July - September 2025

CDTI, HYDERABAD

Bulletin

HORIZON

Our Motto "ज्ञानं सम्यग् वेक्षणम्" which means
"WISDOM LIES IN PROPER PERSPECTIVE"

CENTRAL DETECTIVE TRAINING INSTITUE, HYDERABAD,
BPR&D, MHA

A Quarterly Bulletin of Central Detective Training Institute, Hyderabad

MESSAGE OF THE DIRECTOR

Shri Salmantaj Patil, IPS
Director

It gives me immense pleasure that the Central Detective Training Institute, Hyderabad is going to launch its quarterly yearnews magazine **"HORIZON"** for the period July to September, 2025.

CDTI, Hyderabad designated to be the Centre of Excellence for "**Police Technology, IT and Cybercrime"**. With the establishment of **"National Cyber Research, Innovation and Capacity Building Centre (NCRI&CB)"**under the Indian Cyber Crime Coordination Centre (I4C), MHA in CDTI-Hyderabad the Institute is striving for capacity building in the Law Enforcement Agencies. In order to find solutions to pressing issues of LEAs, CDTI-Hyderabad successfully conducted a National Police Hackathon in collaboration with Telangana Cyber Security Bureau & Indian School of Business, Hyderabad. The proposals received were sent to the Modernization Division of BPR&D for further action.

CDTI is also interacting with its client states for identifying the training and coordinating on issues faced by the States. Feedback related to New Criminal Laws courses from the ground level is obtained by visiting the police stations in different states which is submitted to the Ministry of Home Affairs, Govt of India.

CDTI is striving hard to be a Centre of Excellence in the topic of 'Police Technology, IT & Cyber Crime'.

COURSES CONDUCTED FROM JULY TO SEPTEMBER, 2025

From 01st Jul to 30thSept, 2025a total of 32 Courses (including Workshops, Webinars, Conferences) were conducted in which 1143 Officers were trained.

S. No	Name of the Course	Date		No. of Participants
		From	To	
1	AI, Crypto Currency & Block Chain Technology & Misuse of Crypto -Currency	30.06.2025	04.07.2025	29
2	ITEC Course on Digital Evidence investigation (for Sri Lankan Police)	30.06.2025	11.07.2025	24
3	Dark web/ Deep web, Social Media Investigation & Measure of Social Media	07.07.2025	11.07.2025	33
4	Batch 4 part 1 ToT NCL (in collaboration with PMA Team)	07.07.2025	09.07.2025	31
5	Investigation of Economic Crime Cases (DSI), misuse of crypto currency & MLAT	07.07.2025	18.07.2025	21
6	ToT NCL (Batch 1 Part 2) in collaboration with PMA team	14.07.2025	18.07.2025	24
7	Windows & Linux OS - For Cyber Crime Investigation & Analysis	14.07.2025	16.07.2025	21
8	Drone Forensics & Anti Drone Technology and use cases of 5G in Policing	21.07.2025	18.07.2025	36
9	OSINT Gathering techniques and data collection in social media	21.07.2025	25.07.2025	28
10	Network Forensics & Analysis	28.07.2025	01.08.2025	20
11	Basic course on Cyber Crime Investigation and Digital Forensics	28.07.2025	01.08.2025	36
12	Intermediate course on Cyber Crime Investigation and Digital Forensics	04.08.2025	08.08.2025	36
13	Handling CCTV footages and DVR Forensics and Use of CCTV Network/ Footage	04.08.2025	08.08.2025	45
14	Batch 3 Part 1 NCL ToT (in collaboration with PMA Team)	04.08.2025	08.08.2025	25
15	Batch 2 Part 2 NCL ToT (in collaboration with PMA Team)	04.08.2025	06.08.2025	21
16	Workshop on OSINT	11.08.2025	11.08.2025	108

17	Webinar on New Criminal Laws - 2023`	12.08.2025	12.08.2025	90
18	Webinar on Investigation of Block Chain & Crypto Currency	13.08.2025	13.08.2025	66
19	Digital forensics & incidence response – Electronic and digital records under NCL	18.08.2025	22.08.2025	23
20	Web 3.0 technologies such as blockchain, decentralized applications and smart contracts	18.08.2025	22.08.2025	24
21	ToT NCL Batch 4 Part 2 (in collaboration with PMA team)	18.08.2025	20.08.2025	25
22	Conference on Kali Linux - cyber crime investigation	25.08.2025	25.08.2025	44
23	Workshop on Deep and Darkweb & Block Chain Forensics & Misuse of Crypto Currency	02.09.2025	02.09.2025	72
24	Webinar on ethical and legal implications of AI in Cyber Crime Investigation	04.09.2025	04.09.2025	56
25	Practical Digital Forensics: Search & Seizure of evidence, memory forensics, and use of CCTV footage/ networks, chain of custody	08.09.2025	12.09.2025	22
26	Investigation of cloud based cybercrimes and ransomware attacks	08.09.2025	12.09.2025	20
27	ITEC Course on Cyber Security & Incident Response (for Sri Lankan Police)	08.09.2025	19.09.2025	30
28	Malware virus, Trojenworms analysis	15.09.2025	19.09.2025	20
29	Fraud detection and investigation	15.09.2025	19.09.2025	20
30	Humanitarian and empathetic approach towards drug users	22.09.2025	23.09.2025	20
31	Part 3 TOT NCL for Batch 1 & 2	22.09.2025	26.09.2025	30
32	Conference on OSINT Secrets: Mining the Web for darkweb investigations	29.09.2025	29.09.2025	43
Total				**1143**


