Date:21-10-2023

To,
The Principal
R K College of Engineering.

Through HOD-AI&ML

Sub: Seeking permission to conduct Seminar on "AI IN CYBERSECURITY".

Sir,

I request you to kindly grant permission to conduct a Seminar on 26TH&27thOctober 2023 on "AI IN CYBERSECURITY"The purpose of this project is to exploreGiven the growing importance of Artificial Intelligence in enhancing cybersecurity measures, this seminar aims to provide attendees with valuable insights into how AI is revolutionizing the field of cybersecurity, its benefits, and the challenges involved. the capabilities, This seminar aims to provide participants with regard to the new trends in This will be a very informative seminar for many students.

Our students really need to understand the operation and advantages of Distributed Generation as an alternative generating technique.

Thanking you Sir

Yours Sincerely

SK.SHABAAZ
ASSISTANT PROFESSOR
HOD-AI&ML

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456

TWO-DAY SEMINAR ON

"AI IN CYBERSECURITY"

Organized by
Department of AI&ML Engineering
RK College of Engineering, Vijayawada

PROGRAMME FLOW – 25-10-2023.

TIME	SPEAKER	TOPIC TO BE DELIVERED
10:00 AM to 10:15 AM	SK.SHABAAZ	Welcome speech
10:15 AM to 10:30 AM	Dr.P.PAVAN KUMAR	Introduction about the program
10:30 AM to 11:30 AM	Dr.P.PAVAN KUMAR Associate Professor. KL UNIVERSITY VIJAYAWADA Email:pavankumarklu@gmail.com Phone No:9966733444	Common Applications of AI IN CYBERSECURITY
11:30 AM to 11 :45	TEA BREAK	
11:45 AM to 01:00 PM	Dr.P.PAVAN KUMAR Associate Professor. KL UNIVERSITY VIJAYAWADA Email:pavankumarklu@gmail.com Phone No:9966733444	Basic AI IN CYBERSECURITY Threat Detection Intrusion Detection Systems.
01:00 PM to 02:00 PM	LUNCHBREAK	
02:00 PM to 03:30 PM	Dr.P.PAVAN KUMAR Associate Professor. KL UNIVERSITY VIJAYAWADA Email:pavankumarklu@gmail.com Phone No:9966733444	Technologies Benefits of AI in Cybersecurity:

Coordinator: Mr.SK.SHABAAZ

**Coordinator-IQAC
RKCE**

TWO-DAYS SEMINAR ON

"JAVA FULL STACK"

Organized by
Department of AI & ML ENGINEERING
R K College of Engineering, Vijayawada

PROGRAMME FLOW – 26-10-2023

TIME	SPEAKER	TOPIC TO BE DELIVERED
10:30 AM to 11:30 AM	Dr.P.PAVAN KUMAR Associate Professor. KL UNIVERSITY VIJAYAWADA Email:pavankumarklu@gmail.com Phone No:9966733444	Introduction to AI in Cybersecurity Machine Learning in Cybersecurity Malware Detection and Analysis
11:30 AM to 11 : 45 AM	*TEA BREAK*	
11:45 AM to 01:00 PM	Dr.P.PAVAN KUMAR Associate Professor. KL UNIVERSITY VIJAYAWADA Email:pavankumarklu@gmail.com Phone No:9966733444	Advantages of AI IN CYBERSECURITY Improved Threat Detection
01:00 PM to 02:00 PM	*LUNCH BREAK*	
02:00 PM to 03:30 PM	Dr.P.PAVAN KUMAR Associate Professor. KL UNIVERSITY VIJAYAWADA Email:pavankumarklu@gmail.com Phone No:9966733444	Applications on a AI IN CYBERSECURITY
03:30 PM to 04:00 PM	*Feedback from the participants and vote of thanks by Mr.SK.SHABAAZ*	

Coordinators :Mr.SK.SHABAAZ

**Coordinator-IQAC
RKCE**

Date:21-10-2023

REPORT ON TWO DAY SEMINAR ON "AI IN CYBERSECURITY"

Title:"AI IN CYBERSECURITY"

Expert:Dr.P.Pavan Kumar
Associate professor
KL UNIVERSITY.
VIJAYAWADA
Email: pavankumarklu@gmail.com
Phone No: 9966733444
Date: 22nd&23rdNovember, 2023

Venue: SEMINAR HALL-003, RKCE.

Coordinators :Mr.SK.SHABAAZ
                Mr. D.SUDHARANI

Organized by: COMPUTER SCINECE AND ENGINEERING
Total Participants attended: 111

Details of Participants: Students of II Year 1stsemester.

Students of II Year 1stsemester have attended the seminar on AI IN CYBERSECURITY with full enthusiasm. Dr.P.PAVAN KUMARhas elaborately explained about the operation and advantages of AI IN CYBERSECURITY. Also, he explained about the various types and applications of AI IN CYBERSECURITY. The detailed topics are shown in program flow. This seminar was very useful as well as educative for the participants.

Coordinators

HOD-AI&ML

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

R K COLLEGE OF ENGINEERING
(Accredited by NAAC with 'A' Grade)
Kethanakonda (V), Ibrahimpatnam (M), Vijayawada, AMARAVATI-521456.

