NAAC: C (II CYCLE)

Cycle)

CHATRAPATHI SIVAJI TRI SATA JAYANTHI (CSTS) GOVT. KALASALA

Enter to Learn - Leave to Serve

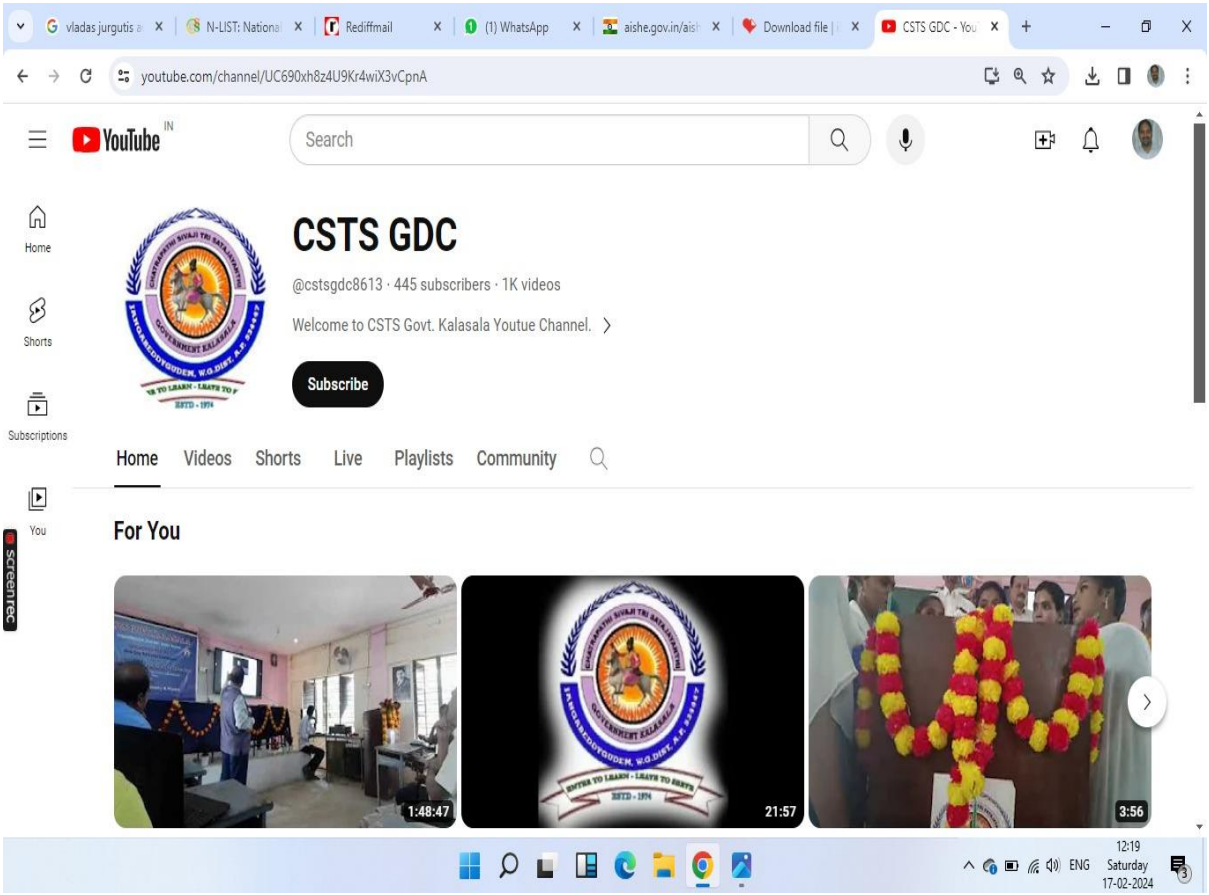
Jangareddigudem, Eluru Dist

Phone : 08821-225310, Visit us at : www.cstsgk.ac.in

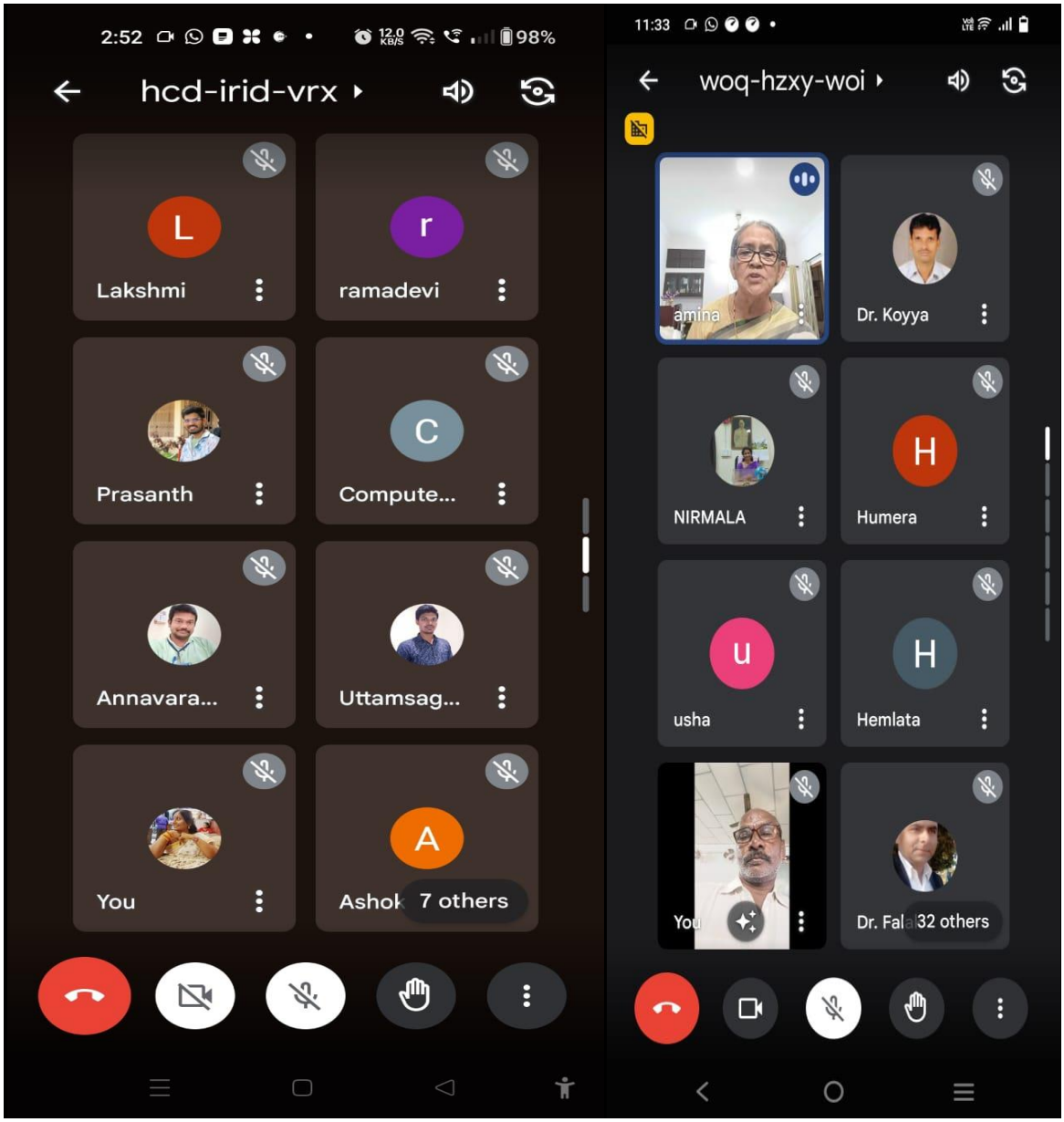
E- Mail : jangareddigudem.manatv@gmail.com

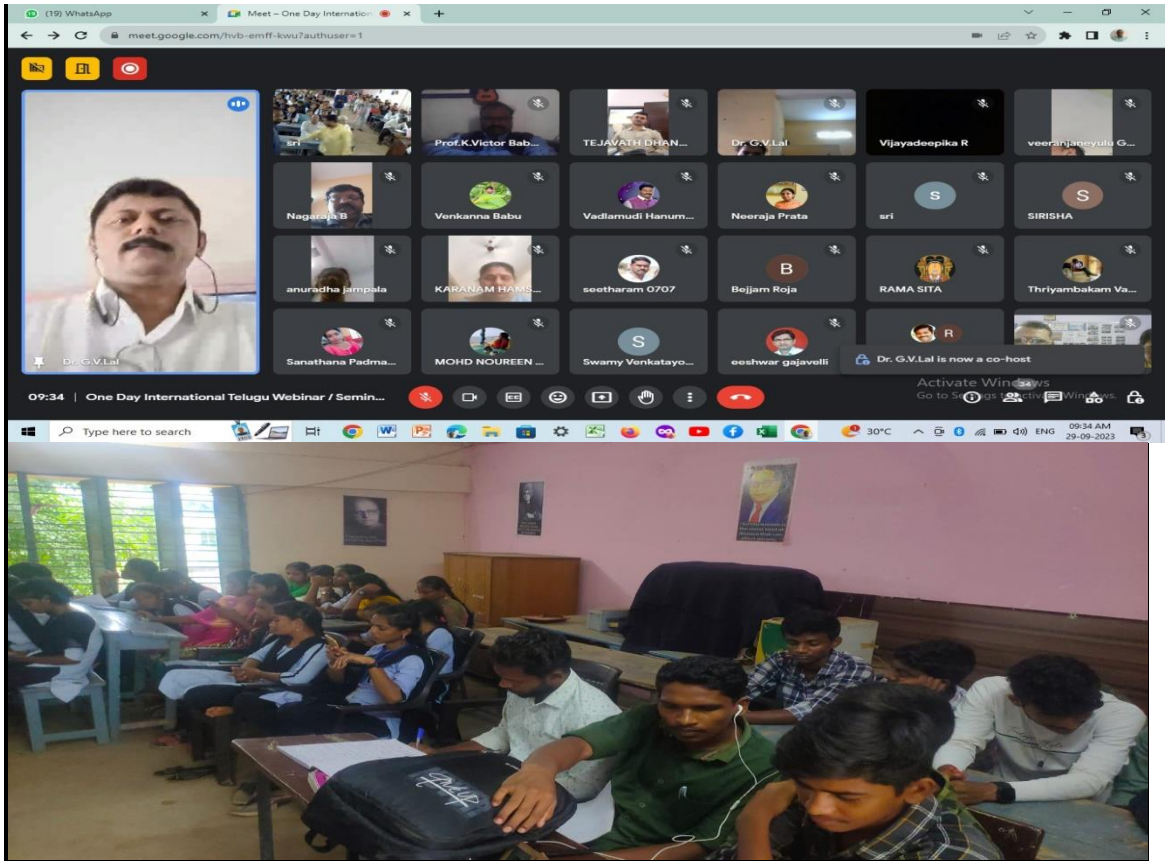
WEBINARS, SEMINAR CONFERENCES, WORK SHOPS

S.NO	Date	Department	Webinars, Conferences, Work shops	Topic
1	23-08-2023	ENGLISH	WORKSHOP	An Effective Way of Teaching in English Medium
2	29-09-2023	TELUGU	INTERNATIONAL SEMINAR	Different trends in modern Telugu Literature
3	07-10-2023	COMMERCE/MATHEMATICS-COMPUTERS	NATIONAL CONFERENCE	Future Challenges and Opportunities in Cyber Security
4	17-10-2023	ECONOMICS	WORKSHOP	Self Help Groups
5	04-11-2023	HISORY/POLITICAL SCIENCE	WORKSHOP	Nurturing Young Administrators
6	08-11-2023	MATHEMATICS	WEBINAR	Numerical Analysis
6	09-11-2023	ECONOMICS	WORKSHOP	Research Methodology
7	10-11-2023	COMMERCE	WORKSHOP	Role of Accounting in Nation Building
8	30-11-2023	BOTANY, ZOOLOGY, HORTICULTURE	NATIONAL SYMPOSIUM	New Trends in Biological Sciences
9	05-01-2024	CHEMISTRY	NATIONAL CONFERENCE	NANO Materials for next Generation