CDTI
CENTRAL DETECTIVE TRAINING

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" ToT ON New Criminal Laws-2023in Collaboration with Ernst&Young LLP(PMA)Project Management Authority"

07-07-2025 to 09-07-2025

Sitting (L to R) S/Sri-Mrs.G.Sriatha,Asst.Director(AP),K.Jayanagaraj,Asst Director(AP),S.V.Balasubramanyam,Asst. Director(AP),Dr.K.Sarma Murty,Advocate, Saimantaj Patil, - IPS,Director,CDTI,Harshwardhan Singh,Consultant,EY,N.Sai Praveen,DSP(AP),Ms.Priya Jha, Scientist-B,CFSL,HYD,G.Rajkumar,Dy.SP,Course co Ordinator,CDTI

Standing 1 (L to R) S/Sri - Kayala Venkata giri,AS(AP), G.Arun Kumar,Dy.Jailor(AP),Md. Usman,Insp(AP),K.Saidulu,DSP(TG),Sandeep Pabba,Asst.Public Prosecutor(TG), Ms. Vishnu - - Priya C.,B. Senior Scientific Assistant,CFSL, Hyd,B.C. Balaji,ASI(AP), N. Satyanarayana,SI(TG), M Abbaiah,ASI(TG),K.Bhagavath,SI(TG),S.K. Sardar,SI(TG).

Stading 2 (L to R) S/Sri- Ashish Kumar Yadav,Sr.Scientific Assistant(physics)CFSL, Hyd, K.Vijay Kumar,Constable(AP), K.Yesu,ASI(TG), N.Sunil,Constable(TG), P.Raji Reddy,SI(TG), Adepu Shiva,Constable(TG),G.Prathapa Reddy,ASI(TG),J. Sammi Reddy,ASI(TG), Raja kumar Manukonda,DSP(AP).

Stading 3 (L to R) S/Sri-Ch.Saidulu,Constable(TG),Bunri Akhil,Constable(TG), M.Venkanna,Constable(TG),N.R.Vishnu V.Rao,PA,CFSL,Hyd,M.S.Naveen Kumar,Senior - Scientific Assistant(Chemistry)CFSL, Hyd, Aravind V,Asst. Photographer CFSL,CFSL, Hyd.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" ToT ON New Criminal Laws-2023in Collaboration with Ernst&Young LLP(PMA)Project Management Authority"

07-07-2025 to 09-07-2025

Sitting (L to R) S/Sri-Mrs.G.Sriatha,Asst.Director(AP),K.Jayanagaraj,Asst Director(AP),S.V.Balasubramanyam,Asst. Director(AP),Dr.K.Sarma Murty,Advocate, Saimantaj Patil, - IPS,Director,CDTI,Harshwardhan Singh,Consultant,EY,N.Sai Praveen,DSP(AP),Ms.Priya Jha, Scientist-B,CFSL,HYD,G.Rajkumar,Dy.SP,Course co Ordinator,CDTI

Standing 1 (L to R) S/Sri - Kayala Venkata giri,AS(AP), G.Arun Kumar,Dy.Jailor(AP),Md. Usman,Insp(AP),K.Saidulu,DSP(TG),Sandeep Pabba,Asst.Public Prosecutor(TG), Ms. Vishnu - - Priya C.,B. Senior Scientific Assistant,CFSL, Hyd,B.C. Balaji,ASI(AP), N. Satyanarayana,SI(TG), M Abbaiah,ASI(TG),K.Bhagavath,SI(TG),S.K. Sardar,SI(TG).

Stading 2 (L to R) S/Sri- Ashish Kumar Yadav,Sr.Scientific Assistant(physics)CFSL, Hyd, K.Vijay Kumar,Constable(AP), K.Yesu,ASI(TG), N.Sunil,Constable(TG), P.Raji Reddy,SI(TG), Adepu Shiva,Constable(TG),G.Prathapa Reddy,ASI(TG),J. Sammi Reddy,ASI(TG), Raja kumar Manukonda,DSP(AP).