Student Attendance for Seminar on "AI IN CYBERSECURITY"

S. No	Reg. No	Name of the Candidate	SIGNATURE OF THE STUDENT	
			DAY 1	DAY 2
1	22MC1A6101	ACHANALA MURALI	P	P
2	22MC1A6102	BALUSUPALLI PRAVALLIKA		
3	22MC1A6103	BANAVATH BALU NAIK		
4	22MC1A6104	BANAVATHU NANDU BAI		
5	22MC1A6105	BESTHA SURESH		
6	22MC1A6107	BODDU BHARATHI RAJ		
7	22MC1A6108	CHINTA JAYA PRAKASH YADAV		
8	22MC1A6109	DHANYASI PRUDHVIKUMAR		
9	22MC1A6110	EJJANA PRIYANKA KEERTHANA		
10	22MC1A6111	GOGAM HARIKRISHNA VAMSIYADAV		
11	22MC1A6113	JAKKIREDDY INDRASENA REDDY		
12	22MC1A6115	JUTTUKA VEERA NAGENDRA		
13	22MC1A6117	KAMSALA SUMANTH KUMAR		
14	22MC1A6118	KELLA ESWAR JOGI ANAND SAI		
15	22MC1A6119	KODATI SHIVA GANESH		
16	22MC1A6120	KOLLIBOINA SURENDRA		
17	22MC1A6121	KONDA PRAMOD		
18	22MC1A6122	KONKALA NARASIMHA NAYUDU		
19	22MC1A6123	KUNCHAPU LOKESH		
20	22MC1A6124	KUNDURU MOUNIKA		
21	22MC1A6125	KURUBA ASHOK		
22	22MC1A6126	MEKALA SANTOSH KUMAR		
23	22MC1A6127	MELLAMPUTI KARTHIK		
24	22MC1A6128	MOHAMMAD REHAN		
25	22MC1A6129	MYNENI THANVIJA		
26	22MC1A6130	NALLADIMME VENKATA SANDHYA	A	A
27	22MC1A6131	NAMA GLORI		
28	22MC1A6132	ONTIPULI ANJALI		
29	22MC1A6133	PANDILLA SARANYA		
30	22MC1A6134	PASUNURI SATEESH		
31	22MC1A6135	PATAN BIBJAN		
32	22MC1A6136	PIRLA VARUN BABU		
33	22MC1A6137	POLEPALLI KIRAN KUMAR		
34	22MC1A6138	RAMAVATHU DURGA BAI		
35	22MC1A6139	RAPETI CHANDRA SEKHAR		
36	22MC1A6140	REVURU KAMAL		

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

R K COLLEGE OF ENGINEERING
(Accredited by NAAC with 'A' Grade)
Kethanakonda (V), Ibrahimpatnam (M), Vijayawada, AMARAVATI-521456.

37	22MC1A6141	SAMPATI JANI SRIKANTH		
38	22MC1A6142	SANA HARITHA		
39	22MC1A6144	SHAIK SHOYAB AKTHAR		
40	22MC1A6145	THATIPARTHI ABHI SHEKHAR REDDY		
41	22MC1A6146	THUPAKULA NAGENDRA BABU		
42	22MC1A6147	THUTHIKA JAHNAVI DEVI		
43	22MC1A6148	VELPURI MANOHAR		
44	22MC1A6149	YANDRA NAGA BHAVANI		
45	22MC1A6150	YARRAJONNA CHAITHANYA		
46	22MC1A6151	CHALUVADI RANGASWAMI		
47	23MC5A6101	ANIL SAI VEJENDLA		
48	23MC5A6102	BORRA BHANU PRAKASH		
49	23MC5A6103	KODURU RAVI TEJA		
50	22MC1A0402	ARAVAPALLI VENKATESWARA RAO		
51	22MC1A0403	BANAGANI VENKATACHANDRA KIRAN		
52	22MC1A0404	BANDI GANGA BHAVANI		
53	22MC1A0405	BATTULA PREMCHANDU		
54	22MC1A0406	BODDU SRINIVASA RAO		
55	22MC1A0407	BOMMISETTI SRI LAKSHMI		
56	22MC1A0408	BOYA GURU PRASAD		
57	22MC1A0409	CHAPPA JAYALAKSHMI		
58	22MC1A0410	CHATHANAMKUZHY AKASH		
59	22MC1A0411	CHAVATAPALLI AKHILA		
60	22MC1A0412	CHILAKALAPUDI REVANTH VARMA		
61	22MC1A0413	CHINAPANA HARIKRISHNA		
62	22MC1A0414	CHINTHAKAYALA SIVA SHANKAR NAIDU		
63	22MC1A0416	DAMARLA PAVAN SATHISH		
64	22MC1A0417	DEVIREDDY AKSHITHA		
65	22MC1A0418	DUGGIPOGU VIJAYA SRI		
66	22MC1A0419	GADDIPATI LALITHA PRIYADARSINI		
67	22MC1A0420	GANTA SWAPNA		
68	22MC1A0421	GOBBURI ADISESHU		
69	22MC1A0422	GUDIPALLI VENKATA RAJESH		
70	22MC1A0423	GUMMA HARSHA VARDHAN		
71	22MC1A0424	GUNTURU SANDEEP		
72	22MC1A0425	GUNUPATI PRATHYUSHA		
73	22MC1A0426	GUTHALA AKHIL		
74	22MC1A0427	IMMADI BALA NAGA PRAVEEN		
75	22MC1A0428	K MOHAN BABU		
76	22MC1A0429	KANCHARLA VISHNU VARDHAN		
77	22MC1A0430	KARRA SANDEEP		