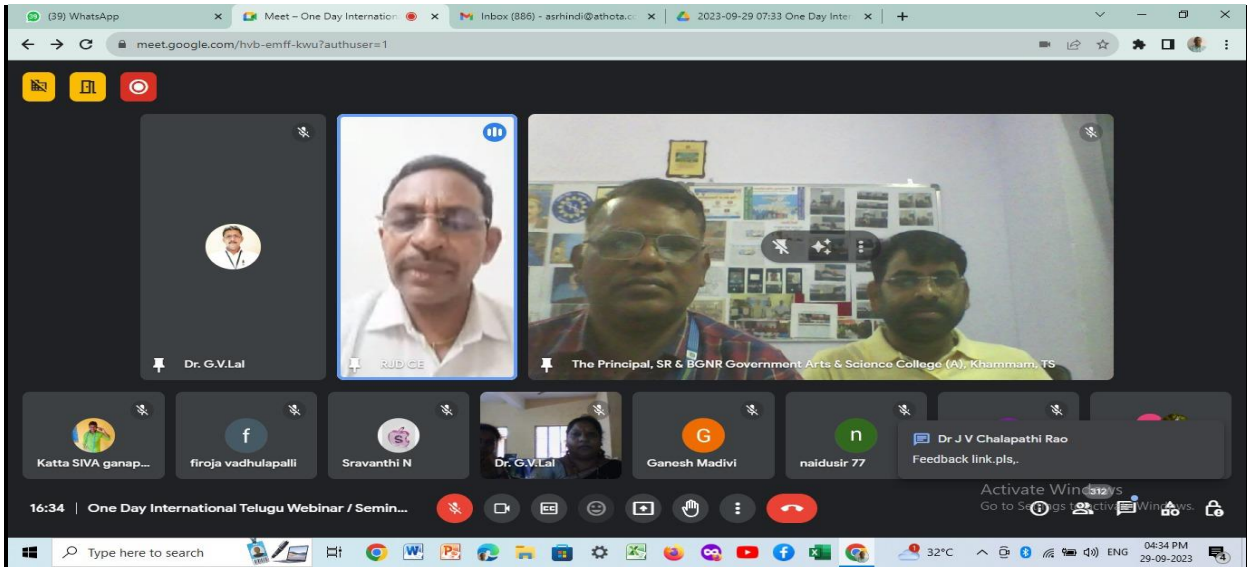

youtube.com/channel/UC690xh8z4U9Kr4wiX3vCpnA
YouTube IN
Search
CSTS GDC
@cstsgdc8613 · 445 subscribers · 1K videos
Welcome to CSTS Govt. Kalasala Youtue Channel.
Subscribe
Home
Videos
Shorts
Live
Playlists
Community
For You
1:48:47
21:57
3:56
Home
Shorts
Subscriptions
You
screenrec
ENG
12:19
Saturday
17-02-2024


REDMI NOTE 12 5G | VINAY
07/02/2024 11:17


2:52
98%
hcd-irid-vrx
L
Lakshmi
r
ramadevi
Prasanth
C
Compute...
Annavara...
Uttamsag...
You
A
Ashok
7 others
11:33
woq-hzxy-woi
amina
Dr. Koyya
NIRMALA
H
Humera
u
usha
H
Hemlata
You
Dr. Fal
32 others


(19) WhatsApp
Meet – One Day Internation
meet.google.com/hvb-emff-kwu?authuser=1
Dr. G.V.Lal
Prof.K.Victor Bab...
TEJAVATH DHAN...
Dr. G.V.Lal
Vijayadeepika R
Nagaraja B
Venkanna Babu
Vadlamudi Hanum...
Neeraja Prata
sri
SIRISHA
anuradha jampala
KARANAM HAMS...
seetharam 0707
Bejjam Roja
RAMA SITA
Thriyambakam Va...
Sanathana Padma...
MOHD NOUREEN ...
Swamy Venkatayo...
eeshwar gajavelli
Dr. G.V.Lal is now a co-host
09:34 | One Day International Telugu Webinar / Semin...
Activate Windows
Type here to search
30°C
ENG
09:34 AM
29-09-2023


meet.google.com/hvb-emff-kwu
venkataramana Indianlanguages
CSTS GOVT KALASALA, JANGAREDDIGUDEM
Sruthi Miriy...
Chitti Karam
Shirisha Kur...
Pavani Pras...
Mandru So...
madhu sun...
292 others
Dr. G.V.Lal
15:27 | hvb-emff-kwu


meet.google.com/hvb-emff-kwu?authuser=1
Dr. G.V.Lal
The Principal, SR & BGNR Government Arts & Science College (A), Khammam, TS
Katta SIVA ganap...
firoja vadhulapalli
Sravanthi N
Dr. G.V.Lal
Ganesh Madivi
naidusir 77
Dr J V Chalapathi Rao
Feedback link.pls,.
16:34 | One Day International Telugu Webinar / Semin...


CSTS Govt Kalasala
GPS Map Camera
Jangareddigudem, Andhra Pradesh, India
12-13 NRAR GOVT DEGREE COLLEGE, Jangareddigudem, Andhra Pradesh 534447, India
Lat 17.131227°
Long 81.289638°
07/10/23 10:59 AM GMT +05:30
Google

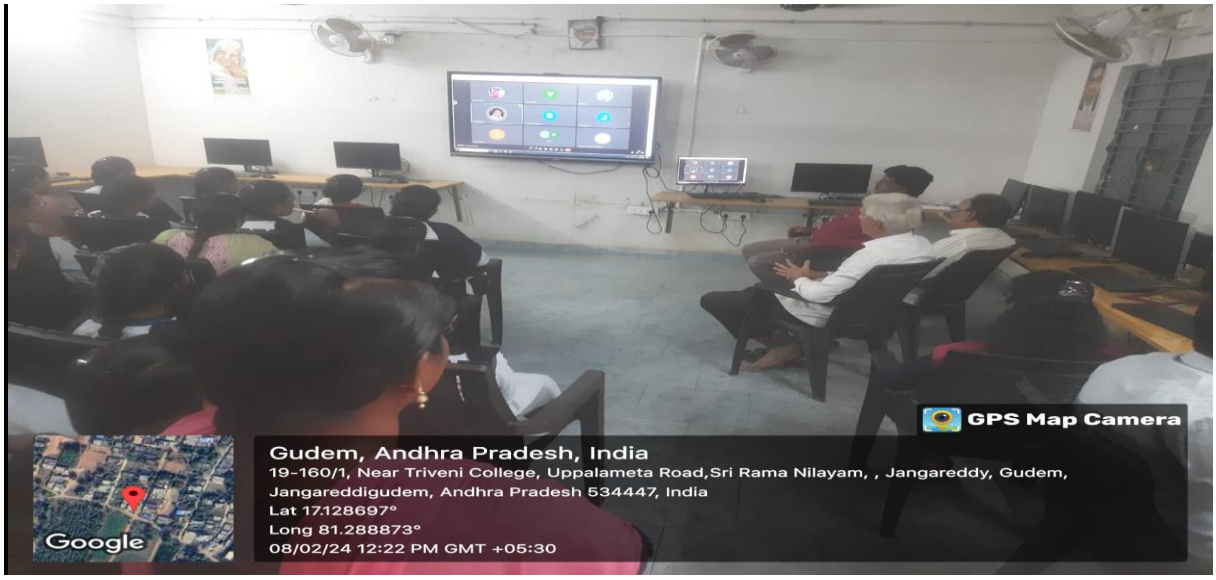

Govt.Kalasala
WELCOMES YOU TO
One Day National Conference
GPS Map Camera
Jangareddigudem, Andhra Pradesh, India
12-13 NRAR GOVT DEGREE COLLEGE, Jangareddigudem, Andhra Pradesh 534447, India
Lat 17.131238°
Long 81.2897°
07/10/23 11:19 AM GMT +05:30
Google


CSTS Govt.Kalasala
Jangareddigudem, Eluru Dist. Andhra Pradesh.
WELCOMES YOU TO
One Day National Conference
on
Opportunities in Cyber Security
Organized by
Computer Science
By
CSTS Govt Kalasala
REDMI NOTE 12 5G | VINAY
07/10/2023 16:04


CSTS Govt.Kalasala
Jangareddigudem, Eluru Dist. Andhra Pradesh.
WELCOMES YOU TO
One Day National Conference
on
Opportunities in Cyber Secu
7th October 2023 (Saturday)
09:00 AM – 05:00 PM
Organized by
Commerce, Computer Science & Mathe
By
REDMI NOTE 12 5G | VINAY
07/10/2023 15:47


CSTS Govt.Kalasala
Jangareddigudem, Eluru Dist. Andhra Pradesh.
WELCOMES YOU TO
One Day National Conference
on
Seminar Hall, CSTS Govt. Kalasala, Jangareddigudem
7th October 2023 (Saturday)
09:00 AM – 05:00 PM
Organized by
Commerce, Computer Science & Mathematics
By
Principal and Staff
CSTS Govt.Kalasala
REDMI NOTE 12 5G | VINAY
07/10/2023 16:06


CSTS Govt.Kalasala
Future Challenges and Opportunities in Cyber Security
REDMI NOTE 12 5G | VINAY
07/10/2023 15:42


GPS Map Camera
Gudem, Andhra Pradesh, India
19-160/1, Near Triveni College, Uppalameta Road,Sri Rama Nilayam, , Jangareddy, Gudem, Jangareddigudem, Andhra Pradesh 534447, India
Lat 17.128697°
Long 81.288873°
08/02/24 12:22 PM GMT +05:30
Google

PINGLE GOVT COLLEGE FOR WOMEN(A),HANUMAKONDA
(Accredited by NAAC with A Grade& ISO 9001-2015 CERTIFIED COLLEGE
(Permanently affiliated to Kakatiya University)

ONE DAY SEMINAR ON NUMARICAL ANALYSIS
Dt: 8th November,2023

COLLABORATION WITH
DEPARTMENT OF MATHEMATICS
PGCW(A),HANAMKONDA

Organizers
Dr CH BADARI NARAYANA
LECTURER IN MATHEMATICS
CSTS GOVERNMENT KALASALA
JANGA REDDI GUDEM
ELURU (DT)

Rersource person
Dr.B.Madhavi
BOS Chair person
Dept. Of Mathematics
PGCW(A),HNK


GPS Map Camera
Jangareddigudem, Andhra Pradesh, India
12-10, near GOVT DEGREE COLLEGE, Jangareddigudem, Andhra Pradesh 534447, India
Lat 17.131221°
Long 81.289413°
10/11/23 01:10 PM GMT +05:30
Google


CSTS GOVT. KALASALA
Jangareddigudem, Eluru Dist.
WELCOMES Y
ONE DAY NATIONAL W OP On
RESEARCH MET GY"
Venue: Seminar Hall, CSTS
Date : 9th-NOVE
Time : 10.0
CSTS GOVERNMENT KALASALA, JANGAREDDIGUDEM
WELCOMES
ONE DAY NATIONAL WORKSHOP