Stading 3 (L to R) S/Sri-Ch.Saidulu,Constable(TG),Bunri Akhil,Constable(TG), M.Venkanna,Constable(TG),N.R.Vishnu V.Rao,PA,CFSL,Hyd,M.S.Naveen Kumar,Senior -

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Investigation of Economic Crime Cases(DSI),Misuse of Crypto Currency & MLAT(Mutual Legal Assistance Treaty)''

07-07-2025 to 18-07-2025

sitting (L to R) S/Sri:- K.Rajesh Babu, Inspr(AP), Pradeep Kumar, Inspr(Tech)BSF, Atharva Roshan Sharma,Asst.Commndt,BSF, Syed Muzaffar Hussain, Sr.Cyber Expert, Hyd, Salmantaj Patil,IPS, Director, CDTI, A.V.Laxmi Narasimha Chary,Dy.SP, CDTI, Mahtab Alam,DSP(Bihar),Pavan Kumar Yadav, DSP(Bihar), Uppada Venu,Inspr(Admn)CDTI.

Standing 1 (L to R) S/Sri :- Ratnadip Salokhe,API(Mah), Amol Divekar, SI(Mah), Laxman Balkrishna Bora, API(Mah), Rajendra Yadav, Inspr(GD)(Chattisgarh), Smt.Manisha Ajay Shinde, - - ASI(Mah), Smt.Gandhimathi,Inspr(TN), Subhash Chand, SI(Haryana), Vinodkumar.P.B, Inspr(Ker), Debabrata Biswas, SI(WB), Lalit Kumar,SI(Haryana), Sunder Singh, SI(Haryana).

Standing 2 (L to R) S/Sri:-Sandeep, SI(Ker), Asim Samul, SI(WB), Samrendra Singh, SI(GD)(Chattisgarh), Lalit Kumar, SI(Haryana), Vijay Kumar, SI(Haryana).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" WINDOWS & LINUX OS – FOR CYBER CRIME INVESTIGATION & ANALYSIS ''

14-07-2025 to 18-07-2025

tting (L to R) S/Sri:- Dharmendra kumar Rajendrabhai Vasava,Inspector(Gujarat),Anushil Kumar,Dy.SP(Bihar),Khushroo Siraj,DySP(Bihar),G.Rajkumar, Dy.SP, Course co - -Ordinator,CDTI, Salmantaj Patil,IPS,Director, CDTI,Dr.S.Karthikeyan,Vice Principal,CDTI,Syed Hussain,Sr.Cyber Expert, Sajjad Ali,Cyber Expert,Uppada Ven - Inspr(Admn)CDTI.

anding 1 (L to R) S/Sri :- Bahadur Singh, SI(Haryana),Sunil Kumar, Inspector(Haryana), Barot Niraj Mukeshbhai,SI(Gujarat),Ms. Shaleeni.M,SI(Tech)(TN), Mrs.S.Siva Sankari,SI(TN), Ms. Siva Meena,SI(Tech)(TN), Mrs.C.Buvaneswari,SI(TN),Rakesh Kumar,Inspector(Haryana),Kali Ram,Inspector(Haryana),Suresh Kumar,Inspector(Haryana).

ading 2 (L to R) S/Sri:-Ashish Behl,Deputy Commandant(BSF),Bhikham Prasad Tandon,SI(Chhattisgarh),A.Deva Kumar,Inspector(Tech),BSF,Bhagwat Naikar,SI(Chhattisga Kamleshkumar Ramsinh Ravat,Inspector(Tech)(Gujarat), Radheshyam Jurri,SI(Chhattisgarh),Prathamesh Sitaram Mahale,SI(Goa), Naresh kumar Yadav, - - ASI(Rajasthan).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Drone Forensics & Anti Drone Technology and use Cases of 5G in Policing "

21-07-2025 to 25-07-2025

itting (L to R) S/Sri:- Dr.K.Ravi Chandra,Inspr(Tech),SI(BI(TG),Saikat Datta,Inspr(Tech)(WB),Prasenjit Khan,Dy.SP(WB),Ravindra Kulkarni,Head Aviation Security,GMR,Hyd, Salmantaj Patil,IPS,Director, CDTI,A.V.Laxmi Narasimha Chary, Dy.SP, CDTI, Upendranath Mahapatra,Asst.Commndt(Odisha Police),Md.Qaisar Alam, - - Dy.SP(Bihar),Uppada Venu,Inspr(Admn)(CDTI).

tanding 1 (L to R) S/Sri :- Rajesh Kumar PP, Nb/Sub, Army/Military Police, Sachin Kumar, CHM, Army/Military Police, Sunil Kumar Meena,ASI(Rajasthan),Vishal Choudhary,- -Inspr(Exe)(Del),Gourav,SI(Haryana),Mrs.Subhalakshmi Gogoi, SI(Assam),Wasim Reja,SI(Tech)(WB), Prakash Kumar,SI(Bihar), Prakash Shukla,SI/GD,CRPF, Saroj Kumar Bhuyan, Warrant Officer,Air Force, Raja.S,SI(TN),Prasanna Balaji R,SI(TN).