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

78	22MC1A0431	KATHI PRABHAKAR		
79	22MC1A0432	KESANA VAMSI KRISHNA		
80	22MC1A0433	KORNE MANIKANTA SRINIVASA RAO		
81	22MC1A0434	KOTA ASHOK REDDY		
82	22MC1A0435	KURICHETI SRINU		
83	22MC1A0436	LAKKINENI INDIRA		
84	22MC1A0437	LINGAVARAPU VAMSI		
85	22MC1A0438	MANIGANTI AJAY BABU		
86	22MC1A0440	NUNSAVATH ANJI KUMAR NAIK		
87	22MC1A0441	PAPPALA SANJAY SRINIVAS		
88	22MC1A0442	PATAN SONIA		
89	22MC1A0443	PAVULURI CHAITANYA SATYANADH		
90	22MC1A0444	PETLURI HARSHAVARDAN		
91	22MC1A0445	PORUMALLA BHAGYA SRI		
92	22MC1A0446	PUJARI ASHOK		
93	22MC1A0447	RAMAVATH VENNELA BAI		
94	22MC1A0448	RATHNAKARAM SAINARAYANA RAJU		
95	22MC1A0449	REDDEM VAISHNAVI		
96	22MC1A0450	SOMANDEPALLY KEERTHANA		
97	22MC1A0451	SURAVARAPU AJAY		
98	22MC1A0452	TUNGALA AKANKSHA		
99	22MC1A0453	UPENDRAM YASASWINI		
100	22MC1A0454	VADDE RAJESH		
101	22MC1A0455	VADLA PAVAN KUMAR		
102	22MC1A0456	VARUGU NAVEEN KUMAR		
103	22MC1A0457	VEERAGANDHAM MOKSHAGNA CHOWDARY		
104	22MC1A0458	VISWANADHAPALLI GOPI CHARAN		
105	22MC1A0459	YAKALA RAJA RAO		
106	22MC1A0460	YAKKATI DHANA LAKSHMI		
107	23MC5A0401	AKULA SUPRIYA		
108	23MC5A0402	AKURATHI NAGA DEVI		
109	23MC5A0403	BATTA MOUNICA SRI		
110	23MC5A0404	BURAGAPALLI NAGA LAKSHMI		
111	23MC5A0405	CHEBROLU BHADRINATH SAI KRISHNA		

Coordinators

Coordinator-IQAC
RKCE

HOD-AIML

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

Resource Person Profile

Presently working as Associate Professor of AI & ML Engineering Department at KL UNIVERSITY from APRIL 2015 (Responsibilities: Teaching UG and PG Students of AIML and performing the works assigned by HOD and Principal). Having 17 years of Teaching and 5 years of Research consultancy in AIML.

APPLICATIONON AI IN CYBERSECURITY:

AI has become an essential tool in enhancing cybersecurity, providing advanced methods to detect, prevent, and respond to various cyber threats. Some key applications of AI in cybersecurity include:

1. Threat Detection and Prevention
   - Anomaly Detection: AI-powered systems can monitor network traffic and system behaviors to identify unusual patterns or activities that may indicate a cyberattack (e.g., malware or unauthorized access).
   - Intrusion Detection Systems (IDS): AI-based IDS can automatically detect unauthorized access and intrusions in real-time by analyzing patterns, making them more efficient than traditional signature-based methods.

2. Automated Incident Response
   - Security Automation: AI can quickly analyze data to identify threats and initiate an automated response, such as isolating infected devices or blocking malicious IP addresses, reducing human intervention and response time.
   - AI algorithms can analyze emails, websites, or other communications to detect phishing attempts. Machine learning models can identify common features in phishing attacks, such as misleading URLs or suspicious language, and flag them before they can harm users.

4. Malware Detection
   - Behavioral Analysis: Instead of relying solely on known signatures, AI can detect new or evolving malware by analyzing its behavior in real-time. This includes recognizing the actions taken by the malware, such as file or system modifications.

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

5. User and Entity Behavior Analytics (UEBA)

- AI can continuously monitor the behavior of users and entities within a network. It can create baseline profiles for typical behavior and flag anomalies, which may indicate compromised accounts or insider threats.

6. Network Traffic Analysis

- AI algorithms can analyze large volumes of network traffic and identify suspicious patterns indicative of potential security breaches, such as Distributed Denial of Service (DDoS) attacks or unauthorized data exfiltration.

7. AI in Vulnerability Management

- AI tools can assist in identifying system vulnerabilities by automatically scanning and assessing the security posture of software, hardware, and networks. They can also recommend and implement patches or mitigation strategies.