CSTS Govt.Kalasala


CSTS Govt.Kalasala
Jangareddigudem ,Eluru Dist, Andhra Pradesh

సామాజిక మార్పుకి నిదర్శనమే సాహిత్యంలో విభిన్న ధోరణులు

ఆచార్య దార్ల వెంకటేశ్వరరావు

భూమిపుత్ర, హైదరాబాద్:

తెలుగు సాహిత్యంలో విభిన్న ప్రక్రియలు, విభిన్న ధోరణులు రావడమనేది సమాజంలో వస్తున్న మార్పులకు, ఒక ప్రజాస్వామిక ఆలోచనా ధోరణికి నిదర్శనమని, తెలుగు సాహితీవేత్తల ప్రతిభా పాటవాలకు పాఠకులు పట్టం కట్టడమేనని హెచ్.సి.యు తెలుగు శాఖ అధ్యక్షులు ఆచార్య దార్ల వెంకటేశ్వరరావు వ్యాఖ్యానించారు. శుక్రవారం నాడు జంగారెడ్డిగూడెంలోని ఛత్రపతి శివాజీ త్రిశత జయంతి ప్రభుత్వ డిగ్రీ కళాశాలలో "ఆధునిక తెలుగు సాహిత్యంలో విభిన్న ధోరణులు" అనే అంశంపై ఒకరోజు అంతర్జాతీయ సదస్సు లో అంతర్జాలం ద్వారా ఆచార్య దార్ల వెంకటేశ్వరరావు ముఖ్యపత్రగా మాట్లాడారు. తెలుగు సాహిత్యం ఒకవైపు భారతీయ సమైక్యతను, సాంస్కృతిక వారసత్వాన్ని కొనసాగిస్తూనే, తెలుగు వారి అస్తిత్వాన్ని నిలుపుకుంటూ సామాజిక మార్పుని ఆహ్వానిస్తూ వివిధ సాహిత్య ధోరణులు వచ్చాయని ఆయన సోదాహరణంగా వివరించారు. వ్యాసుని భారతాన్ని తెలుగులో కవిత్రయం, వాల్మీకి రామాయణాన్ని వివిధ కవులు తెలుగులోకి అనుసృజన చేయడంతో పాటు, భాగవతం, మహాకవి కాళిదాసు రచనలు, ప్రబంధాలు, కావ్యాలు, తర్వాత కథలు, నవలలు, నాటకాలు, వచన కవిత్వం, మినీ కవిత్వం వంటి అనేక ప్రక్రియలు, రూపాల్లో ఎంతో వైవిధ్యంతో కూడిన సాహిత్యం వచ్చిందన్నారు. ఆధునిక వచన కవిత్వంలో వచ్చిన రూపపరమైన మార్పుల్లో మినీకవిత్వం, హైకూలు, నానీలు, నానోలు, ముక్తకాలు, టుమ్రీలు, మొగ్గలు, రవ్వలు, రెక్కలు మొదలైన ప్రయోగాలు కనిపిస్తున్నాయనీ వాటిని సాహిత్యంలో నూతనత్వానికీ, మార్పుకీ, నూతన అభిరుచులకు ప్రాతినిధ్యాలుగా తీసుకోవాలని ఆచార్య దార్ల వ్యాఖ్యానించారు. ఈ కార్యక్రమంలో ముఖ్య అతిథిగా కమీషన్ ఆఫ్ కాలేజియేట్ ఎడ్యుకేషన్ కమీషనర్ పోలాభాస్కర్ ఈ సదస్సులో సమర్పించబోయే ప్రసంగాలు, పరిశోధన వ్యాసాల సంచికను ఆవిష్కరించారు. ఈ కార్యక్రమంలో గౌరవఅతిథిగా జాయింట్ సెక్రటరీ డా.ఆర్.జేవిడ్ కుమారస్వామి, రీజనల్ జాయింట్ డైరెక్టర్ డా.చప్పిడి కృష్ణ, కళాశాల ప్రిన్సిపాల్ డా.ఎన్.ప్రసాద్ బాబు, వైస్ ప్రిన్సిపాల్ బి.శ్రీనివాసరావు,ఐక్యుఏసి కోర్డినేటర్ డా.ఎం.మధు, సదస్సు నిర్వాహకులు, తెలుగుశాఖ అధ్యక్షులు డా.జి.వెంకట్ లాల్, సహ నిర్వాహకులు

పి.నాగేశ్వరరావు, ప్రధాన వక్తలుగా వివిధ విశ్వవిద్యాలయాలు, కళాశాలలకు చెందిన నారాయణ స్వామి యోగి (న్యూజెర్సి), డా.తొట్టెంపూడి శ్రీగణేశ్ (జర్మనీ), ఆచార్య కొప్పుల ఈశ్వర్ బాబు (ఇథియోపియా), ఆచార్య విస్తాలి శంకరరావు (చెన్నై), ఆచార్య గోనానాయక్, ఆచార్య చింతకింద కాశీం (హైదరాబాద్), ఆచార్య ఎ.జ్యోతి(వరంగల్), ఆచార్య ఎన్.కృష్ణారావు (గుంటూరు), డా.కెవిఎన్ డి ప్రసాద్, డా.టి. సత్యనారాయణ (రాజమహేంద్రవరం), ఆచార్య జొన్నలగడ్డ వెంకటరమణ (మదురై), డా. బూసి వెంకటస్వామి (విశాఖపట్టణం) తదితరులు పాల్గొని తెలుగు సాహిత్యంలోని విభిన్నధోరణుల గురించి ప్రసంగించారు.

చత్రపతి శివాజీ త్రీ శతజయంతి ప్రభుత్వ డిగ్రీ కళాశాల లో నేషనల్ కాన్ఫరెన్స్

అక్టోబర్ 7 పత్రిజ్యోతి ప్రతినిధి
సివోసిటిఎస్ గవర్నమెంట్ కళాశాల జంగారెడ్డిగూడెం ఏలూరు డిస్ట్రిక్ట్ లో కళాశాల స్వర్ణోత్సవ కార్యక్రమాల ను పురస్కరించుకుని నేషనల్ కాన్ఫరెన్స్ నిర్వహించడం జరిగింది. డిపార్ట్మెంట్ ఆఫ్ కామర్స్, కంప్యూటర్ సైన్స్ వారి ఆధ్వర్యంలో నిర్వహించడం జరిగింది. ఈ సెమినార్ లో న్యూనార్ చాలెంజెస్ ఇంట్ ఇవల్యుషనీస్ ఇన్ సైబర్ సెక్యూరిటీ అనే అంశం మీద కాన్ఫరెన్స్ నిర్వహణ జరిగింది. ఈ కార్యక్రమానికి కళాశాల ప్రిన్సిపాల్ డాక్టర్ ఎన్ ప్రసాద్ బాబు అధ్యక్షత వహించారు. ప్రిన్సిపల్ డాక్టర్ ప్రసాద్ బాబు మాట్లాడుతూ ఈనాడు సైబర్ నేరాలు బాగా పెరగడంతో ఎంతోమంది అర్థికంగా నష్టాన్ని గురవుతున్నారు అన్నారు. ఈ కార్యక్రమానికి ముఖ్యఅతిథిగా కాలేజీ డెవలప్మెంట్ కౌన్సిల్ మెంబర్ ఎం వెంకటేశ్వరరావు విద్యార్థులనుద్దేశించి మాట్లాడారు. రిసోర్స్ పర్సన్ అనిల్ రాచమళ్ళఫౌండర్ ఎండ్ సిఇఓ ఫ్రాంజేమన్ క్రూం హైదరాబాద్ వాట్సాప్, ఫేస్బుక్, ఇమెయిల్ మొబైల్ హాకింగ్స్ ఏవిధంగా జరుగుతాయి రిసోర్సుపర్సన్ శ్రీ కిరణ్ కుమార్ కందుల మాట్లాడుతూ యువత తమకు సంబంధించిన వ్యక్తిగత ఇన్ఫర్మేషన్ ని జాగ్రత్తగా ఉంచుకోవడం వల్ల సైబర్ నేరాలు జరగకుండా అరికట్టవచ్చు అన్నారు. ఈ కార్యక్రమంలో మరొక రిసోర్స్ పర్సన్ శ్రీనివాస్ భూసారపు ఫౌండర్ చీఫ్ ఇన్ఫర్మేషన్ సెక్యూరిటీ ఆఫీసర్, సిఎఫ్ ఆర్ డి ఐ డైరెక్టర్ మాట్లాడుతూ సైబర్ సెక్యూరిటీ ద్వారా సైబర్ నేరాలని అరికట్టవచ్చు కోడింగ్ స్కిల్స్ ని పెంచుకోవాలి అని అన్నారు. ఈ కార్యక్రమంలో మరొక ప్రత్యేక విశిష్ట అతిథి కిరణ్ కుమార్ కందుల సెక్యూరిటీ స్పెషలిస్ట్ ఇన్ డిజిటల్ సినిమా ఆపరేషన్స్ మాట్లాడుతూ ఏ విధంగా హ్యాకింగ్ కి గురి అవుతుంది ఏ జాగ్రత్తలు మనం తీసుకోవాలి అనే అంశాన్ని గురించి వివరించారు. ఈ కార్యక్రమంలో ముఖ్య అతిథి అనిల్ కుమార్ సైకాలజిస్ట్ మాట్లాడుతూ ఈరోజు సమాజంలో యువతలో ఒక దురాశను కల్పించి తద్వారా సైబర్ నేరాలకు పూనుకుంటున్నారు అని అన్నారు. ఈ కార్యక్రమం డాక్టర్ బోలా భాస్కర్ ఐఏఎస్ కమిషనర్ ఆఫ్ కాలేజ్ ఎడ్యుకేషన్ ఆంధ్ర ప్రదేశ్ వారి ప్రసంగంతో ఈ కార్యక్రమం ప్రారంభమైంది ఈ కార్యక్రమంలో జోన్ వన్ అండ్ టు రీజనల్ జాయింట్ డైరెక్టర్ డాక్టర్ చప్పిడి కృష్ణ అంతర్జాలం ద్వారా అధ్యక్షోపన్యాసం చేశారు ఈ కార్యక్రమంలో కళాశాల డిపార్ట్మెంట్ ఆఫ్ కామర్స్ లెక్చరర్ డాక్టర్ కే ఉత్తమ్ సాగర్ సి. హెచ్ రమాదేవి కే వి వి శిరీష కళాశాల మ్యాథమెటిక్స్ డిపార్ట్మెంట్ సిహెచ్ బుచ్చి నారాయణ, కంప్యూటర్ సైన్స్ విభాగం రాజా శ్రీకాంత్ కళాశాల వైస్ ప్రిన్సిపల్ వి శ్రీనివాసరావు యు వెంకటరాయుడు కళాశాల బర్సార్ డాక్టర్ ఎం మధు డాక్టర్ వెంకట లాల్ మరియు కాలేజ్ టీచింగ్ అండ్ నాన్ టీచింగ్ స్టాఫ్ విద్యార్థిని విద్యార్థులు పాల్గొన్నారు