tading 2 (L to R) S/Sri:-Rajput Bharatbhai Ganeshbhai,Army/Military Police, Hav,Durgesh Chaudhari,Hav,Army/Military Police, Chaudhary Alpesh Kumar Jagamalbhai,Ha - Army/Military Police, Centhil Kumar D,ASI(RM)BSF, Goutam Kundu,ASI(WB),Ranjith Kumar Mahato,SI(Jharkhand),Manjeet Kumar,ASI(Del),Pankaj Namd - Shinde,API(Mah),Vikas Bains,SI(Haryana),Ravi,SI(Haryana).

tanding 3 (L to R) S/Sri :- Hmangai R Hmar,Inspr(GD)CRPF,Sunil,SI(Haryana),Parveen Kumar,SI(Haryana), Veeresh G.Jakkannavar, SI(Kar),Md.Arman,SI(Bihar),Basavaraj Kale -Inspr(Kar),Akhil Madhusoodanan, Corporal,Air Force,Veknesh V,Cpl,Air Force, Rajanish Kumar Tiwari,SGT,Air Force.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Network Forensics and Analysis "

28-07-2025 to 01-08-2025

ting (L to R) S/Sri:- Mohammed Khaleel, SI(TG),Anoop A,Inspr(Ker), K.K.V.Reddy,Dy.SP, CDTI, S.Karthikeyan, Vice Principal, CDTI, Salmantaj Patil, IPS,Director, CDTI, Sandeep Mudalkar, Cyber Expert,Hyd, Mrs P.Vasanthi, Inspr(TN), Mrs V.Rama, Inspr(TN),Uppada Venu, Inspr(Admn)CDTI.

anding 1 (L to R) S/Sri : - Mohammed Sohail, SI(TG), Suresh Lal, SI(Tech)BSF, Krishna Murthy K, SI(AP), K.P.Madhu Prasad, SI(AP), Mrs.Yashica Sancoalkar,SI(Exe)Goa Police, Ms.Noor Neha Begum, SI(Assam Police), Ms.Shirisha Gogula, SI(TG), Rajesh Varma,ASI(Rajasthan Police), Md.Shadabul Haque,Inspr(Bihar).

ading 2 (L to R) S/Sri-D.Srinivas, SI(TG), Aloke Maji,ASI(Kolkata Police),Anup Kumar Sahu,SI(Jharkhand Police), Probhash Karmakar,SI(Assam Police),Alakuntla Naresh, -

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on"Basic and Intermediate on Cyber Crime Investigation & Digital Forensics"

28-07-2025 to 08-08-2025

Sitting (L to R) S/Sri:-Narendra Dayama,Dy.SP(Rajasthan),Amit Kumar Vishwakarma,Deputy Commandant,BSF, Pavitra Chakravarty,21C, CRPF, S.Karthikeyan, Vice Principal,--CDTI, Salmantaj Patil,IPS,Director,CDTI, Rupesh Mittal,Cyber Expert & Advocate,Ayush Srivastava, Dy.SP(Bihar),Anand Kumar Singh,Dy.SP(Bihar), Ms.Shahana Mukherjee, Dy.SP(Meghalaya).

Standing 1 (L to R) S/Sri :-G.Rajkumar, Dy.SP, Course co Ordinator, CDTI,Raju.P, Inspr(Exe)(Ker),Md.Shadab Alam, ASI(Bihar), M.E.Rajagopal, Inspr(Exe)(Ker),Niranjan Kumar Meena, -- SI(Exe)(Rajasthan),Mrs.Lekhika Mahanta,Inspr(Assam),Mrs.Sarita Dinesh Tawde, Inspr(GD)(Mah),Ms.Tukuna Swain,SI(Odisha),Ms.Karthika C,SI(TN), Ms.N.Swathika, SI(TN),Mrs.Manisha Ajay Shinde, ASI(Mah),Subir Santra, Dy.SP(WB), Uppada Venu,Inspr(Admn)C,DTI.

Stading 2 (L to R) S/Sri:-Sanjeev Kumar,SI(GD)CRPF, Kunal Verlekar, SI(Goa),Amol Nirmala Dilip Suryavanshi,SI(GD)(Mah),Mandip Urawn,Inspr(Jharkhand),Dwarika Nath --Thakur,SI(Jharkhand),Shambhu Sharan Das,Inspr(Jharkhand),Sidheshwar Bugappa Pujari,Inspr(Mah),Yuvraj Jagannath Suryawanshi,API(Mah), Chandan - Phukon,SI(Assam),Ratna Sadhan Noatia,Dy.SP(Tripura).