8. Fraud Detection

- AI systems can analyze transaction data to detect fraudulent activity by identifying inconsistencies and patterns that deviate from typical user behavior, which is especially useful in financial systems and e-commerce platforms.
- Real-time Fraud Alerts: AI algorithms can quickly flag suspicious activities and trigger alerts in real-time, helping to prevent or minimize the impact of fraud.

9. Deepfake Detection

- AI is being used to detect deepfakes (manipulated videos or images) by analyzing inconsistencies in the media, such as facial expressions, voice, or video artifacts that are difficult for humans to identify.
- Authenticity Verification: AI systems help verify the authenticity of video or audio content, protecting against misinformation and social engineering attacks.

10. Security Information and Event Management (SIEM)

- AI can enhance SIEM systems by correlating large volumes of log data across different sources, identifying potential threats, and offering automated responses. It can also filter out false positives and ensure that security teams focus on critical incidents.

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

21-10-2023

To
Dr.P.PAVAN KUMAR
Associate professor
KL UNIVERSITY.
VIJAYAWADA

Sir,

Subject: Request invitation for delivering expert lecture Two-day seminar on "
AI IN CYBERSECURITY:" on dates 26-10-2023 &27-10-2023– Reg.

Respected Sir,

The department of AI&ML., RKCE, Kethanakonda (V).Ibrahimpatnam(M), Andhra
Pradesh is organizing a two-day Seminar on Advancement in AI&ML. during 26-10-
2023 &27-10-2023. I am happy to invite you as a Resource Person. I request you to
accept the invitation and arrange to send the relevant study material so as to include
in the course book.

Thanking You,

Yours Sincerely

SK.SHABAAZ
HOD-AI&ML

**Coordinator-IQAC
RKCE**

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

REPORT ON AI IN CYBERSECURITY

Introduction

Artificial Intelligence (AI) has become an integral tool in the evolution of cybersecurity. With the increasing sophistication of cyber threats, traditional security measures alone are no longer sufficient to safeguard sensitive data, systems, and infrastructure. AI in cybersecurity leverages machine learning (ML), natural language processing (NLP), and data analytics to detect, prevent, and respond to threats in real-time. This report explores how AI is transforming cybersecurity, its applications, benefits, challenges, and future trends.

AI Applications in Cybersecurity

1. **Threat Detection and Prevention**
   - **Anomaly Detection:** AI systems analyze vast amounts of network traffic and system logs to identify unusual patterns that may signify potential security breaches, such as malware or intrusion attempts.
   - **Intrusion Detection Systems (IDS):** AI-enhanced IDS solutions learn from historical data to identify threats more efficiently than traditional methods.
   - **Phishing Detection:** AI-powered systems use NLP and ML to detect phishing emails, websites, and messages by analyzing the content, metadata, and sender behavior.

2. **Behavioral Analytics**
   - **User and Entity Behavior Analytics (UEBA):** AI tracks the normal behavior of users, devices, and applications within a network. When unusual behavior is detected, such as unauthorized access or abnormal file transfers, it triggers alerts for investigation.
   - **Insider Threat Detection:** By analyzing patterns and behaviors within an organization, AI can identify potential insider threats (e.g., disgruntled employees or compromised accounts) that traditional security systems may miss.

3. **Automated Incident Response**
   - **Automated Remediation:** AI systems can autonomously respond to incidents by isolating affected systems, blocking malicious IP addresses, or disabling compromised accounts. This rapid response minimizes the damage caused by attacks.
   - **Playbooks and Response Automation:** AI can use predefined playbooks to execute automated responses to security incidents, reducing the burden on security teams and accelerating mitigation efforts.

4. **Threat Intelligence and Prediction**
   - **Threat Intelligence Platforms (TIPs):** AI can process massive datasets to predict emerging threats, analyze cyberattack trends, and assess vulnerabilities before they are exploited.
   - **Predictive Analytics:** Machine learning algorithms can identify patterns and predict potential attacks before they occur, allowing organizations to strengthen defenses proactively.

5. **Malware Analysis and Detection**
   - **Static and Dynamic Analysis:** AI analyzes files or software code both statically (without execution) and dynamically (during execution) to identify malware and zero-day exploits.
   - **Automated Malware Classification:** Using ML, AI systems can classify malware based on its behavior, significantly reducing response time and improving detection rates.

Benefits of AI in Cybersecurity

1. **Improved Threat Detection**
   - AI can detect even the most sophisticated threats, including advanced persistent threats (APTs) and zero-day vulnerabilities, with greater accuracy and fewer false positives.

2. **Enhanced Efficiency**
   - AI automates routine security tasks, such as monitoring and incident response, freeing up human resources to focus on more complex tasks and strategic decision-making.

3. **Scalability**
   - AI systems can scale to handle massive amounts of data, something that traditional cybersecurity solutions struggle to achieve. This is particularly important as organizations grow and generate more data.

4. **Real-Time Response**
   - AI enables real-time detection and response, significantly reducing the window of opportunity for cyber attackers.

5. **Cost Reduction**
   - By automating tasks and improving the accuracy of threat detection, AI can reduce the costs associated with cybersecurity breaches, as well as the manpower required to manage security operation.

