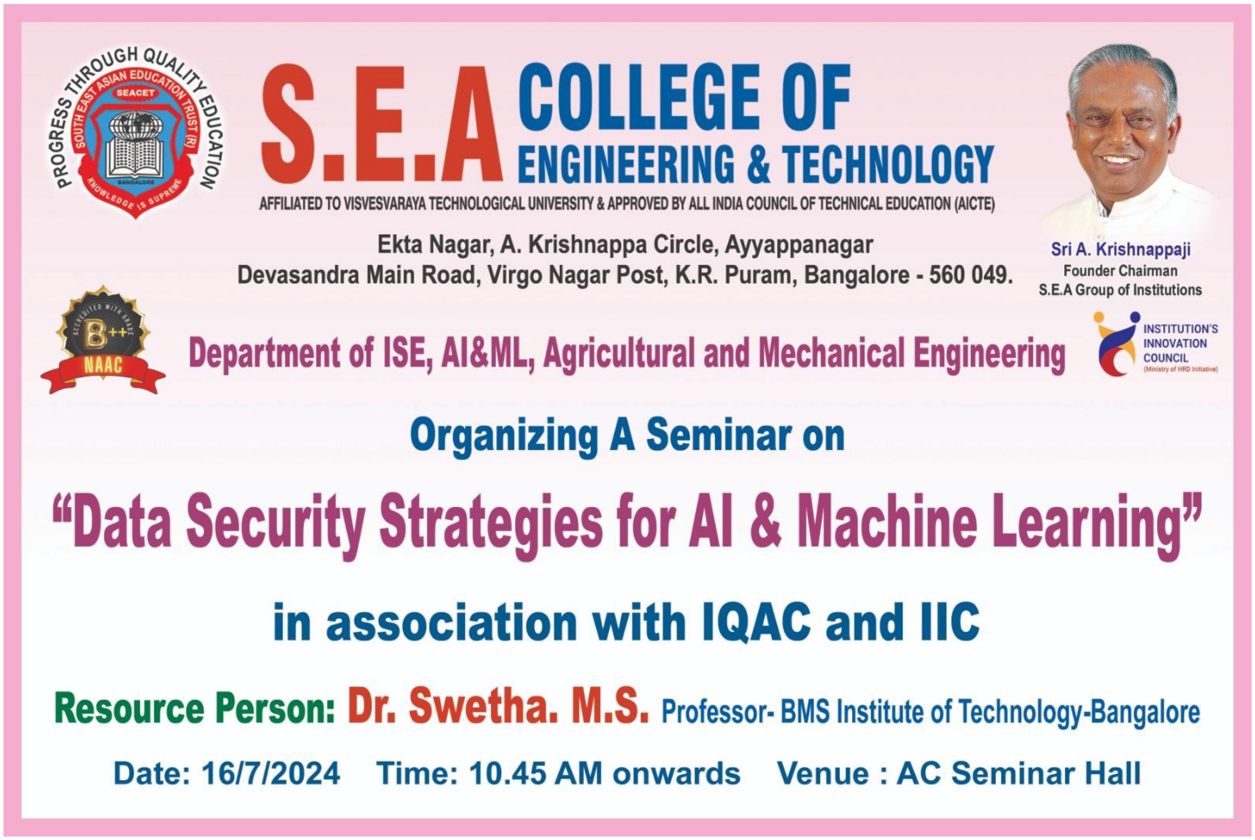
SOUTH EAST ASIAN EDUCATION TRUST ®

S.E.A. COLLEGE OF ENGINEERING & TECHNOLOGY

(Approved by All India Council for Technical Education (AICTE), New Delhi
Affiliated to Visvesvaraya Technological University (VTU), Belagavi, Accredited B++ by NAAC)

Seminar Report: Data Security Strategies for AI & Machine Learning



S.E.A COLLEGE OF ENGINEERING & TECHNOLOGY

AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY & APPROVED BY ALL INDIA COUNCIL OF TECHNICAL EDUCATION (AICTE)

Ekta Nagar, A. Krishnappa Circle, Ayyappanagar
Devasandra Main Road, Virgo Nagar Post, K.R. Puram, Bangalore - 560 049.