చత్రపతి శివాజీ త్రీ శతజయంతి ప్రభుత్వ డిగ్రీ కళాశాలలో నేషనల్ కాన్ఫరెన్స్

జంగారెడ్డిగూడెం, అక్టోబర్ 8 (గోదావరి విలేఖరి) : సిఎస్‌టిఎస్ గవర్నమెంట్ కళాశాల జంగారెడ్డిగూడెం ఏలూరు జిల్లాలో కళాశాల స్వర్ణోత్సవ కార్యక్రమాలను పురస్కరించుకుని నేషనల్ కాన్ఫరెన్స్ నిర్వహించడం జరిగింది. డిపార్ట్మెంట్ ఆఫ్ కామర్స్, కంప్యూటర్ సైన్స్ మ్యాథమెటిక్స్ వారి ఆధ్వర్యంలో నిర్వహించడం జరిగింది. ఈ సెమినార్ లో ఫ్యూచర్ చాలెంజెస్ అండ్ ఆపర్చునిటీస్ ఇన్ సైబర్ సెక్యూరిటీ అనే అంశం మీద కాన్ఫరెన్స్ నిర్వహణ జరిగింది. ఈ కార్యక్రమానికి కళాశాల ప్రిన్సిపాల్ డాక్టర్ ఎన్ ప్రసాద్ బాబు అధ్యక్షత వహించారు. ప్రిన్సిపల్ డాక్టర్ ప్రసాద్ బాబు మాట్లాడుతూ ఈనాడు సైబర్ నేరాలు బాగా పెరగడంతో ఎంతోమంది ఆర్థికంగా నష్టానికి గురవుతున్నారు అని అన్నారు. ఇలాంటి కార్యక్రమాలు జరిపించడం వల్ల విద్యార్థిని విద్యార్థులు ఈ సైబర్ నేరాలకు లోను అవ్వకుండా ఉంటారని అన్నారు. ఈ కార్యక్రమానికి ముఖ్యఅతిథిగా కాజీజీ డెవలప్మెంట్ కౌన్సిల్ మెంబర్ ఎం వెంకటేశ్వరరావు విద్యార్థులనుదేశించి మాట్లాడారు. రిసోర్స్ పర్సన్ అనీల్ రాచమళ్ళఫౌండర్ ఎండ్ సి ఫౌండేషన్ ప్రాం హైదరాబాద్ వాట్సప్, ఫేస్బుక్, ఇమెయిల్ మొబైల్ హాకింగ్స్ ఏవిధంగా జరుగుతాయి వాటిని నివారించాలంటే ఏ విధమైన జాగ్రత్తలు తీసుకోవాలి అనే విషయాలు తెలిపారు.మరొక రిసోర్సుపర్సన్ కిరణ్ కుమార్ కందుల మాట్లాడుతూ యువత తమకు సంబంధించిన వ్యక్తిగత ఇన్ఫర్మేషన్ ని జాగ్రత్తగా ఉంచుకోవడం వల్ల సైబర్ నేరాలు జరగకుండా అరికట్టవచ్చు అన్నారు. ఈ కార్యక్రమంలో మరొక రిసోర్స్ పర్సన్ అయినా శ్రీనివాస్ భూసారవు ఫార్మర్ చీఫ్ ఇన్ఫర్మేషన్ సెక్యూరిటీ ఆఫీసర్, పిఎఫ్ ఆర్ డి ఐ డైరెక్టర్ మాట్లాడుతూ సైబర్ సెక్యూరిటీ ద్వారా సైబర్

నేరాలని అరికట్టవచ్చు కోడింగ్ స్కిల్స్ ని పెంచుకోవాలి అని అన్నారు. ఈ కార్యక్రమంలో మరొక ప్రత్యేక విశిష్ట అతిథి కిరణ్ కుమార్ కందుల సెక్యూరిటీ స్పెషలిస్ట్ ఇన్ డిజిటల్ సినిమా ఆపరేషన్స్ మాట్లాడుతూ నేను మాట్లాడుతూ సినీ ఇండస్ట్రీలో పైరసీని అరికట్టాలంటే ఏం చేయాలి ఎందువల్ల సినిమాలు పైరసీకి గురి అవుతున్నాయి ఏ విధంగా హ్యాకర్స్ హాక్ చేస్తున్నారు నివారించాలంటే ఏ విధమైన టెక్నిక్ ఉపయోగించాలి నేడు డిజిటల్ రంగమంతా ఏ విధంగా హ్యాకింగ్ కి గురి అవుతుంది ఏ జాగ్రత్తలు మనం తీసుకోవాలి అనే అంశాన్ని గురించి వివరించారు. ఈ కార్యక్రమంలో ముఖ్య అతిథి అనిల్ కుమార్ సైకాలజిస్ట్ మాట్లాడుతూ ఈరోజు సమాజంలో యువతలో ఒక దురాశను కల్పించి తద్వారా సైబర్ నేరాలకు పూనుకుంటున్నారు అని అన్నారు కాబట్టి యువత ఏ దురాశలకు లోను కావద్దని ఆశలు ఎక్కువయ్యే కొద్దీ దుష్పరిణామాలకు గురికావలసి ఉంటుందని కాబట్టి అందరూ సైబర్ నేరాలపై అవగాహన కలిగి ఉండాలని అన్నారు.ఈ కార్యక్రమం డాక్టర్ పోలా భాస్కర్ ఐపిఎస్ కమిషనర్ ఆఫ్ కాజీజీ ఎడ్యుకేషన్ ఆంధ్ర ప్రదేశ్ వారి ప్రసంగంతో ఈ కార్యక్రమం ప్రారంభమైంది

ఈ కార్యక్రమంలో జోన్ వన్ అండ్ టు రీజనల్ జాయింట్ డైరెక్టర్ డాక్టర్ చప్పిడి కృష్ణ అంతర్వాలం ద్వారా అధ్యక్షఉపన్యాసం చేశారు ఈ కార్యక్రమంలో కళాశాల డిపార్ట్మెంట్ ఆఫ్ కామర్స్ లెక్చరర్ డాక్టర్ కే ఉత్తమ్ సాగర్ సి. హెచ్ రమాదేవి కే వి వి శిరీష కళాశాల మ్యాథమెటిక్స్ డిపార్ట్మెంట్ సిహెచ్ ఐ్రి నారాయణ, కంప్యూటర్ సైన్స్ విభాగం రాజా కాంత్ కళాశాల వైస్ ప్రిన్సిపల్ బి శ్రీని వాసరావు యు.వెంకటాచార్యులు కళాశాల ఐక్యూఎస్సి కోఆర్డినేటర్ డాక్టర్ ఎం మధు డాక్టర్ వెంకట్ లాల్ మరియు కాజీజీ టీజింగ్ అండ్ నాన్ టీజింగ్ స్టాఫ్ విద్యార్థినీ విద్యార్థులు పాల్గొన్నారు.

ఘనంగా అంతర్జాతీయ పేదరిక నిర్మూలన దినోత్సవం

(తెలుగువార్తన్యూస్) జంగారెడ్డిగూడెం : మంగళవారం జంగారెడ్డిగూడెం శ్రీ చత్రపత శివాజీ త్రీ శతజయంతి ప్రభుత్వ డిగ్రీ కళాశాల లో డిపార్ట్మెంట్ ఆఫ్ ఎకనామిక్స్ శాఖ ఆధ్వర్యంలో అంతర్జాతీయ పేదరిక నిర్మూలన దినోత్సవం ఘనంగా జరుపుకున్నారు ఈ కార్యక్రమం కళాశాల స్వర్ణోత్సవాల సందర్భంగా ఈ కార్యక్రమాన్ని జంగారెడ్డిగూడెం స్వయం సహాయక బృందాలు (డ్రోక్రా) గ్రూప్స్ మరియు తాడేపల్లిగూడెం వెంకట రామన్న గూడెం డాక్టర్ వైఎస్ రాజశేఖర్ రెడ్డి హార్టికల్చర్ యూనివర్సిటీ మరియు మెప్మా ఏలూరు డిస్ట్రిక్ట్ వారి సౌజన్యంతో ఈ కార్యక్రమాన్ని రూపొందించారు ఈ కార్యక్రమానికి కళాశాల ప్రిన్సిపాల్ డాక్టర్ ఎన్ ప్రసాద్ బాబు అధ్యక్షత వహించి విద్యార్థులను ఉద్దేశించి మాట్లాడుతూ పేదరిక నిర్మూలన జరగాలంటే దానికి ప్రభుత్వ కార్యకలాపాలు ప్రభుత్వం చేపట్టిన వినూత్న కార్యక్రమాలు ప్రజలు తెలుసుకోవాలని మారుతున్న పరిస్థితులకు అనుగుణంగా వ్యవస్థలో మార్పు రావాలని ప్రతి వ్యక్తి పేదరిక నిర్మూలన చేయాలనే సంకల్పం దీక్ష బునాలి అన్నారు ఈ కార్యక్రమంలో వైఎస్సార్ హార్టికల్చర్ యూనివర్సిటీ ప్రొఫెసర్ డాక్టర్ సుజాత మాట్లాడుతూ పేదరిక నిర్మూలన జరగాలంటే అది మన చేతిలోనే ఉందని మారుతున్న కాలానికి అనుగుణంగా ఉత్పత్తుల్లో

మార్పు తీసుకొచ్చి ఎక్కువ ధరకు వస్తువుల అమ్మడం వల్ల ఎక్కువ లాభాలు గడించాలని ఇలా చేయటం వల్ల స్వయం సమృద్ధి జరుగుతుంది అని అన్నారు భారతదేశంల ప్రభుత్వం పేదరిక నిర్మూలనకు ప్రభుత్వం ఎన్నో పథకాలు రూపొందించింది మారుతున్న కాలాన్ని అర్థం చేసుకోవడం ద్వారా నూతన ఆర్థిక విధానం వైపు వెళ్లొచ్చు అన్నారు ఈ కార్యక్రమంలో మెప్మా జంగారెడ్డిగూడెం ఏరియా కన్వీనర్ పి నాగమణి మరియు ఏలూరు డిస్ట్రిక్ట్ కోఆర్డినేటర్ రత్నకుమారి విద్యార్థులనుదేశించి స్వయం సహాయక బృందాలను ఉద్దేశించి మాట్లాడారు ఈ కార్యక్రమంలో కళాశాల %అనంఎ% కోఆర్డినేటర్ డాక్టర్ ఎం మధు విద్యార్థులను ఉద్దేశించి ప్రసంగించారు.

స్థానిక ప్రభుత్వ డిగ్రీ నందు అకౌంటింగ్ డే సందర్భంగా కార్యశాల నిర్వహించడం జరిగింది