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456

About AI IN CYBERSECURITY:

- Artificial Intelligence (AI) is rapidly transforming cybersecurity by enhancing both defensive and offensive capabilities. Here's how AI is being used in the field:

- 1. Threat Detection and Prevention

- AI can process massive amounts of data and recognize patterns that might indicate potential security threats. Machine learning models, a subset of AI, are particularly effective in detecting abnormal behavior, such as malware or phishing attempts, that may otherwise go unnoticed by traditional systems.

- Anomaly Detection: AI systems can learn what "normal" network traffic looks like and flag anything abnormal, such as unexpected spikes in data flow, which could signal an attack.

- Malware Detection: AI algorithms can identify previously unknown types of malware by recognizing their behavior, even without seeing the specific code before.

- 2. Automated Response

- AI systems can act quickly in response to threats. For example, when an intrusion is detected, AI-powered systems can automatically isolate infected systems, block malicious IPs, or disable compromised accounts without human intervention, reducing the time it takes to contain and mitigate damage.

- 3. Phishing Detection

- AI tools use natural language processing (NLP) and machine learning to analyze emails, websites, or messages to detect signs of phishing attempts. These systems can identify patterns, such as malicious links or suspicious language, to prevent users from falling victim to phishing scams.

- 4. Behavioral Analytics

- AI can be used for behavior-based security. By continuously monitoring and analyzing user activity across networks, AI models can spot deviations from typical user behavior. For example, if a user suddenly tries to access sensitive data they typically don't interact with, this might trigger an alert for further investigation.

- 5. Vulnerability Management

- AI is used to automatically identify and prioritize vulnerabilities in systems. AI-powered tools can quickly analyze large amounts of code or configurations to find potential weaknesses that attackers might exploit, helping organizations stay ahead of potential breaches.
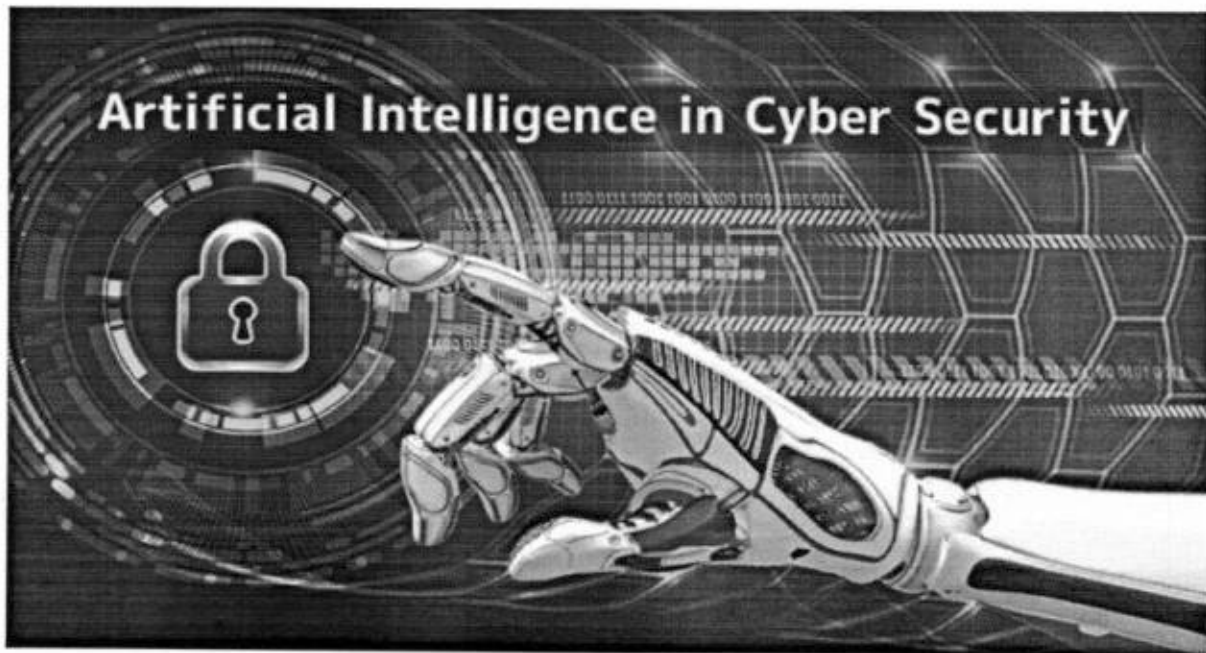
**Coordinator-IQAC
RKCE**

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

AI IN CYBERSECURITY:

Artificial Intelligence in Cyber Security

AI is playing an increasingly vital role in cybersecurity, offering powerful tools to detect, prevent, and respond to cyber threats. Here are several ways AI is being applied in this field:

1. Threat Detection and Prevention

- **Anomaly Detection:** AI can analyze large volumes of network data to identify patterns and detect anomalies that may indicate malicious activity. Machine learning algorithms can learn the "normal" behavior of a system and flag deviations that could suggest a breach or attack.

- **Intrusion Detection Systems (IDS):** AI-driven IDS solutions can automatically recognize and respond to suspicious activities in real-time, minimizing human intervention and accelerating response times.

2. Malware Analysis

- AI-powered tools can automatically identify and classify new types of malware. By analyzing the behavior of files or processes in a system, AI can predict whether they pose a potential threat, even if the malware has never been seen before.