Stading 3 (L to R) S/Sri:-Chandrarajan. A,Inspr(Ker),Ishan Kaushal,Head Constable(BSF),Madan Singh,Hav(Army/Military Police),Rupendara,Hav(Army/Military Police), Rajesh Kumar Choudhary,ASI(Rajasthan),Vikash Kumar Meena,ASI(Rajasthan),Kundan gipariya,Nk(Army/Military Police)

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" "Handling CCTV Footages & DVR/NVR Forensices And Use Of Network/Footage''

04-08-2025 to 08-08-2025

itting (L to R) S/Sri:- T.Venugopal,Inspr(AP), Sandeep Mudalkar, Cyber Expert,Hyd, A.V.Laxmi Narsimha Chary,Dy.SP, CDTI, S.Karthikeyan,Vice Principal,CDTI, Salmantaj Patil, - IPS,Director, CDTI, Ms.Isha Gupta,Dy.SP(Bihar), Adham Khan A,Inspr(Exe)(Ker), Vijay.S, Inspr(TN), Uppada Venu,Inspr(Admn)CDTI.

itanding 1 (L to R) S/Sri : - Santhosh Kumar D,Hav(Army/Military Police), Chaudhari Alpeshkumar Jagamalbhai,Hav(Army/Military Police), Amitav Das,Inspr(Odisha),Tapan Kumar - - Pradhan,Inspr(Odisha), Sreejith S,SI(Exe)(Kev), Mrs.Savitra Chetan Yadav,PSI(Mah),Hans Raj,ASI(Himachal Pradesh), Bhag Singh,ASI(Himachal Pradesh), Ravi Bhushan,Sgt(Air Force),Avdesh Bhadouria,Sgt(Air Force),Rajiv Sing, JWO(AirForce).

Stading 2 (L to R) S/Sri:-Dharmender,SI(Exe)(CISF),Gautam,SI(Exe)(CISF),Ch.Vijay,RSI(TG), S.Mahesh,SI(TG),Jayakumar.A,SI(TN),Sanjeevi Kumar S K,SI(TN),Shebeeb Rahman.C - SI (Exe)(Ker),Rupesh Kumar Singh,Hav(Army/Military Police),Sunil Sharma,SI (Exe)(CISF), Deepak Kumar,SI (Exe)(CISF).

Stading 3 (L to R) S/Sri:-Sudarsi Govindaiah,SI(AP),S.Raju,SI(TG),Naveen Donapati.L/NK(Army/(Military Police),Annavarapu Praveen Naidu,SI(GD)(CRPF),Gourav Mahour,SI, - - (GD)(CRPF),Suresh Melmani,Asst. Jailor(Karnataka),Dungar Singh,SI (Exe)(CISF),Sharan A, Jailor(Kar),Venkatesh,Jailor(Karn), Amarjit Mahato,SI(WB).

itading 4 (L to R) S/Sri:-B.Nagaraju,CA,CDTI,Bipul Roy,ASI(WB),D.Chinnagangaram,ASI(TG),Mahantesh D.Badiger,Asst.jailor(Kar),Amit Sarkar,SI(WB),Shyamal Sarkar, ASI(WB Vidya Sagar Morya,Inspr (GD)(CRPF), Nilmoy Some,Inspr (GD)(CRPF),Rahul Kumar,SI(Bihar), Sanjay Patil,SI(Mah),S.Sreenivasulu,SI(GD)(CRPF).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on"Digital Forensics & Incidence responce-Electronic and Digital records under NCL"

18-08-2025 to 22-08-2025

Sitting (L to R) S/Sri:- Sandeep Mudalkar,Cyber Crime Investigator(Hyd),Subhash Dudhgaonkar,Dy.SP/DSP(Mah), Ms.Anisha Rana,Dy.SP/DSP(Bihar),Sunil Kumar,Deputy -
-Commandant,CRPF,Salmantaj Patil,IPS,Director,CDTI,Dr.Shrabanee Nayak,Addl.SP(Odisha),Ms.Papiya Sultana,SP(WB),Rajakishore Behera,Inspr(Odisha
K.K.V.Reddy,Dy.SP, CDTI.

Standing 1 (L to R) S/Sri : - Dhanraj Sibar,ASI/RO,BSF, Aravind V.R, SI(Ker),Anoop Chandran,SI(Ker),Vishal Vasudev Kuttikar,SI(Goa),Mahender Aher,API(Mah),Faisal M.S,Inspr(Ker),
Rajkumar Pegu,SI(Assam),Bitupon Chutia,Inspr(Assam),Bijit Kumar Behera,Inspr(Odisha),Deependra Kumar Sharma,SI(Rajasthan).

Stading 2 (L to R) S/Sri:-B.Shiva Kumar Yadav,SI(TG),Alok Kumar Alok,SI(Bihar),Nilesh N.Shirodkar,Inspr(Goa),Ranjitbhai Premjibhai Bavaliya,ASI(Guj),K.J.Patel,SI(Guj)
Ms.Gattu Sruthi,SI(TG),Jupally Gautham,SI(TG).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on "Web 3.0 technologies such as blockchain,decentralized applications and smart contracts

18-08-2025 to 22-08-2025

Sitting (L to R) S/Sri:- Amit Kumar,SI (Exe)CISF, Aakash Kishor,Dy.SP(Bihar),Mrs.Karanam Lakshmi Tulasi,Deputy Commandant(CRPF), A.V.Laxmi Narasimha Chary, Dy.SP, C
- Salmantaj Patil, IPS,Director, CDTI,Ms.Anjana Tudu,Addl.SP(Odisha), Mrs.Jyotsna Patil,API(Mah),Rajni kant,Insr(GD).ITBP,Uppada Venu, Inspr, -
- (Admn)CDTI.

