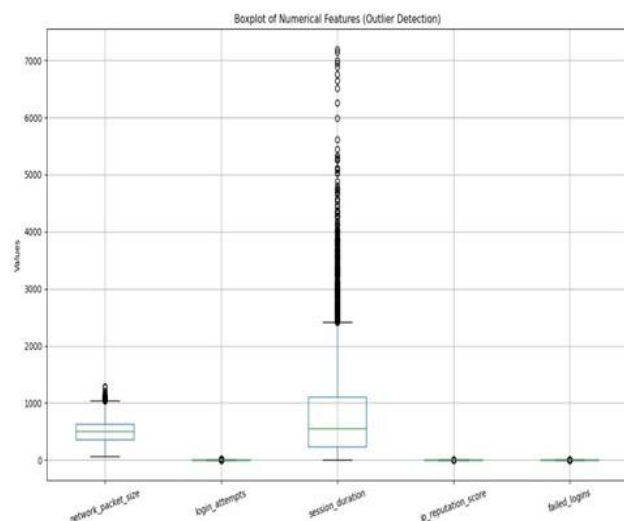


Fig. 3. Data Cleaning: Outlier Detection

C. Data Selection

To understand the network whether it is normal or malicious, relevant parameters of the data sets are selected based on their significance. Based on priorities of the parameters such as session flags,

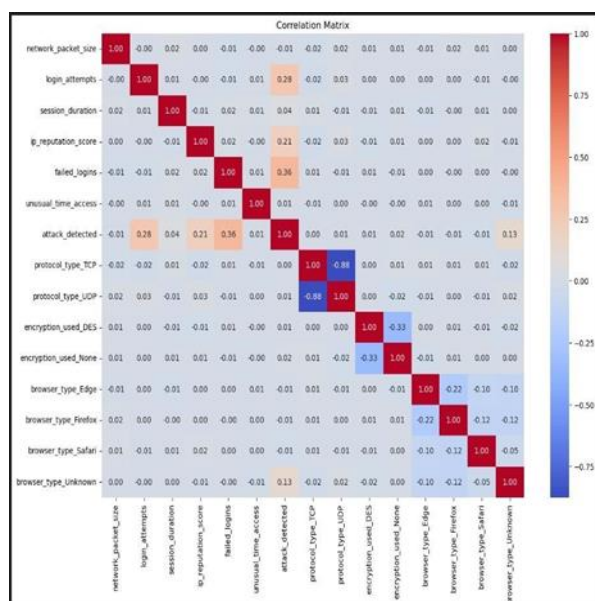


Fig. 4. Attribute correlation

D. Data Selection

Using Label Encoding techniques all categorical parameters are converted into numerical form. Moreover, Standard Scalar is used to scale features, normalizing their numerical ranges so the model learns evenly across all attributes without being skewed by any particular one.

E. Data Selection

The proposed system follows a structured pipeline:

Data Ingestion -> Data Pre-processing -> Intrusion Detection (IDS classification) -> Key Rotation trigger.

This architecture is designed so that any detected anomaly triggers the cryptographic key management process right away.

F. Platform or Tool selection

To develop this algorithm, python programming language is used for both , model and backend logic. The Flask framework is used to build APIs that manage intrusion detection and key management processes. The frontend interface is developed with React and styled using Tailwind CSS to deliver an engaging user experience.

G. Algorithm

Several supervised machine learning algorithms such as Random Forest, K-Nearest Neighbours (KNN), and Decision Trees are assessed. The XGBoost classifier is chosen for final deployment because it offers the highest accuracy, is highly robust, and can effectively manage intricate, non-linear patterns in network traffic data.

=== Model Performance Comparison ===								
	Accuracy	Precision	Recall	F1 Score	AUC	Train Time (s)	Predict Time (s)	Model Size (MB)
Logistic Regression	0.7290	0.7193	0.6460	0.6807	0.7876	0.0620	0.0010	0.0011
Random Forest	0.8863	0.9969	0.7479	0.8547	0.8800	5.6407	0.1569	16.4134
SVM	0.8737	0.9665	0.7433	0.8403	0.8730	30.7626	2.0012	0.3899
KNN	0.8014	0.8624	0.6612	0.7485	0.8356	0.0762	0.6253	0.9950
XGBoost	0.8821	0.9758	0.7550	0.8513	0.8813	2.7916	0.0113	0.2251

Fig. 5. Model Comparison

H. Behavioural Analysis

The system analyses network sessions in real time by evaluating traffic patterns and user behaviour. This allows for precise categorization of activities as either normal or malicious, thereby improving the effectiveness of intrusion detection.

I. Implimentation

The model is developed and trained within a Jupyter Notebook environment. The trained model is stored as a serialized file (xgboost_model.pkl) and incorporated into the Flask backend (app.py). The backend also interacts with the key management module (key_rotation.py) to carry out dynamic cryptographic operations.