- **Behavioral Analysis:** Instead of relying solely on signature-based methods (which may fail to detect new malware), AI can track and analyze behaviors, allowing it to detect zero-day threats and sophisticated evasive techniques.

3. Phishing Detection

- AI systems are increasingly used to detect phishing emails and websites. Machine learning models are trained to identify patterns in email content, URLs, and sender behavior that are characteristic of phishing attacks, helping prevent data breaches and fraud.

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456.

5. Advanced Threat Intelligence

- AI can analyze vast amounts of data from various sources (social media, dark web, internal logs) to provide actionable intelligence about emerging threats. By identifying trends and potential vulnerabilities, AI helps organizations stay ahead of attackers.

6. Security Automation

- Many cybersecurity tasks, like patch management, vulnerability scanning, and log analysis, can be automated using AI. This not only reduces the workload of security teams but also ensures that critical tasks are performed consistently and quickly.

7. User Behavior Analytics (UBA)

- AI systems can analyze users' typical behavior within a network and flag any deviations that could indicate a compromised account or insider threat. For example, logging in from unusual locations or accessing sensitive files without authorization can trigger alerts for further investigation.

8. Predictive Security

- By examining patterns in historical data, AI can predict potential future cyber threats and vulnerabilities. This proactive approach helps organizations strengthen their defenses before an attack occurs.

Challenges and Limitations:

While AI offers significant benefits, there are some challenges to consider:

- **False Positives:** AI systems may incorrectly flag benign activity as a threat, leading to unnecessary alerts and resource allocation.

Coordinators   HOD-AIML   Principal

Coordinator-IQAC
RKCE

- ### 6. Security Automation

- AI-driven security platforms can automate routine cybersecurity tasks like system patching, vulnerability scanning, or policy enforcement. This reduces the administrative burden on security teams, allowing them to focus on higher-priority tasks.
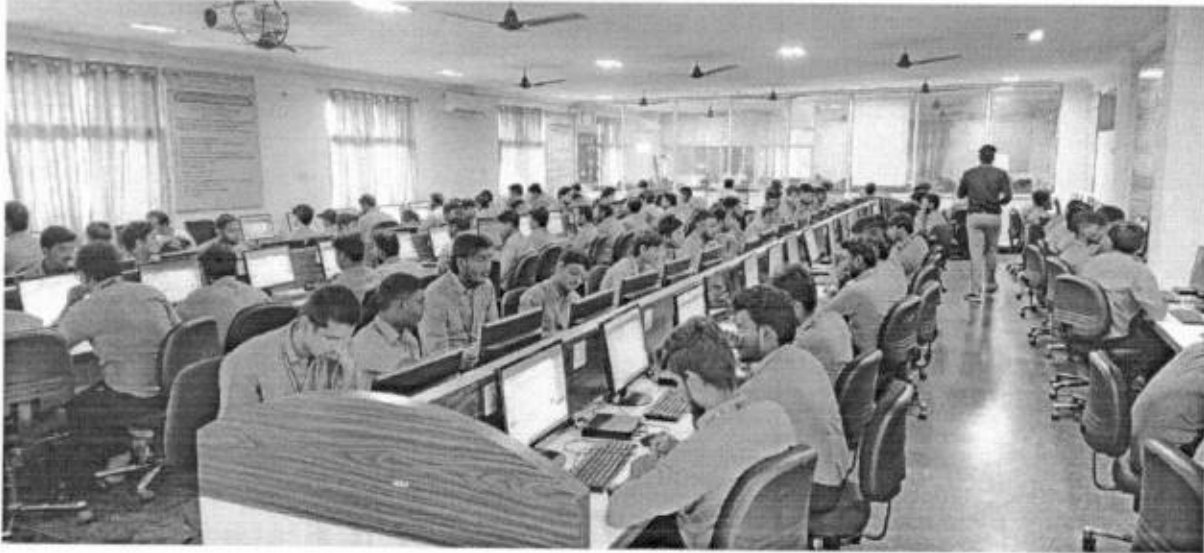
2. AI Technologies in Cybersecurity
- **Machine Learning (ML):** How algorithms detect patterns and predict threats.
- **Natural Language Processing (NLP):** AI in threat intelligence, analyzing communication, and detecting phishing attacks.
- **Anomaly Detection:** Identifying abnormal network traffic and user behavior.
- **Automation:** AI-based automation of routine cybersecurity tasks to save time and reduce human error.
- **Deep Learning:** Neural networks for identifying complex and evolving threats.

3. AI for Threat Detection and Prevention
- Real-time threat detection using AI algorithms.
- Predictive analytics to forecast and mitigate potential breaches.
- AI-powered firewalls and intrusion detection systems (IDS).
- Behavior analysis to spot insider threats.
- Case studies of AI successfully thwarting major cybersecurity threats.
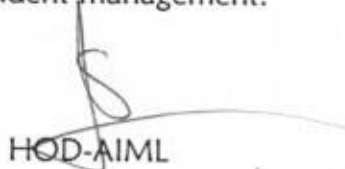
4. AI in Risk Management
- How AI can help with vulnerability assessments and risk profiling.
- AI tools for prioritizing cybersecurity efforts based on threat severity and business impact.
- Automating risk reporting and incident management.