Standing 1 (L to R) S/Sri : - Atul Kumar Verma,SI (Exe)CISFI, Manjeet Singh,SI(Exe),CISF, Dilip Tukaram Bhande,API(Mah), Ms.Smita Ramrai Naik,SI(Goa), Ms.Nashipun Shaikh,SI(
Mrs. Savita bhaskar Unde,SI(Mah),Arun Kumar,SI(Exe)CISF, Bhaskar Jyoti Saikia,SI(Assam),Nunavath Nishith,SI(TG).

Stading 2 (L to R) S/Sri:-Manish Kumar Choubey,Sergeant(Kolkata), Mukesh Kumar, ASI,BSF, Dilip Rajak, ASI(Bihar), Surinder Kumar,SI/Exe, CISF,Narayan Sharma,ASI(Raj
Manphool Bishnoi,ASI(Rajasthan).

Stading 3 (L to R) S/Sri:-Dhananjoy Karmakar,ASI(Kolkata), Satish Chand,SI(Rajasthan), Neeraj Kumar,SI (GD)ITBP,

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Investigation of Cloud Based Cyber Crime and Ransomware Attacks
08-09-2025 to 12-09-2025

Sitting (L to R) S/Sri:- Ms.Garima Dader,Dy.SP(Chhattisgarh),Shiv Pratap Singh Yadav,Asst.Commndt, CRPF, Munafkhan Pathan,Dy.SP/DSP(Guj),Rupesh Mittal,Cyber Expert,I Salmantaj Patil,IPS,Director,CDTI,Dr.B.Sriram,CEO,DSCI,Hyd,Dr.S.Karthikeyan,Vice Principal,CDTI, Vinod Rawat,Second in Command,CRPF,Thangachamy - Asst.Commndt, CRPF, G.Rajkumar, Dy.SP, Course co Ordinator,CDTI.

Standing 1 (L to R) S/Sri :- Sandeep Kumar Singh, SI(Chhattisgarh), Neelamadhab Das, ASI(Odisha), Arvind Mansingh Jadhav, ASI(Mah), Pankaj Kumar, ASI(Bihar), Laxman Narayan - Sormare,SI(Mah),Yashpalsinh Hardevsinh Chudasama,ASI(Guj),Tareshwar Pradhan,ASI(Chhattisgarh),Mayur Vegad,SI(Guj),Sagar Pathak,Inspr(Chhattisga Joyprakash Sarma, SI(Assam), L.Rathnasekhar Reddy, ASI(RO)BSF, Alpurappa, Dy.SP,CDTI.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Practical Digital Forensics:Search & Seizure of Evidence,Memory Forensics and use of CCTV Networks/Footage: Chain of Custody"
08-09-2025 to 12-09-2025

ing (L to R) S/Sri:- Rahul Chimasaheb Nimbalkar, Asst.Commndt, CRPF, Subhash Ramesh Dudhgaonkar, Dy.SP(Mah), Nishant Vaishnav, Second in Command, CRPF, Sandeep Mudalkar, Cyber Expert,Hyd, Salmantaj Patil, IPS,Director,CDTI, Dr.B.Sriram, CEO, DSCI,Hyd, A.V.Laxmi Narasimha Chary, Dy.SP, CDTS, Pankaj Shukla, Addl.SP(Chhattisgarh),Uppada Venu, Inspr(Admn)CDTI.

nding 1 (L to R) S/Sri : - Takbir Ahmad Khan, ASI(Bihar), Sunny Jain,ASI,CISF, G.Gopi Krishna, ASI,CISF, Rishi Raj, Sergeant, Air Force, Binod Kumar, Sergeant, Air Force,Chandan - Phukon,SI(Assam), Deepak, ASI(FP)(Del), Satish Anandrao Jaybhaye, SI(Mah),Ravi Kumar,Inspr(GD)BSF, Markose K.V, Inspr(Tech)BSF,Divy Pratap,SI(Exe)CISF.

ding 2 (L to R) S/Sri:- Sampad Kumar Mohanty, SI(Odisha), Harish Trimbak Choure,SI(Mah),S.Vijay, Inspr(TN),Duwendra Singh Tekam,Inspr(Chhattisgarh),Ravirajsinh M. - - Chauhan,SI(Guj), Yogesh J.Hadiya, ASI(Guj), Ashok Yadav, SI(Chhattisgarh), Amol P.Tiwalkar, ASI(Mah).