Sri A. Krishnappaji
Founder Chairman
S.E.A Group of Institutions

Department of ISE, AI&ML, Agricultural and Mechanical Engineering

Organizing A Seminar on

"Data Security Strategies for AI & Machine Learning"

in association with IQAC and IIC

Resource Person: Dr. Swetha. M.S. Professor- BMS Institute of Technology-Bangalore

Date: 16/7/2024 Time: 10.45 AM onwards Venue : AC Seminar Hall

Department of ISE, AI&ML, Agricultural and Med
Organizing A Seminar
"Da ty Strategies for AI & M
ssociation with IQAC
Swetha. M.S. Professor- BMS
e: 10.45 AM o ards Ven

neering
e Learning"
Technology-Bangalore
ar Hall

GPS Map Camera
Bengaluru, Karnataka, India
South East Asian College Engineering & Management, Basavanapura Rd, Lourdu Nagar,
Virgonagar, Krishnarajapuram, Bengaluru, Karnataka 560049, India
Lat 13.008623°
Long 77.715199°
16/07/24 11:08 AM GMT +05:30
Google

Seminar Report: Data Security Strategies for AI & Machine Learning

Introduction

In the evolving landscape of Artificial Intelligence (AI) and Machine Learning (ML), the role of data security is increasingly crucial. This seminar explores the strategies and challenges associated with safeguarding data in AI and ML applications. The integration of these technologies into various sectors has highlighted the need for robust data protection measures to mitigate risks and ensure trust.

Importance of Data Security in AI & ML

AI and ML algorithms heavily rely on data for training, inference, and decision-making. Ensuring the integrity, confidentiality, and availability of this data is fundamental to prevent adversarial attacks, data breaches, and unauthorized access. Moreover, compliance with regulations such as GDPR, CCPA, and sector-specific laws further emphasizes the necessity for stringent data security measures.

Strategies for Data Security

1. **Data Encryption**: Employing strong encryption methods (e.g., AES-256) ensures that data remains unreadable to unauthorized users or attackers.
2. **Access Control**: Implementing strict access control mechanisms ensures that only authorized personnel and systems can access sensitive data. Role-based access control (RBAC) and multi-factor authentication (MFA) are commonly used.
3. **Anonymization and Pseudonymization**: Removing or obfuscating personally identifiable information (PII) minimizes the risk associated with data breaches.

4. **Secure Data Sharing**: When sharing data among different entities or for collaborative purposes, employing secure data sharing protocols such as differential privacy or secure multi-party computation can protect data confidentiality.
5. **Regular Audits and Monitoring**: Continuous monitoring of AI and ML systems for anomalies or suspicious activities can help detect potential security breaches early. Regular audits ensure compliance with security policies and regulations.
6. **Secure Model Training**: Protecting data during the training phase by using techniques like federated learning, where models are trained locally on decentralized data, helps maintain data privacy.
7. **Adversarial Defense Mechanisms**: Implementing techniques to detect and mitigate adversarial attacks on AI models, such as adversarial training or robust model architectures, enhances model security.

Challenges

1. **Data Complexity**: Managing and securing large volumes of diverse data types (structured and unstructured) pose significant challenges.
2. **Privacy Concerns**: Balancing data utility with privacy protection is a persistent challenge in AI and ML applications.
3. **Regulatory Compliance**: Keeping up with evolving data protection regulations and ensuring compliance across different jurisdictions can be complex.
4. **Emerging Threats**: Rapidly evolving cyber threats and techniques used by malicious actors require continuous adaptation of security measures.

Conclusion

Data security is integral to the successful deployment and operation of AI and ML systems. By adopting comprehensive strategies that encompass encryption, access control, secure sharing, and robust monitoring, organizations can mitigate risks and build trust with stakeholders. However, addressing the challenges posed by data complexity, privacy concerns, regulatory requirements, and emerging threats requires ongoing collaboration between researchers, developers, and policymakers.

In conclusion, safeguarding data in AI and ML environments demands a proactive approach that prioritizes security at every stage of the data lifecycle. This seminar underscores the importance of integrating robust data security strategies into the foundation of AI and ML initiatives to foster innovation while safeguarding privacy and integrity.

No. of students attended: 2nd year B.E Students(120 students)