Coordinators   HOD-AIML   Principal

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456

RK COLLEGE OF ENGINEERING

(APPROVED BY AICTE, NEW DELHI & AFFILIATED TO JNTUK, KAKINADA)
An ISO 9001 : 2015 Certified Institution
Kethanakonda(V), Ibrahimpatnam(M), Vijayawada, Amaravati, AP - 521456
Phone No: 08659 - 282956 / 66   Website: www.rkce.in

SRC e-solutions   vXL   # Certificate   **MICROLINK** MICROLINK INFORMATION TECNOLOGIES

This is to certify that Mr./ Ms. _____

has Successfully completed a Course / Workshop / Seminar on " _Al in Cyber_

_Security_____ " from _25/10/2023_ to _26/10/2023_

in association with _VXL_____ at RK College of Engineering.

CO-ORDINATOR   HOD   PRINCIPAL

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456

Coordinator-IQAC
RKCE

Feedback form for Two days seminar on "AI IN CYBERSECURITY"

* (0-Low, 5 High)

Sl. No.	Hall Ticket Number	Information was new to you? (Yes/No)	Would you like to learn more about this topic? (Yes/No)	Rate* the Speaker Knowledge.	Rate* the Speaker presentation.	Rate* the content of slides.	Rate* the session compared to your expectations.	Rate* the Overall session	Additional comments
1	22MC1A6101	Yes	Yy	5	5	5	5	5	Good
2	22MC1A6102	Yes	Yes	5	5	5	5	5	Good
3	22MC1A6103	Yes	Yy	5	5	5	5	5	Good
4	22MC1A6104	Yy	Yy	5	5	5	5	5	Good
5	22MC1A6105	Yes	Yy	5	5	5	5	5	Good
6	22MC1A6107	Yy	Yes	5	5	5	5	5	Good
7	22MC1A6108	Yes	Yy	5	5	5	5	5	Good
8	22MC1A6109	Yes	Yy	5	5	5	5	5	Good
9	22MC1A6110	Yes	Yy	5	5	5	5	5	Good
10	22MC1A6111	Yy	Yy	5	5	5	5	5	Good
11	22MC1A6113	Yy	Yes	5	5	5	5	5	Good
12	22MC1A6115	Yy	Yy	5	5	5	5	5	Good
13	22MC1A6117	Yes	Yy	5	5	5	5	5	Good
14	22MC1A6118	Yy	Yy	5	5	5	5	5	Good

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456

15	22MC1A6119	Yes	Yes	5	5	5	5	5	Good
16	22MC1A6120	Yes	Yes	5	5	5	5	5	Good
17	22MC1A6121	Yes	Yes	5	5	5	5	5	Good
18	22MC1A6122	Yes	Yy	5	5	5	5	5	Good
19	22MC1A6123	Yes	Yy	5	5	5	5	5	Good
20	22MC1A6124	Yes	Yy	5	5	5	5	5	Good
21	22MC1A6125	Yes	Yy	5	5	5	5	5	Good
22	22MC1A6126	Yes	Yy	5	5	5	5	5	Good
23	22MC1A6127	Yes	Yy	5	5	5	5	5	V.Good
24	22MC1A6128	yy	Yy	5	5	5	5	5	Good
25	22MC1A6129	Yes	Yes	5	5	5	5	5	Good
26	22MC1A6130	Yy	Yes	5	5	5	5	5	Good
27	22MC1A6131	Yy	Yes	5	5	5	5	5	Good
28	22MC1A6132	Yy	Yy	5	5	5	5	5	Good
29	22MC1A6133	Yy	Yes	5	5	5	5	5	Good
30	22MC1A6134	Yes	Yy	5	5	5	5	5	Good
31	22MC1A6135	Yes	Yy	5	5	5	5	5	V. good
32	22MC1A6136	Yy	Yy	5	5	5	5	4	Good

Coordinator-IQAC
RKCE

PRINCIPAL
R K COLLEGE OF ENGINEERING
Kethanakonda (V), Ibrahimpatnam (M),
Vijayawada, AMARAVATI-521 456

33	22MC1A6137	Yes	Yes	5	5	5	5	5	Good
34	22MC1A6138	Yes	Yes	5	5	5	5	5	Good
35	22MC1A6139	Yes	Yes	5	5	5	5	5	Good
36	22MC1A6140	Yes	Yes	5	5	5	5	5	Good
37	22MC1A6141	Yes	Yes	5	5	5	5	5	Good
38	22MC1A6142	Yes	Yes	5	5	5	5	5	Good
39	22MC1A6144	Yes	Yes	5	5	5	5	5	Good
40	22MC1A6145	Yes	Yes	5	5	5	5	5	Good
41	22MC1A6146	Yes	Yes	5	5	5	5	5	Good
42	22MC1A6147	Yes	Yes	5	5	5	5	5	Good
43	22MC1A6148	Yes	Yes	5	5	5	5	5	Good
44	22MC1A6149	Yes	Yes	5	5	5	5	5	Good
45	22MC1A6150	Yes	Yes	5	5	5	5	5	Good
46	22MC1A6151	Yes	Yes	5	5	5	5	5	Good
47	23MC5A6101	Yes	Yes	5	5	5	5	5	Good
48	23MC5A6102	Yes	Yes	5	5	5	5	5	Good
49	23MC5A6103	Yes	Yes	5	5	5	5	5	Good
50	22MC1A0402	Yes	Yes	5 5	5	5	5	5	Good