NATIONAL POLICE HACKATHON – CIPHERCOP 2025

The BPR&D/CDTI-Hyderabad, in collaboration with the Telangana State Cyber Security Bureau and Indian School of Business, Hyderabad organized a National Police Hackathon “CipherCop 2025” on 10th& 11th September, 2025 at CDTI-Hyderabad. Out of 360 proposals, selected 28 teams, with 3-5 members in each team, presented their proposals in the 2-day event of the Hackathon. The Hackathon was conducted on two themes which were identified from the 155 problem statements identified under the Police Technology Mission:

II. Themes:

a) Tracing illegal cryptocurrency transactions involving Bitcoin and other crypto currencies due to pseudo-anonymity.

b) Develop an AI/ML-powered system to detect and categorize fraudulent online content, including fake websites and mobile applications.

III. The Hackathon was inaugurated on the 10th September, 2025. Smt. Shikha Goel, IPS, Director, Telangana Cyber Security Bureau (TGCSB) was the Chief Guest and Shri Ravi Joseph Lokku, IPS, ADG, BPR&D was the Special Guest in the inaugural Ceremony. Other dignitaries present on the occasion are Shri Harshvardhan, IPS, SP, TGCSB and Smt. Shruti Mantri, Professor, ISB, Hyderabad.

IV. The Award Distribution Ceremony was held on 11-09-2025. Shri Bandi Sanjay Kumar, Hon'ble Minister of State, Ministry of Home Affairs was the Chief Guest of the event. Smt. Shikha Goel, IPS, Director, Telangana Cyber Security Bureau (TGCSB); Shri Ravi Joseph Lokku, IPS, ADG, BPR&D; Shri Harshvardhan, IPS, SP, TGCSB and Smt. Shruti Mantri, Professor, ISB, Hyderabad were present on the occasion.

V. A 3-member Jury consisting of (1) Shri Owais Ahmad, Executive Director, J.P. MorganChase (2) Shri Naguru Vema Sunny, Cyber Crime Investigation Expert (3) Dr. Sistla Srinivas Murthy, Dy. Director &HoD (Ballistics Division), CFSL, Hyderabad adjudged the presentations of the participants and selected the winners in both the themes.

PHOTOS FROM THE AWARD DISTRIBUTION CEREMONY OF THE NATIONAL POLICE HACKATHON HELD AT CDTI, HYDERABAD

PHOTOS OF THE 2 DAY NATIONAL POLICE HACKATHON HELD AT CDTI, HYDERABAD

ITEC (INDIAN TECHNICAL AND ECONOMIC COOPERATION) COURSES

I. Conducted two weeks ITEC course on 'Digital Evidence Investigation' from 30.06.2025 to 11.07.2025. 24 Sri Lankan Police Officers of the rank of SP/ ASP were participated

Dr. G K Goswami, IPS, ADGP & Director, UPSIFS, Lucknow inaugurated the ITEC course on 30.06.2025 and Mrs. J Snehaja, IFS Head of MEA Branch Secretariat & Regional Passport Officer, Hyderabad was the Guest of Honour.

Valedictory function was conducted on 11.07.2025. Sh. Sudheer Babu, IPS, CP, Rachakonda and Dr. P V K Prasad, Director Prosecution/ DG HG, Uttarakhand graced the occasion as Chief Guest & Guest of Honour respectively.

II. Conducted two weeks ITEC course on 'Cyber Security & Incident Response' from 08.09.2025 to 19.09.2025. 30 Sri Lankan Police Officers of the rank of ASP and CIs participated.

Dr. B Sriram, CEO, Data Security Council of India, Hyderabad was the Chief Guest in the inaugural ceremony of the ITEC course held on 08.09.2025

Valedictory function was conducted on 19.09.2025. Mrs. J Snehaja, IFS, Head of MEA Branch Secretariat & Regional Passport Officer, Hyderabad graced the occasion as Chief Guest and Shri. Rajeev Giroti, Director, CFSL, Hyderabad was the Special Guest.

MEMORANDUM OF UNDERSTANDING (MOU)

On 09.09.2025, CDTI – Hyderabad signed a MoU with the below mentioned Instituteswas held at the Conference Hall:

i. National Skill Training Institute (NSTI), Hyderabad and

ii. Faculty of Science & Technology (ICFAITech), Hyderabad Deemed to be University, Hyderabad

MoU was signed in the presence of

1. Shri. K Srininvasa Rao, Regional Director, SDE, NSTI, Ramanthapur, Hyderabad
2. Dr. K.L Narayana, Director, ICFAI Tech, ICFAI Foundation for Higher Education, Deemed-to-be University, Hyderabad
3. Dr. S Karthikeyan, Vice Principal, CDTI, Hyderabad
4. Shri N.P. Bhagi, Dy Director & Principal, NSTI, Hyderabad
5. Shri Vara Prasad, HoD, ICFAI Tech,Hyderabad and Staff of CDTI, Hyderabad

AWARENESS PROGRAMMES

❖ Conducted Cyber Awareness Programme for the students of Zilla Parishad High School, Ramanthapur, Hyderabad on 29.07.2025. 81 students/ teaching staff have participated in this programme.