(తెలుగువార్తన్యూస్) జంగారెడ్డిగూడెం : స్థానిక ఛత్రపతి ప్రభుత్వ డిగ్రీ కళాశాల నందు 10-11-2023 నాడు అంతర్జాతీయ అకౌంటింగ్ డే ని పురస్కరించుకొని కళాశాల కామర్స్ డిపార్ట్మెంట్ ఆధ్వర్యంలో కళాశాల ప్రిన్సిపాల్ డా. ఎన్. ప్రసాద్ బాబు గారి అధ్యక్షతన దేశ అభివృద్ధి లో అకౌంటింగ్ పాత్ర అనే అంశం పై కార్యశాల నిర్వహించడం జరిగింది. ఈకార్యక్రమం లో వి. రవికిరణ్ చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ కామర్స్ కున్న గుర్తింపు గురించి రాబోయే రోజుల్లో అకౌంటింగ్ కి వచ్చే డిమాండ్ గురించి వివరించారు ఈ కార్యక్రమం లో భాగంగా కామర్స్ విద్యార్థులందరికి ఉపయోగ పడాలనే ఉద్దేశంతో టాలీ విత్ జి ఎస్ టి మల్టీ యూజర్ సాఫ్ట్ వేర్ ను ఇవ్వటం జరిగింది. దాకారపు కృష్ణ చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ అకౌంటింగ్ కు , కామర్స్ కు ఉన్న వ్యత్యాసాన్ని గురించి, మార్కెటింగ్ గురించి వివరించటం జరిగింది. ఈ కార్యక్రమం లో భాగంగా బాలురకు రెస్ట్ రూమ్స్ తయారు చేయిస్తానని హామీ ఇవ్వటం జరిగింది. జి.వీరేంద్ర కుమార్ చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ టాలీ గొప్పతనం గురించి టెక్నాలజీ గొప్పతన్నాన్ని గురించి ఇటీవల కాలంలో వాడుతున్న చాట్ జీపీటీ, ఆర్టిఫిషల్ ఇంటిలిజెన్స్ బ్లాక్ చైన్ టెక్నాలజీ గురించి వివరించారు అకౌంటింగ్ డే ని పురస్కరించుకొని బి.కామ్ కంప్యూటర్ ల్యాబ్ కి నాలుగు ఫ్యాన్ ఫ్యాన్ లను ఇవ్వటం జరిగింది. కోటేశ్వరరావు గారు చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ జి ఎస్ టి గురించి ఇన్ కమ్ టాక్స్ ఫైలింగ్ గురించి వాటిని నేర్చుకుంటే బి.కామ్ విద్యార్థులకు కలిగే ప్రయోజనాలను గురించి వివరించారు. బి.కామ్ డిపార్ట్మెంట్ ఇన్చార్జ్ డా. కే. ఉత్తమ్ సాగర్ మాట్లాడుతూ బీకాం విభాగం నుంచి ఇలాంటి కార్యక్రమాలు నిర్వహించడం ఆనందంగా ఉందన్నారు. దీనిని ప్రతి ఒక్క విద్యార్థి ఉపయోగించుకొని దేశ నిర్మాణంలో అకౌంటింగ్ పాత్ర ఎంత ప్రధానమైనదో తెలుసుకోవాలన్నారు. కళాశాల ప్రిన్సిపల్ ఎన్.ప్రసాద్ బాబు మాట్లాడుతూ ఎప్పుడూ కాలేజీలో బి.కామ్ విద్యార్థుల శాతం మిగిలిన అన్ని గ్రూపుల కంటే ఎక్కువ అని విద్యార్థులు ఇలాంటి కార్యక్రమాల్ని నిర్వహించినప్పుడు వాటిని సద్వినియోగం చేసుకుని మంచి ప్రయోజకులుగా మారాలన్నారు. వక్తలుగా విచ్చేసిన ఆడిటర్స్ కి కళాశాల తరుపున ప్రత్యేక ధన్యవాదాలు తెలియజేశారు. ఈ కార్యక్రమంలో బి.కామ్ విభాగం నుంచి శ్రీమతి సిహెచ్ రమాదేవి, కె వి వి శిరీష కళాశాల వైస్ ప్రిన్సిపల్ బి. శ్రీనివాసరావు కార్యక్రమ నిర్వహణ కమిటీ తరపున పి. ఎస్. రావు ఇతర అధ్యాపక అధ్యాపకేతర సిబ్బంది బీ.కాం విద్యార్థులు పాల్గొన్నారు.

తెలుగు సాహిత్య ఔన్నత్యాన్ని చాటుదాం

జంగారెడ్డిగూడెం, న్యూస్‌టుడే: తెలుగు సాహిత్యం ఔన్నత్యాన్ని ప్రపంచానికి చాటుదామని ఆదికవి నన్నయ విశ్వవిద్యాలయం తెలుగు విభాగం ఆచార్యుడు తరపట్ల సత్యనారాయణ అన్నారు. జంగారెడ్డిగూడెం సీఎస్‌టీఎస్ ప్రభుత్వ డిగ్రీ కళాశాలలో శుక్రవారం 'తెలుగు సాహిత్యం.. విభిన్న కోణాలు' అనే అంశంపై అంతర్జాతీయ వెబినార్ నిర్వహించారు. తెలుగు అధ్యాపకుడు డాక్టర్ వెంకట్‌లాల్ ఆధ్వర్యంలో నిర్వహించిన ఈ కార్యక్రమంలో పాల్గొన్న సత్యనారాయణ మాట్లాడుతూ తెలుగు సాహిత్యంలోని ఔనత్యాన్ని మరింత ప్రాచుర్యంలోకి తేవాలన్నారు. ఉన్నత విద్య కమిషనర్ పోలా

ప్రసంగిస్తున్న సత్యనారాయణ

భాస్కర్ వర్చువల్ విధానంలో వెబినార్‌ను ప్రారంభించారు. వివిధ విశ్వవిద్యాలయాల ఆచార్యులు ఉపన్యసించారు. ఉన్నత విద్య రాజమహేంద్రవరం ఆర్జేడీ డాక్టర్ చప్పిడి కృష్ణ ముగింపు ఉపన్యాసం ఇచ్చారు.

ప్రభుత్వ డిగ్రీ కళాశాల నందు అంతర్జాతీయ అకౌంటింగ్ డే కార్యశాల

జంగారెడ్డిగూడెం నవంబర్ 11 (గోదావరి విలేఖరి) ఏలూరు జిల్లా జంగారెడ్డిగూడెం ఛత్రపతి ప్రభుత్వ డిగ్రీ కళాశాల నందు అంతర్జాతీయ అకౌంటింగ్ డే ని పురస్కరించుకొని కళాశాల కామర్స్ డిపార్ట్మెంట్ ఆధ్వర్యంలో కళాశాల ప్రిన్సిపాల్ డా. ఎన్. ప్రసాద్ బాబు అధ్యక్షతన దేశ అభివృద్ధి లో అకౌంటింగ్ పాత్ర అనే అంశం పై కార్యశాల నిర్వహించడం జరిగింది. ఈ కార్యక్రమంలో వి. రవికిరణ్ చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ కామర్స్ కున్న గుర్తింపు గురించి రాబోయే రోజుల్లో అకౌంటింగ్‌కి వచ్చే డిమాండ్ గురించి వివరించారు ఈ కార్యక్రమంలో భాగంగా కామర్స్ విద్యార్థులందరికి ఉపయోగ పడాలనే ఉద్దేశంతో టాలీ విత్ జి ఎస్ టి మల్టీ యూజర్ సాఫ్ట్ వేర్‌ను ఇవ్వటం జరిగింది. దాకారపు కృష్ణ చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ అకౌంటింగ్‌కు, కామర్స్‌కు ఉన్న వ్యత్యాసాన్ని గురించి, మార్కెటింగ్ గురించి వివరించటం జరిగింది. ఈ కార్యక్రమంలో భాగంగా బాలురకు రెస్ట్ రూమ్స్ తయారు చేయిస్తానని హామీ ఇవ్వ టం జరిగింది. జి.వీరేంద్ర కుమార్ చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ టాలీ గొప్పతనం గురించి టెక్నాలజీ గొప్పతనాన్ని గురించి ఇటీవల కాలంలో వాడుతున్న చాట్ జీపీటీ, ఆర్టిఫిషల్ ఇంటిలిజెన్స్ బ్లాక్ చైన్ టెక్నాలజీ గురించి వివరించారు అకౌంటింగ్ డే ని పురస్కరించుకొని బి.కామ్ కంప్యూటర్ ల్యాబ్ కి నాలుగు ఫ్యాన్ ఫ్యాన్ లను ఇవ్వటం జరిగింది. కోటేశ్వరరావు చార్టెడ్ అకౌంటెంట్ మాట్లాడుతూ జి ఎస్ టి గురించి ఇన్ కమ్ టాక్స్ ఫైలింగ్ గురించి వాటిని నేర్చుకుంటే బి.కామ్ విద్యార్థులకు కలిగే ప్రయోజనాలను గురించి వివరించారు. బి.కామ్ డిపార్ట్మెంట్ ఇన్చార్జ్ డా. కే. ఉత్తమ్ సాగర్ మాట్లాడుతూ బీకాం విభాగం నుంచి ఇలాంటి కార్యక్రమాలు నిర్వహించడం ఆనందంగా ఉందన్నారు. దీనిని ప్రతి ఒక్క విద్యార్థి ఉపయోగించుకొని దేశ నిర్మాణంలో అకౌంటింగ్ పాత్ర ఎంత ప్రధానమైనదో తెలుసుకోవాలన్నారు. కళాశాల ప్రిన్సిపల్ ఎన్. ప్రసాద్ బాబు మాట్లాడుతూ ఎప్పుడూ కాలేజీలో బి.కామ్ విద్యార్థుల శాతం మిగిలిన అన్ని గ్రూపుల కంటే ఎక్కువ అని విద్యార్థులు ఇలాంటి కార్యక్రమాల్ని నిర్వహించినప్పుడు వాటిని సద్వినియోగం చేసుకుని మంచి ప్రయోజకులుగా మారాలన్నారు. వక్తలుగా విచ్చేసిన ఆడిటర్స్ కి కళాశాల తరుపున ప్రత్యేక ధన్యవాదాలు తెలియజేశారు. ఈ కార్యక్రమంలో బి.కామ్ విభాగం నుంచి శ్రీమతి సిహెచ్ రమాదేవి, కె వి వి శిరీష కళాశాల వైస్ ప్రిన్సిపల్ బి. శ్రీనివాసరావు కార్యక్రమ నిర్వహణ కమిటీ తరపున పి. ఎస్. రావు ఇతర అధ్యాపక అధ్యాపకేతర సిబ్బంది బీ.కాం విద్యార్థులు పాల్గొన్నారు.

ప్రభుత్వ డిగ్రీ కళాశాల నందు

జీవ శాస్త్రాలలో కొత్త పోకడలపై సదస్సు

జంగారెడ్డిగూడెం నవంబర్ 30 (గోదావరి విలేఖరి) : ఏలూరు జిల్లా జంగారెడ్డిగూడెం చత్రపతి శివాజీ త్రి శతజయంతి ప్రభుత్వ డిగ్రీ కళాశాల నందు గురువారం నాడు వృక్ష శాస్త్రము జంతు శాస్త్రము ఉద్యాన శాస్త్ర విభాగాలు కలిసి సదస్సు నిర్వహించడం జరిగింది. ఈ కార్యక్రమంలో కళాశాల ప్రిన్సిపల్ డా. ఎన్. ప్రసాద్ బాబు మాట్లాడుతూ బయోలాజికల్ సైన్స్ ప్రాముఖ్యతను గురించి వివరించారు. దీనితో పాటు 23 పేపర్లు ప్రచురితమైన జర్నల్ ని రిసోర్స్ పర్సన్స్‌తో కలిసి ఆవిష్కరించడం జరిగింది. ఈ కార్యక్రమంలో రిసోర్స్ పర్సన్ డాక్టర్ డి. శ్రీధర్ అసిస్టెంట్ ప్రొఫెసర్, ఆదికవి నన్నయ్య యూనివర్సిటీ మాట్లాడుతూ బయో డైవర్సిటీ గురించి ఆక్వా కల్చర్ గురించి చేపల పెంపకంలో సుస్థిర అభివృద్ధి గురించి వివరించారు. డా. టి.సుజాత ఆర్ట్స్ కాలేజ్ రాజమండ్రి అసోసియేట్ ప్రొఫెసర్,మైక్రో బయాలజీ విభాగం మాట్లాడుతూ మానవుని ఆరోగ్యంలో సూక్ష్మజీవుల పాత్ర ఏ విధంగా ఉంటుంది అనే అంశం గురించి వివరించారు. డా. జె.రాముడు లక్కిరెడ్డి హనిమిరెడ్డి ప్రభుత్వ డిగ్రీ కళాశాల మైలవరం వృక్ష శాస్త్ర అధ్యాపకులు మాట్లాడుతూ విపత్తులో ఉన్న వృక్షజాతులు గురించి వాటిని రక్షించుకోవాలంటే మనం ఏ విధమైన చర్యలు తీసుకోవాలి అనే అంశం గురించి వివరించారు. డా. జి. సౌజన్య తిరువళ్లూరు యూనివర్సిటీ అసిస్టెంట్ ప్రొఫెసర్ జీవ సాంకేతిక శాస్త్ర విభాగం మాట్లాడుతూ