J. Data Visualization

Performance evaluation employs visualization tools like Matplotlib and Seaborn to produce confusion matrices and accuracy plots. Moreover, a React-based dashboard offers real-time oversight of detected intrusions, active encryption keys, and key rotation logs.

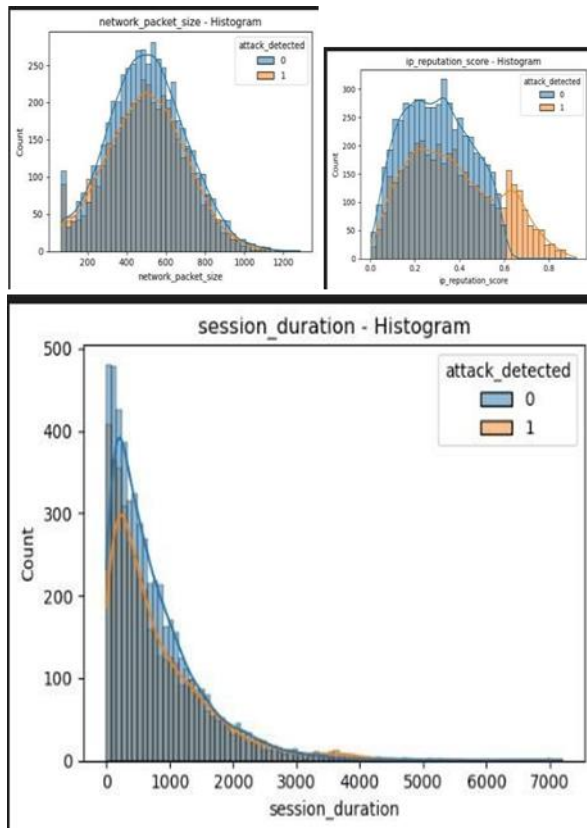


Fig. 6. Data Visualization

```
plt.figure(figsize=(15,8))
df[numerical_features].boxplot(
) plt.xticks(rotation = 15)
plt.title("Boxplot of Numerical
Features (Outlier Detection)")
plt.ylabel("Values")
plt.show()
```

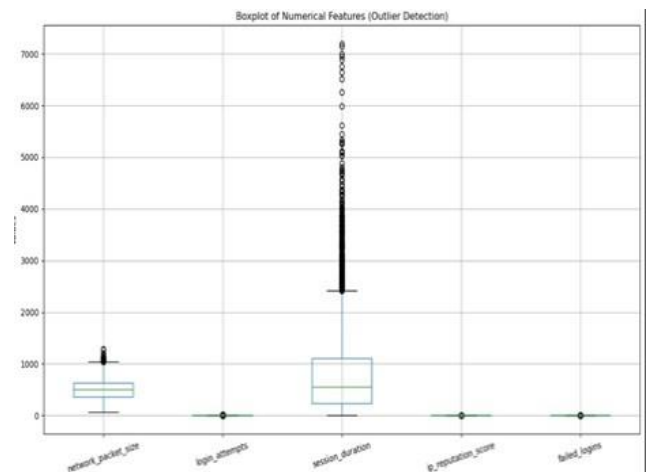


Fig. 7. Visualization in Tableau

IV. CONCLUSION

This study aimed to overcome the shortcomings of conventional cryptographic systems that depend on static keys, known to be especially susceptible to contemporary cyber-attacks. To address this challenge, a flexible framework was introduced by combining Machine Learning-based Intrusion Detection with dynamic cryptographic key management. The main goal was to investigate and assess different Machine Learning and Data Science methods for identifying network intrusions and safeguarding secure communication. The system successfully showed that integrating real-time intrusion detection with automatic key rotation greatly improves security. By employing AES for encryption and ECDH for secure key exchange, the framework guarantees that any compromised key is swiftly replaced, thereby minimizing the risk of data exposure. Nevertheless, some challenges emerged during implementation, especially in combining various system components and enhancing real-time performance. These limitations underscore the necessity for greater refinement in system architecture and deployment strategies. Overall, the proposed approach offers an effective and scalable solution for contemporary cyber security threats by facilitating intelligent, adaptive, and automated defence of communication systems.

ACKNOWLEDGMENT

The authors would like to thank everyone.