51	22MC1A0403	Yes	Yes	5	5	5	5	5	Excellent
52	22MC1A0404	Yes	Yes	5	5	5	5	5	Good
53	22MC1A0405	Yes	Yes	5	5	5	5	5	Good
54	22MC1A0406	Yes	Yes	5	5	5	5	5	Good
55	22MC1A0407	Yes	Yes	5	5	5	5	5	Good
56	22MC1A0408	Yes	Yes	5	5	5	5	5	Good
57	22MC1A0409	Yes	Yes	5	5	5	5	5	Good
58	22MC1A0410	Yes	Yes	5	5	5	5	5	Good
59	22MC1A0411	Yes	Yes	5	5	5	5	5	Good
60	22MC1A0412	Yes	Yes	5	5	5	5	5	Good
61	22MC1A0413	Yes	Yes	5	5	5	5	5	Good
62	22MC1A0414	Yes	Yes	5	5	5	5	5	Good
63	22MC1A0416	Yes	Yes	5	5	5	5	5	Good
64	22MC1A0417	Yes	Yes	5	5	5	5	5	Good
65	22MC1A0418	Yes	Yes	5	5	5	5	5	Good
66	22MC1A0419	Yes	Yes	5	5	5	5	5	Good
67	22MC1A0420	Yes	Yes	5	5	5	5	4	Good
68	22MC1A0421	Yes	Yes	5	5	5	5	4	Good

69	22MC1A0422	Yes	Yes	5	5	5	5	5	V.Good
70	22MC1A0423	Yes	Yes	5	5	5	5	5	V.Good
71	22MC1A0424	Yes	Yes	5	5	5	5	5	V.Good
72	22MC1A0425	Yes	Yes	5	5	5	5	5	Good
73	22MC1A0426	Yes	Yes	5	5	5	5	4	Good
74	22MC1A0427	Yes	Yes	5	5	5	5	4	Good
75	22MC1A0428	Yes	Yes	5	5	5	5	4	Good
76	22MC1A0429	Yes	Yes	5	5	5	5	4	Good
77	22MC1A0430	Yes	Yes	5	5	5	5	5	Good
78	22MC1A0431	Yes	Yes	5	5	5	5	5	Good
79	22MC1A0432	Yes	Yes	5	5	5	5	5	Good
80	22MC1A0433	Yes	Yes	5	5	5	5	5	Good
81	22MC1A0434	Yes	Yes	5	5	5	5	5	Good
82	22MC1A0435	Yes	Yes	5	5	5	5	5	Excellent
83	22MC1A0436	Yes	Yes	5	5	5	5	4	Good
84	22MC1A0437	Yes	Yes	5	5	5	5	4	Good
85	22MC1A0438	Yes	Yes	5	5	5	5	4	Good
86	22MC1A0440	Yes	Yes	5	5	5	5	4	Good

87	22MC1A0441	Yes	Yes	5	5	5	5	5	Excellent
88	22MC1A0442	Yes	Yes	5	5	5	5	5	Excellent
89	22MC1A0443	Yes	Yes	5	5	5	5	5	Good
90	22MC1A0444	Yes	Yes	5	5	5	5	5	V·Good
91	22MC1A0445	Yes	Yes	5	5	5	5	5	V·Good
92	22MC1A0446	Yes	Yes	5	5	5	5	5	Good
93	22MC1A0447	Yes	Yes	5	5	5	5	5	Good
94	22MC1A0448	Yes	Yes	5	5	5	5	4	Good
95	22MC1A0449	Yes	Yes	5	5	5	5	4	Good
96	22MC1A0450	Yes	Yes	5	5	5	5	4	Good
97	22MC1A0451	Yes	Yes	5	5	5	5	4	Good
98	22MC1A0452	Yes	Yes	5	5	5	5	4	Good
99	22MC1A0453	Yes	Yes	5	5	5	5	4	Good
100	22MC1A0454	Yes	Yes	5	5	5	5	5	Good
101	22MC1A0455	Yes	Yes	5	5	5	5	5	Good
102	22MC1A0456	Yes	Yes	5	5	5	5	5	Good
103	22MC1A0457	Yes	Yes	5	5	5	5	5	Good
104	22MC1A0458	Yes	Yes	5			5	5	Good

105	22MC1A0459	Yy	Yy	5	5	5	5	5	Good
106	22MC1A0460	Yy	Yy	5	5	5	5	5	Good
107	23MC5A0401	Yy	Yy	5	5	5	5	5	Good
108	23MC5A0402	Yy	Yes	5	5	5	5	5	V Good
109	23MC5A0403	Yy	Yy	5	5	5	5	5	V. Good
110	23MC5A0404	Yy	Yy	5	5	5	5	5	Good
111	23MC5A0405	Yy	Yy	5	5	5	5	5	Good

COORDINATOR

HOD

PRINCIPAL

Coordinator-IQAC
RKCE