అనువర్తిత జీవశాస్త్రంలో ప్రస్తుత పరిణామాలు గురించి వివరించారు. డా. యు. వి. ప్రసాద్ నేరశాస్త్ర విభాగంలో పిసిఆర్ మరియు డిఎన్ఏ ఫింగర్ ప్రింటింగ్ గురించి వివరించడం జరిగింది.ఈ కార్యక్రమంలో వృక్ష శాస్త్ర విభాగం నుంచి టి . రూన్సీ రాణి, జంతు శాస్త్ర విభాగం నుంచి ఆర్. విజయ దీపిక, ఉద్యానవన శాస్త్ర విభాగం నుంచి సిహెచ్.వెంకటలక్ష్మి, కళాశాల వైస్ ప్రిన్సిపల్ బి. శ్రీనివాసరావు, కళాశాల ఐక్యూ ఏసి కోఆర్డినేటర్ డా. ఎమ్.మధు, కార్యక్రమ నిర్వహణ కమిటీ పి.ఎస్.రావు, యు.వెంకటాచార్యులు, డా. సిహెచ్. బదరీ నారాయణ, ఇతర అధ్యాపక అధ్యాపకేతర సిబ్బంది కళాశాల సైన్స్ విభాగ విద్యార్థులు పాల్గొన్నారు.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

CRYPTOCURRENCY AND BLOCK CHAIN SECURITY

Shaik. Asha and Koppula Ajay
2nd Bcom [Computers]
CSTS Govt Degree Kalsala, Jangareddigudem

Abstract

Cryptocurrency is a digital or virtual form of currency that uses cryptography for security. It operates independently of a central authority, such as a government or bank, and relies on a technology called blockchain for its operation and security.Blockchain is a distributed ledger technology that records all transactions across a network of computers in a way that is secure, transparent, and tamper-resistant. Here's how blockchain security works

INTRODUTION

Cryptocurrency and blockchain security are essential aspects of the rapidly evolving digital financial landscape. Let's start with some key concept

ADAVANTAGES:

- Cryptocurrency: Cryptocurrency is a digital or virtual form of currency that uses cryptography for security. Bitcoin, Ethereum, and many others are examples. They enable secure and decentralized transactions.
- Blockchain: A blockchain is the underlying technology behind cryptocurrencies. It's a distributed ledger that records all transactions across a network of computers. Once a transaction is added to the blockchain, it's virtually immutable.
- Now, let's delve into security:
- Cryptography: Cryptography ensures the confidentiality and integrity of transactions. It encrypts data, making it unreadable without the proper keys. Public and private keys are used to secure crypto currency wallets and transactions.
- Decentralization: Block chain operates on a decentralized network of nodes, reducing the risk of a single point of failure or control. This makes it resistant to censorship and fraud.
- Consensus Mechanisms: Crypto currencies rely on consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. These mechanisms prevent double-spending and maintain the integrity of the blockchain.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

- Wallet Security: Users must safeguard their cryptocurrency wallets and private keys. Hardware wallets, paper wallets, and secure software wallets are common options. Losing access to your keys can result in loss of funds.
- Smart Contract Audits: Blockchain platforms like Ethereum allow for the creation of smart contracts. Auditing these contracts is crucial to identify vulnerabilities and prevent exploits.
- Phishing and Scams: Beware of phishing websites and scams targeting cryptocurrency users. Always verify the authenticity of websites and offers.
- Regulatory Compliance:
- Be aware of the legal and tax implications of cryptocurrency transactions in your jurisdiction. Compliance is essential to avoid legal issues.
- Cold Storage: For long-term storage, consider cold storage options that keep your cryptocurrency offline, away from potential online threats.
- Multi-Signature Wallets: Some wallets support multi-signature functionality, requiring multiple keys to authorize transactions, enhancing security.
- Security Updates: Stay informed about updates and security patches for the blockchain software and wallet applications you use.
- Security in the cryptocurrency and blockchain space is an ongoing concern. It requires users to stay vigilant, adopt best practices, and adapt to evolving threats to protect their digital assets effectively
- Cryptocurrency and blockchain technology have revolutionized the way we think about money, transactions, and security. Cryptocurrencies like Bitcoin and Ethereum offer a decentralized and secure way to transfer value digitally, while blockchain serves as the underlying technology that makes it all possible.
- In this evolving landscape, understanding the principles of cryptocurrency and blockchain security is crucial. This includes grasping concepts such as cryptography, decentralization, consensus mechanisms, wallet security, and the importance of staying vigilant against scams and fraud.
- As you explore this fascinating realm, you'll discover how these innovations are reshaping finance, business, and beyond, and how you can navigate this digital frontier securely to harness its potential benefits.
- disadvantage
- Certainly, let's explore the advantages and disadvantages of cryptocurrency and blockchain technology:

In the past few years, Blockchain security has taken the world by storm. Its ability to create a secure and tamper-proof network for transactions has made it an incredibly valuable tool. Blockchain technology was first developed in 2008 for the cryptocurrency Bitcoin. However, the potential applications of Blockchain extend far beyond cryptocurrencies. Today, blockchains are being used for everything from supply chain management to identity verification.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

Blockchain technology is revolutionizing the world as we know it. But with great power comes great responsibility- and this is especially true when it comes to Blockchain security. In this post you will know about Blockchain security, from the basics to more advanced concepts. We will also provide tips on how to stay safe while using Blockchain technology. Also, you can consider taking an online Blockchain technology course to pump up your Blockchain security knowledge and skills.

Basic Blockchain Security

When it comes to security, Blockchain technology is often lauded for its tamper-proof and distributed ledger features. However, it's important to remember that no system is completely secure. In order to ensure the safety of your data, it's crucial to understand the basics of Blockchain security.

One of the key advantages of Blockchain is that it allows decentralized control. There is no central authority that can be hacked or taken offline. Instead, the network is made up of nodes, each of which stores a copy of the Blockchain. In order for a hacker to tamper with the Blockchain, they would need to hack every single node in the network - an extremely difficult feat.

Another important security feature of Blockchain is its cryptographic hashing. This allows each block in the chain to be uniquely identified and linked to the previous block. As a result, it's nearly impossible to insert bogus data into the Blockchain without raising suspicion. Any attempt to do so would require not only changing the data in the block, but also all subsequent blocks - an impractical task for even the most skilled hacker.

While Blockchain technology is certainly impressive from a security standpoint, it is important to remember that no system is impenetrable and there are some Blockchain security vulnerabilities as well. Thus, to protect your data, it is important to take basic security precautions as discussed further.

How is Blockchain Used for Security?

A Blockchain is a shared database that is managed by a network of computers rather than a single party. This decentralized structure allows for increased transparency and security, as each party on the chain can verify every transaction against the entire history of the Blockchain.

The key to understanding how Blockchain works is to think of it as a digital ledger. In traditional ledgers, transactions are recorded and managed by a central authority, such as a bank or government. In contrast, blockchains are decentralized, meaning that there is no central authority managing the ledger. Instead, the ledger is shared among all parties on the chain.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

Each time a new transaction occurs, it is recorded on the Blockchain. These transactions are then verified by all parties on the chain using complex mathematical algorithms. Once a transaction is verified, it cannot be changed or deleted. This creates a permanent and secure record of all transactions that have ever occurred on the Blockchain.

The decentralized nature of blockchains makes them particularly well-suited for applications that require increased transparency and security, such as financial transactions or supply chain management.

Thus, blockchains are still one of the most promising new technologies to emerge in recent years. This is why there is a high jump in applicants looking for Blockchain security jobs and projects. With their ability to provide increased security and transparency, they have the potential to revolutionize many industries and change the way we interact with technology in our everyday lives.

Blockchain Types and Security Threats
There are 4 types of Blockchain namely:

1. Public Blockchain
Public blockchains, such as Bitcoin, are open to anyone. Anyone can view the transaction history and create new transactions. Public blockchains are decentralized and secure, but they can be slow and expensive. Because public blockchains are open and accessible to anyone, they are often more secure than private or permissioned blockchains. This is because it is much more difficult for bad actors to achieve a 51% attack on a public Blockchain than it is on a private blockchain.

2. Private Blockchain
It is a distributed database that allows only approved members to have access to the data and perform transactions. Private Blockchains are usually permissioned, meaning that there is a central authority that controls who has access to the network. This contrasts with public Blockchains, such as Bitcoin, which anyone can join.

Private Blockchains are often used by businesses or other organizations where security and privacy are paramount. Since only approved members have access to the data, it is more difficult for hackers to breach the network. In addition, transactions on a private Blockchain can be carried out faster than on a public Blockchain, since there is no need to wait for consensus from all members of the network.

Private Blockchains are sometimes considered less secure, as they rely on a single entity to maintain security. This means that if the entity is compromised, the entire network can be disrupted.


Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

3. Hybrid Blockchain

It is a type of Blockchain that combines the features of both public and private blockchains. A hybrid Blockchain can be customized, where users can decide who can take part within the Blockchain or which transactions are made public. A hybrid Blockchain has the benefits of both public and private blockchains.

The security drawback is that maintaining a real-time record of all users' preferences becomes very difficult for the central authority. This is why many reputable websites offer Blockchain security certification for free to help users enlighten about various security issues and give them basic related skills.

4. Consortium Blockchain

Consortium blockchains include known participants preapproved to participate in the consensus by a central authority within a Blockchain network. A consortium Blockchain allows only pre-selected nodes to participate in the consensus process. Consortium blockchains are often used in business settings where there is a need for increased security and speed, but where decentralization is not a priority.

For example, a group of banks may use a consortium Blockchain to streamline their back-end operations. By pre-selecting who can participate in the network, they can be sure that only trusted actors are able to access sensitive data. This can help to improve efficiency while still maintaining security. Coming to security, they are less secure than public blockchains and more secure than private ones.

How Fraudsters Attack Blockchain Technology?

Blockchain and data security are always a topic of concern for users. Blockchain technology also deals with security vulnerabilities, and it is vulnerable to four types of attacks: phishing, routing, Sybil, and 51% attacks.

1. Phishing

A phishing attack is a type of cyberattack where an attacker impersonates a trusted entity in order to trick victims into revealing sensitive information, such as login credentials or financial information. Phishing attacks are often used to steal cryptocurrency from victims by sending them fake links that redirect them to malicious websites designed to look like legitimate exchanges or wallets.

These websites will then prompt the user to enter their login credentials, which the attacker can then use to gain access to their account and steal their cryptocurrency. This is why Blockchain security salary is high in many different countries because the engineers and developers have to work really hard to avoid Phishing.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

2. Routing Attack

Another type of attack that can occur in Blockchain technology is a routing attack. This is when hackers intercept data as it's transferring to internet service providers. By doing this, they can disrupt the network and prevent transactions from being completed.

Routing attacks can be difficult to detect and prevent, but there are some measures that can be taken. For example, data can be encrypted before it's sent, and node operators can monitor their networks for suspicious activity. If possible, try to hire the best crypto auditors to be on the safe side.

3. Sybil Attack

A Sybil attack is a type of Blockchain attack where hackers create and use many false identities to crowd the network and crash the system. This can be done by creating multiple accounts, computers, or ids. Sybil attacks can reduce confidence in the Blockchain, as well as lead to financial losses. In order to prevent a Sybil attack, it is important to have strong security measures in place. This may include using digital signatures or ids, as well as maintaining a list of known ids.

4. 51% Attack

A 51% attack is a type of Blockchain attack where a group of miners or a single miner controls more than 50% of the network's mining power. This control allows them to manipulate the ledger, which could lead to double-spending or other types of fraud. While 51% attacks are very rare, they are a serious security concern for Blockchain security. In order to protect against them, it is important for Blockchain networks to have a large and decentralized mining community.