REFERENCES

- [1] Amodh Kumar; Akshat Kapil; Deepak Ahlawat "Exploring The Data Science", 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)
- [2] J. Ranjani; V.K.G. Kalaichelvi; Swathi Anbalagan; Niranjani Kumar S; Murari Reddy Sudarsan "A Deep study of Data science related problems, application and machine learning algorithms utilized in Data science", 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)
- [3] Kexin Chen "Research on Popular Machine Learning Algorithms", 2023 IEEE 6th International Conference on Information Systems and Computer Aided Education (ICISCAE)
- [4] Fatih Er; Ibraheem Shaya; Bilal Saoud; Leila Rzayeva; Aigerim Alibek "Machine Learning and Deep Learning Algorithms in Times Series Analysis", 2024 IEEE International Conference on Big Data & Machine Learning (ICBMDL)
- [5] Sheena Angra; Sachin Ahuja "Machine learning and its applications: A review", 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC)
- [6] Surbhi Sharma, Baijnath Kaushik, Mohammad Khalid Imam Rahmani, Md. Ezaz Ahmed "Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles", IEEE Access
- [7] LOUAI A. MAGHRABI, "Automated Network Intrusion Detection for Internet of Things: Security Enhancements", IEEE Access 2024
- [8] Venkata Ramani Varanasi, Shaik Razia, "Network Intrusion Detection using Machine Learning, Deep Learning - A Review", Conference: 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)
- [9] K. SASIKUMAR, SIVAKUMAR NAGARAJAN "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing", IEEE Access
- [10] M. Rekha; P.Shobha Rani; Aashida S; Elakkiya S; Ezhil Arasi S; Amirtha A, "Intelligent Security Monitoring: Machine Learning-based Intrusion Detection", 2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)
- [11] Rahat Afreen, S.C. Mehrotra "A REVIEW ON ELLIPTIC CURVE CRYPTOGRAPHY FOR EMBEDDED SYSTEMS", International Journal of Computer Science & Information Technology (IJSIT), Vol. 3, No 3, June 2011
- [12] MANOHAR SRINIVASAN, N. C. SENTHILKUMAR "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework", IEEE Access
- [13] Hamza Kheddar , Senior Member, IEEE, Diana W. Dawoud , Senior Member, IEEE, Ali Ismail Awad , Senior Member, IEEE, Yassine Himeur , Senior Member, IEEE, and Muhammad Khurram Khan , Senior Member, IEEE "Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review.", IEEE

COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 27, NO. 4, AUGUST 2025

- [14] Darzi Mehtaab Siddiq, Myle Vijayalakshmi, Kuruva Sravani, Mala Anitha, Kyrupla Harika, "ADAPTIVE CLOUD SECURITY USING ML-DRIVEN AUTHENTICATION AND CRYPTO-AGILE ENCRYPTION", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 26 Issue 02 (February), 2026.
- [15] K. SASIKUMAR, SIVAKUMAR NAGARAJAN "Enhancing

Cloud

Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques", IEEE open journal of The Computer Society

- [16] Frederic Setievi; Jessica Natalia; Theodore Raynard Tjhang; Ivan Sebastian Edbert; Derwin Suhartono "A Comparative Study of Supervised Machine Learning Algorithms for Fake Review Detection", 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)
- [17] Khawla Ali Maodah, "Integrating Machine Learning and Intrusion Detection for Improved Cloud Security.", International Journal of Cloud Applications and Computing Volume 16, Issue 1, 22 January 2026
- [18] Yakub Kayode Saheed, Aremu Idris Abiodun, Sanjay Misra, Monica Kristiansen Holone, Ricardo Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks", Alexandria Engineering Journal Volume 61, Issue 12, December 2022, Pages 9395-9409.
- [19] Abhinav Vishnu; Jeyanthi Narasimhan; Lawrence Holder; Darren Kerbyson; Adolfo Hoisie "Fast and Accurate Support Vector Machines on Large Scale Systems", 2015 IEEE International Conference on Cluster Computing
- [20] CHI ZHANG; DAN LI; HAO-YANG LI; LAN-FEI MA; JIA-YI SONG; YU-XIN YING "Application of Support Vector Machine Of Quantum Genetic Algorithm With Gauss Initialization In Multi-Class Classification", 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing
- [21] Noor Hafsa, Hadeel Alzoubi, and Sajida Imran, "Machine Learning-based Intrusion Detection and Prevention using Cross-layer Features in Internet of Things (IoT) Networks", JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 27, NO. 5, OCTOBER 2025.

AUTHOR

Prof Ashish Dudhale is currently working as an Assistant Professor in the Department of Electronics and Telecommunication Engineering at Army Institute of Technology (AIT), Pune, India. He received his bachelor's degree in Electronics and Telecommunication engineering from PVG's COE, Pune, India and M.Tech. in Embedded systems from Bharti Vidyapeeth, Pune, India. His research interest includes Embedded systems, IoT, Robotics, Cyber security, AI and ML. He has over 17 years of experience in embedded systems, Robotics and AI. He has delivered many training sessions to trainee engineers, faculties, students on IoT, AI and AI.

Dr. Rajashree Prashant Suryawanshi is currently working as an Associate Professor in the Department of Electronics and Telecommunication Engineering at Army Institute of Technology (AIT), Pune, India. She received her Ph.D. in Electronics Engineering and holds a Master's degree in Electronics. Her research interests include wireless communication, 5G/6G networks, spectrum allocation, and artificial intelligence in communication systems, and signal processing. She has authored several research papers in reputed international journals and conferences, with a focus on emerging technologies in next-generation communication networks.

She has more than 25 years of teaching and research experience and has guided numerous undergraduate and postgraduate projects in the areas of communication systems and networking. She is actively involved in academic development, curriculum design, and laboratory innovation. Dr. Suryawanshi is a member of IETE.