These are just a few of the many ways that can impact Blockchain cybersecurity and cause harm.

Blockchain Security for the Enterprise

As enterprises increasingly explore the use of Blockchain technology, security concerns must be addressed to ensure that data is protected. There are several security controls that should be considered when implementing a Blockchain solution for an enterprise.

Identity and access management (IAM) is important to ensure that only authorized users have access to the system.
Key management is also critical, as private keys are needed to sign transactions and unlock data.
Data privacy must be considered to protect sensitive information from being accessed by unauthorized individuals.
Secure communication must be established between nodes in order to prevent eavesdropping or man-in-the-middle attacks.


Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

Smart contract auditing is also essential to prevent vulnerabilities that could be exploited by attackers. An authentic smart contract auditing service helps enterprises launch and maintain their Blockchain applications. Finally, transaction endorsement can help increase a Blockchain's security by requiring multiple parties to sign off on each transaction.

Blockchain Penetration Testing

Blockchain technology is gaining traction in various industries, from banking and finance to healthcare and supply chain management. Interested learners can even opt for Blockchain Solution Architect training to understand the basics of blockchain architecture and design an application.

As the use of Blockchain grows, so does the need for effective penetration testing services. Blockchain penetration testing helps assess Blockchain applications' security and identify vulnerabilities that attackers could exploit.

Functional testing, performance testing, API testing, security testing, and integrating testing are all essential components of effective Blockchain penetration testing. During a penetration test, ethical hackers attempt to identify and exploit vulnerabilities in the system. This helps to find and fix potential exploits before criminals can use them.

What are Blockchain Security Testing Tools?

There are several Blockchain Security testing tools available on the market today. Here is a brief overview of some of the more popular options:

Truffle –Truffle is a popular Ethereum development framework with a suite of tools for testing and debugging smart contracts.

Ganache – Ganache is a personal Ethereum Blockchain that can be used for testing and development. It includes a user interface for interacting with smart contracts.

TestRPC – TestRPC is a Node.js-based simulator for Ethereum smart contracts. It allows you to test contracts on a simulated Ethereum network.

MythX – A smart contract security analysis

SWC-registry – Test cases and Smart contract weakness classification

Oyente – A static analysis tool

Manticore – A symbolic execution tool

SmartCheck – Static smart contract security analyzer.

Securify 2.0 –A security scanner

Surya – A utility tool

Solgraph – Generates a DOT graph and highlights potential security vulnerabilities.


Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

Octopus – A security analysis framework
Solidity security blog – involves a detailed list of bugs, vulnerabilities, crypto-related hacks, and preventative measures.
These are just some of the most popular Blockchain Security testing tools. There are many others available, each with its unique features and capabilities. Choosing the right tool for your needs will depend on the specific requirements of your project.

Blockchain Security Tips and Best Practices
There are certain Blockchain security tips and practices that apply to everyone:

1. Implementing Two-factor Authentication
One of the most important aspects of security in the Blockchain space is two-factor authentication (2FA). Implementing 2FA adds an extra layer of security to your online accounts by requiring a second factor, in addition to your password, to log in. This second factor can be a one-time code generated by an authenticator app, a hardware token, or a biometric factor like your fingerprint or iris scan.

While 2FA is not foolproof, it significantly increases the security of your online accounts and should be used whenever possible. In the Blockchain space, 2FA is especially important due to the high value of digital assets and the often-irreparable damage that a hack or theft can cause. Also, try to find reputable Blockchain security audit companies that can identify any loopholes in the system and eliminates any vulnerabilities.

2. Allow Listing Trusted Senders and Recipients
One of the best things you can do to secure your Blockchain platform is to allow only trusted senders and receivers. This may seem like a no-brainer, but it's incredibly important. By allowing only trusted entities to interact with the Blockchain, you can dramatically reduce the chances of malicious activity. Of course, this doesn't mean you should never allow new entities onto the Blockchain.

Rather, it simply means that you should be very careful about who you allow access to. Take the time to verify the identity of each sender and receiver identity, and ensure they are credible before allowing them onto the network.

3. Keep your Software Up to Date
That means installing security updates and patching any vulnerabilities as soon as they are discovered. By staying on top of the latest security threats, you can help ensure that your Blockchain network remains safe and secure. Additionally, it's important to choose a reputable and reliable provider for your Blockchain security needs. Look for a provider with a proven track record of keeping their networks safe and secure.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

4. Using VPNs - Virtual Private Network

While the use of VPNs is not new, it is gaining popularity due to increased awareness of online security threats. A VPN is a secure, encrypted connection between two devices. This connection can tunnel data traffic through an untrusted network like the internet.

By encrypting the data traffic, a VPN can help to protect your information from malicious actors. In addition, a VPN can also help to improve your privacy by hiding your real IP address and location. While there are many different VPN providers to choose from, selecting a reputable provider with strong encryption and security features is important.

5. Use Anti-Phishing Tools

Phishing attacks are becoming increasingly common and can be difficult to detect and prevent. An anti-phishing tool can help to identify and block phishing attempts, keeping your Blockchain safe. Additionally, it's important to be aware of the signs of a phishing attack. Be suspicious of any email or message that asks you to click on a link or provide personal information. If you are skeptical about the legitimacy of an email, contact the sender to verify its authenticity.

CONCULUTION:

However, it's important to note that while blockchain technology itself is highly secure, vulnerabilities can still arise due to human error, software bugs, or external factors. Security measures such as wallet protection, strong passwords, and secure storage of private keys are crucial for individuals using cryptocurrencies to protect their assets. Additionally, the security of a blockchain network depends on the specific consensus mechanism and the level of adoption and decentralization it has achieved.

Cryptocurrency Security:

1. *Wallet Security*: Secure your cryptocurrency by using reputable wallets and implementing strong passwords or passphrase. Hardware wallets are considered one of the most secure options.
2. *Two-Factor Authentication (2FA)*: Enable 2FA whenever possible to add an extra layer of security to your accounts.
3. *Phishing Awareness*: Be cautious of phishing attempts. Always verify the legitimacy of websites and emails related to cryptocurrency.
4. *Updates and Patches*: Keep your wallet software, apps, and operating systems up to date to protect against vulnerabilities.
5. *Private Key Protection*: Never share your private keys, and store them in a secure, offline location.
1. Blockchain Security:

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

1. *Consensus Mechanisms*: Understand the consensus mechanism of the blockchain you're using. Bitcoin, for example, uses proof-of-work (PoW) while Ethereum is transitioning to proof-of-stake (PoS).
2. *Smart Contract Auditing*: If you're developing or using smart contracts, ensure they undergo thorough auditing to identify vulnerabilities.
3. *Network Security*: Protect the network from attacks like 51% attacks by decentralizing mining power and using robust security measures.
4. *Immutable Records*: Be aware that data once written to a blockchain is typically immutable, so ensure data integrity before it's added.
5. *Privacy*: Consider the privacy features of the blockchain. Some, like Monero, offer enhanced privacy compared to Bitcoin.

References

1. Morris, David Z. (15 May 2016). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune. Archived from the original on 21 May 2016. Retrieved 23 May 2016.
2. Popper, Nathan (21 May 2016). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". The New York Times. Archived from the original on 22 May 2016. Retrieved 23 May 2016.
3. "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.
4. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, New Jersey: Princeton University Press. ISBN 978-0-691-17169-2.
5. Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Cambridge, Massachusetts: Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.
6. Oberhaus, Daniel (27 August 2018). "The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995". Vice. Retrieved 9 October 2021.
7. Lunn, Bernard (10 February 2018). "Blockchain may finally disrupt payments from Micropayments to credit cards to SWIFT". dailyfintech.com. Archived from the original on 27 September 2018. Retrieved 18 November 2018.
8. Hampton, Nikolai (5 September 2016). "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin". Computerworld. Archived from the original on 6 September 2016. Retrieved 5 September 2016.


Cover Page

DOI: http://ijmer.in.doi./2023/12.10.25
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October:2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received:2nd October2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication:www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

9. Bakos, Yannis; Halaburda, Hanna; Mueller-Bloch, Christoph (February 2021). "When Permissioned Blockchains Deliver More Decentralization Than Permissionless". Communications of the ACM. 64 (2): 20–22. doi:10.1145/3442371. S2CID 231704491.
10. Sherman, Alan T.; Javani, Farid; Zhang, Haibin; Golaszewski, Enis (January 2019). "On the Origins and Variations of Blockchain Technologies". IEEE Security Privacy. **17** (1): 72–77. arXiv:1810.06130. doi:10.1109/MSEC.2019.2893730. ISSN 1558-4046. S2CID 53114747.


Cover Page

DOI: http://ijmer.in.doi./2023/12.10.40
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd October 2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

ETHICAL HACKING AND RED TEAMING

[1]Sank Sampath and [2]Ganta Anjali
[1]2nd B.Com General and 2ND B.Com Computer[2]
[1,2]C.S.T.S Govt Kalasala, Jangareddigudem

Abstract:

Ethical hacking and red teaming are cybersecurity practices aimed at identifying vulnerabilities and weaknesses in an organization's digital infrastructure, applications, and security measures. Ethical hacking involves authorized professionals, known as ethical hackers or penetration testers, who use their skills to simulate cyberattacks on an organization's systems. The goal is to uncover security flaws before malicious hackers can exploit them, ultimately enhancing overall security. On the other hand, red teaming takes a more comprehensive approach. It involves creating a team of skilled individuals who simulate real-world cyberattacks by mimicking the tactics, techniques, and procedures of actual threat actors. Red teams aim to provide a holistic assessment of an organization's security posture, going beyond technical vulnerabilities to assess human and process-related weaknesses as well. Overview of the core principles and objectives of ethical hacking and red teaming, which are essential components of a robust cybersecurity strategy.

INTRODUCTION:

In the realm of cybersecurity, the battle between defenders and attackers is relentless and ever-evolving. To safeguard digital assets and sensitive information, organizations must adopt proactive approaches to identify and mitigate vulnerabilities. Two powerful techniques in this endeavor are ethical hacking and red teaming.

1. Ethical Hacking:

Ethical hacking, often referred to as penetration testing or white-hat hacking, involves skilled individuals who are authorized to simulate cyberattacks on an organization's systems, networks, and applications. These cybersecurity experts employ their knowledge of hacking techniques to uncover vulnerabilities before malicious hackers can exploit them. Ethical hackers act as allies, helping organizations fortify their defenses, patch vulnerabilities, and enhance overall security.

2. Red Teaming:

Red teaming takes a broader and more comprehensive approach to assess an organization's security posture. It entails assembling a team of experts who mimic the tactics, techniques, and procedures of real-world threat actors. The red team's objective is to challenge an organization's defenses comprehensively. They not only target technical weaknesses but also evaluate human factors, processes, and response capabilities. This holistic assessment provides valuable insights into an organization's ability to withstand sophisticated cyberattacks.

ADVANTAGES OF ETHICAL HACKING AND RED TEAMING:

1. Security Improvement:* These practices help identify vulnerabilities and weaknesses in a system or network, allowing organizations to patch them before malicious hackers can exploit them.

2. Real-World Testing:* Ethical hackers and red teams simulate real-world attacks, providing a more accurate assessment of an organization's security posture.

3. Risk Mitigation:* By proactively identifying and addressing vulnerabilities, organizations can reduce the risk of data breaches and other security incidents.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.40
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd October 2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

4. Compliance: Many industries and regulations require regular security testing and assessment. Ethical hacking and red teaming help organizations meet these compliance requirements.

5. Enhanced Security Awareness: These practices raise awareness among employees and stakeholders about security best practices and potential threats.

6. Cost Savings: Detecting and fixing vulnerabilities early is usually less expensive than dealing with the consequences of a security breach.

7. Continuous Improvement:* Ethical hacking and red teaming are ongoing processes, ensuring that security measures evolve to counter new threats.

8. Incident Response Preparedness:* Identifying weaknesses in incident response plans allows organizations to better prepare for and respond to security incidents.

9. Client Trust:* Demonstrating a commitment to security through ethical hacking and red teaming can build trust with clients and customers.

10. Competitive Advantage: Having robust security measures can be a competitive advantage, especially in industries where data protection is critical.

Overall, ethical hacking and red teaming are valuable practices for enhancing cybersecurity and protecting sensitive information.

DISADVANTAGES OF ETHICAL HACKING:

While ethical hacking and red teaming are valuable practices for identifying and addressing security vulnerabilities, they do come with some disadvantages:

1. Legal and Ethical Concerns: Ethical hackers and red teams must operate within legal and ethical boundaries. If they cross these lines or make mistakes, they could potentially face legal consequences or damage an organization's reputation.

2. Costly: Hiring or training skilled ethical hackers and conducting red team exercises can be expensive. Smaller organizations with limited budgets may struggle to afford these services.

3. Time-Consuming: Comprehensive security assessments and penetration testing take time to plan and execute properly. This can disrupt regular business operations and result in downtime.

4. False Positives/Negatives: The findings of ethical hacking and red teaming may sometimes produce false positives (indicating vulnerabilities that don't exist) or false negatives (failing to identify real vulnerabilities). This can lead to wasted time and resources.

5. Resistance from Employees: Some employees may view ethical hacking and red teaming as invasive or disruptive, leading to resistance or a lack of cooperation during the testing process.

6. Limited Scope: These practices may not cover all aspects of an organization's security posture. They might focus on specific areas or scenarios, potentially leaving other vulnerabilities unaddressed.


Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd October 2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.10.40
www.ijmer.in

7. Skill and Resource Dependence: Finding skilled ethical hackers and maintaining an effective red team can be challenging. Organizations may need to constantly update their expertise and tools to keep up with evolving threats.

8. Confidentiality Concerns: Sharing sensitive information with ethical hackers or red teams can be risky. Organizations must carefully manage the confidentiality of their data during these assessments.

9. Risk of Exposure: During red teaming exercises, there's a risk that attackers could exploit vulnerabilities before they are discovered by the team, potentially causing damage or data breaches.

Despite these disadvantages, the benefits of ethical hacking and red teaming, such as identifying and mitigating security weaknesses, often outweigh the drawbacks when conducted thoughtfully and with proper planning.

CONCLUSION:

Ethical hacking and red teaming represent indispensable pillars of contemporary cybersecurity strategies. These proactive approaches serve as vital safeguards against the ever-evolving landscape of cyber threats. By systematically probing and testing an organization's defenses, ethical hackers and red teams uncover vulnerabilities that could otherwise be exploited by malicious actors. This process isn't a one-time endeavor but an ongoing, adaptive practice, ensuring that security remains resilient over time. Furthermore, it facilitates regulatory compliance, bolsters risk mitigation efforts, and fosters collaboration between security teams and management. Ethical considerations and confidentiality are paramount, and continuous education and customization are essential to success. Ultimately, ethical hacking and red teaming offer a cost-effective means of enhancing security and protecting valuable assets in an interconnected digital world.

References

1. Walker, Matt; CEH Certified Ethical Hacker All-In-One Exam Guide, The McGraw-Hill Companies, 2011. ISBN 978-0-07-177229-7
2. Oriyano, Sean-Philip; CEH: Certified Ethical Hacker Version 8 Study Guide, Sybex Publishing, 2014. ISBN 978-1-118-64767-7
3. Gregg, Michael; Certified Ethical Hacker Exam Prep, Que Publishing, 2006. ISBN 978-0-7897-3531-7
4. DeFino, Steven; Greenblatt, Larry; Official Certified Ethical Hacker Review Guide: for Version 7.1 (EC-Council Certified Ethical Hacker (Ceh)), Delmar Cengage Learning, March 2, 2012. ISBN 978-1-1332-8291-4
5. IP Specialist; CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs: Exam: 312-50, May 2018, ISBN 978-1983005473
6. Ric Messier; CEH v10 Certified Ethical Hacker Study Guide, Sybex publishing, May 7, 2019. ISBN 978-1119533191

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.41
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd October 2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CYBER SECURITY

Panuganti Supraja
C.S.T.S Govt Kalasala, Jangareddigudem

Abstract:

The ever-evolving landscape of cyber threats presents a formidable challenge to organizations worldwide. To combat these threats effectively, there has been a paradigm shift towards the integration of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity. This abstract explores the critical role of AI and ML in fortifying digital defenses and proactively identifying, mitigating, and responding to cyberattacks.

AI and ML technologies have revolutionized the cybersecurity domain by enabling automated threat detection, prediction, and adaptive response mechanisms. They harness vast datasets to train models that can recognize anomalies and patterns indicative of cyber threats. This newfound capability is particularly crucial in today's interconnected and data-driven world, where traditional rule-based approaches fall short.

Introduction:

In an age where digital footprints span across all aspects of life, the ever-expanding digital landscape is a playground not only for legitimate users but also for malicious actors seeking to exploit vulnerabilities and steal sensitive information. This incessant battle between cyber security defenders and cybercriminals has reached a critical juncture. The rapid proliferation of data and the sophistication of cyber threats have made traditional security approaches inadequate. To adapt to this evolving threat landscape, the field of cybersecurity has turned to Artificial Intelligence (AI) and Machine Learning (ML) as its vanguard.

Artificial Intelligence, encompassing ML techniques, has emerged as a powerful ally in the realm of cybersecurity. The marriage of AI and cybersecurity represents a seismic shift in how we protect our digital assets. It empowers us to proactively identify, respond to, and mitigate cyber threats in ways that were inconceivable with rule-based systems alone.considerations that accompany their integration into the cybersecurity landscape.AI and ML empower cybersecurity professionals to transcend human limitations in analyzing vast datasets, identifying complex patterns, and making real-time decisions. They enable us to build intelligent systems that not only detect known threats but also predict and counter emerging ones. Whether it's recognizing unusual patterns in network traffic, swiftly identifying zero-day vulnerabilities, or fortifying authentication systems, AI and ML have become indispensable tools in the arsenal of the modern cybersecurity expert.

However, with great power comes great responsibility. As AI/ML-driven cybersecurity becomes ubiquitous, it raises questions about privacy, transparency, and the potential for malicious use. Adversarial attacks that manipulate AI models are a real concern, and the ethical implications of AI decisions in security contexts demand careful consideration.

ADVANTAGES:

Artificial Intelligence (AI) and Machine Learning (ML) bring several advantages to cyber security, enhancing the ability to protect digital assets and respond to evolving threats. Here are some key advantages:

1. Real-Time Threat Detection: AI and ML systems can continuously monitor network traffic, system behavior, and user activities in real-time. They can quickly identify and flag suspicious activities or anomalies, enabling rapid threat detection.

Cover Page

DOI: http://ijmer.in.doi./2023/12.10.41
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd October 2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

2. Advanced Anomaly Detection: These technologies excel at recognizing patterns and anomalies that may be indicative of cyber threats. They can identify previously unseen attack patterns, helping to detect zero-day vulnerabilities and sophisticated attacks.

3. Reduced False Positives: By learning from historical data, AI/ML systems can reduce false positives. This means security teams can focus their efforts on genuine threats, rather than wasting time investigating benign incidents.

4. Automation: AI can automate routine security tasks, such as log analysis and threat prioritization. This allows security professionals to focus on more strategic tasks and incident response.

5. Predictive Analysis: ML algorithms can predict potential security threats based on historical data and current trends. This proactive approach helps organizations prepare for and mitigate emerging threats before they become major issues.

6. Enhanced User Authentication: Behavioral biometrics and ML-based authentication methods can strengthen user authentication. These systems analyze user behavior patterns, making it difficult for attackers to impersonate legitimate users.

7. Efficient Incident Response: AI/ML can assist in incident response by providing real-time insights into the scope and impact of a security incident. This enables faster and more effective containment and remediation efforts.

DISADVANTAGES

While Artificial Intelligence (AI) and Machine Learning (ML) offer significant advantages in cyber security, they also come with certain disadvantages and challenges:

1. False Positives and Negatives: AI/ML systems are not infallible and can produce false positives (flagging benign activities as threats) or false negatives (failing to detect actual threats). These inaccuracies **can** lead to security teams becoming complacent or wasting time investigating non-issues.

2. Complex Implementation :Integrating AI/ML into existing cybersecurity infrastructure can be complex and resource-intensive. It may require specialized skills and substantial financial investments.

3. Data Quality and Quantity: AI/ML models heavily rely on data quality and quantity. If the training data is incomplete, biased, or outdated, it can lead to inaccurate results. Gathering and maintaining high-quality data can be challenging.

4. Adversarial Attacks: Attackers can exploit vulnerabilities in AI/ML models through adversarial attacks. They manipulate input data to deceive AI systems, leading to incorrect security decisions.

5. Interpretability: Many AI/ML algorithms are complex "black boxes" that make it challenging to understand how they arrive at their decisions. This lack of transparency can be a significant issue when explaining security decisions to stakeholders or regulators.

6. Over-Reliance on Automation: Over-reliance on AI-driven automation can lead to complacency among security professionals. It's important to maintain human oversight and expertise.

7. Privacy Concerns: AI/ML systems may process and store large amounts of sensitive data, raising privacy concerns. Ensuring compliance with data protection regulations like GDPR and HIPAA is crucial.


Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:10(1), October: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd October 2023
Publication Date:30th October 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.10.41
www.ijmer.in

8. Resource Intensiveness: Some AI/ML algorithms require significant computational resources, which can strain an organization's infrastructure and lead to higher operational costs.

9. Skill Gap: Finding and retaining personnel with expertise in AI/ML and cybersecurity can be challenging. Skilled professionals in this intersection are in high demand.

CONCLUSION:

In conclusion, while AI and ML have the potential to revolutionize cybersecurity, they are not without challenges. Organizations must carefully assess the benefits and drawbacks and implement these technologies in a way that complements human expertise and addresses privacy and ethical concerns. Cyber security remains a dynamic field, and a holistic approach that combines technology, expertise, and best practices is essential for effective defense. In conclusion, the integration of Artificial Intelligence (AI) and Machine Learning (ML) into the realm of cyber security marks a significant step forward in our ability to protect digital assets and defend against evolving cyber threats. These technologies offer a compelling mix of advantages and challenges that shape the future of digital security**.**

References:

1. Shackleford, D. (2018). How Machine Learning is Revolutionizing the Field of Cybersecurity. O'Reilly Media.
2. Almohri, H., & Amer, I. A. (2020). Artificial Intelligence and Machine Learning in Cybersecurity: A Comprehensive Survey. IEEE Access, 8, 115473-115506.
3. Kim, H., Kim, H., Kim, J., & Kim, J. (2019). A survey of deep learning-based network anomaly detection. Cluster Computing, 22(6), 13585-13599.
4. Dua, S., & Du, X. (2016). Data mining and machine learning in cybersecurity. Auerbach Publications.
5. Mahmood, A. N., & Hu, J. (2018). Cybersecurity Threat Detection and Mitigation Using Machine Learning in Internet of Things (IoT). Procedia Computer Science, 141, 439-446.
6. Huang, W., Wang, W., & Guo, S. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Network and Computer Applications, 149, 102498.
7. Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep Learning (Vol. 1). MIT press Cambridge.