❖ Conducted Awareness Programme on Cyber Stalking/ bullying and Cyber Crime against Women/ Children on 11.08.2025 for the students of University of Madras, Chennai. 36 students/teaching staff have participated. After the programme, they were visited various labs of CDTI, Hyderabad.

❖ Conducted Cyber Awareness Programme on "Cybercrime & its implications in law & technology" on 26-08-2025 for students of Aurora Higher Education & Research Academy, Hyderabad. 76 students and 2 faculty members participated in the programme.

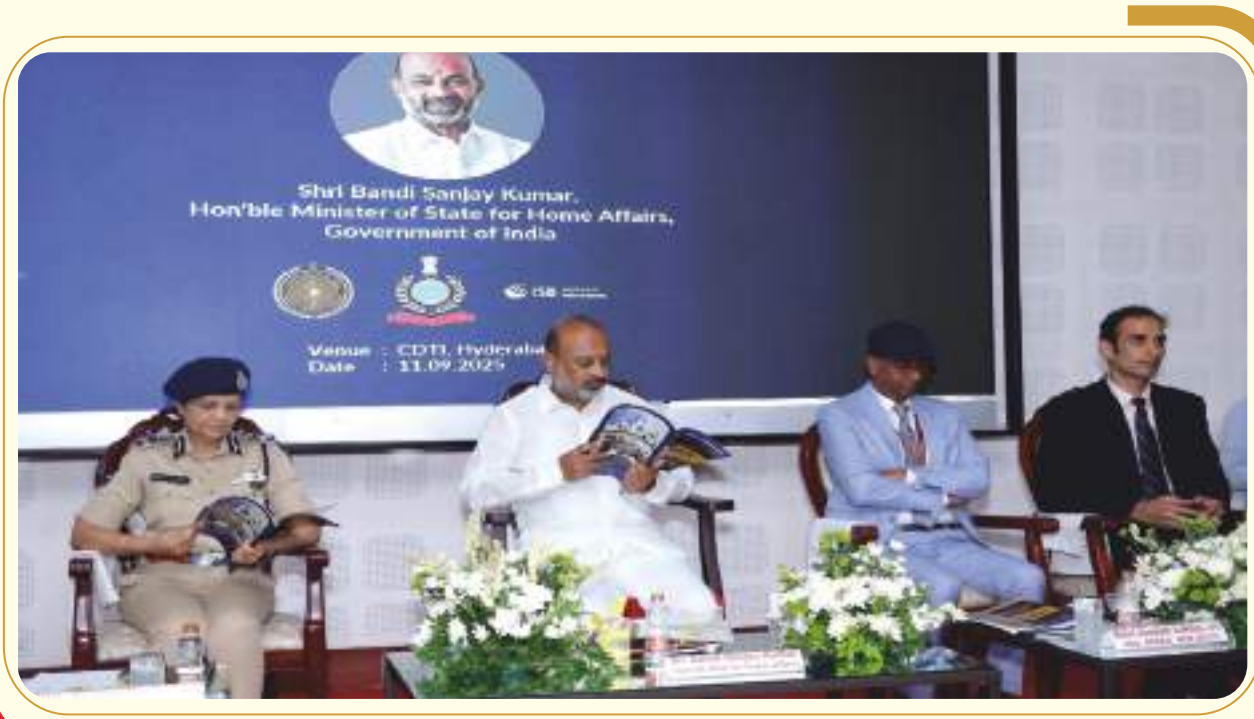
INTERNSHIP PROGRAMMES

The following students from NFSU, Dharwad and KLU, Guntur successfully completed unpaid internship programme at CDTI, Hyderabad for a period of One month in July, 2025:

S.No	Name of Student	Education	University Name
1	Ms. Kelavath Saritha	B.Sc M.Sc Forensic Science	NFSU, Dharwad
2	Ms. Aditi Swarnkar	B.Sc M.Sc Forensic Science	NFSU, Dharwad
3	Mr. Poluru Jiji Dhanve	B. Tech M.Tech Computer Science and Engineering (Cyber Security)	NFSU, Dharwad
4	Mr. Vishal Prashant S	B. Tech M.Tech Computer Science and Engineering (Cyber Security)	NFSU, Dharwad
5	Mr. K Methushueal Chandra	MBA	KLU, Guntur
6	Ms. I Chitti	B.Sc M.Sc Forensic Science	NFSU, Dharwad

PUBLICATIONS

Hon'ble MoS (Home), Govt. of India, Sh. Bandi Sanjay Kumar released CDTI quarterly magazine "Horizon" for the period Apr - Jun, 2025 on 11.09.2025 at the CDTI-Hyderabad's Auditorium during the closing ceremony of the National Police Hackathon.



OTHER ACTIVITIES

❖ Celebrated Independence Day on 15.08.2025 with the CDTI Staff and their family members. Director, CDTI, Hyderabad hoisted the national flag and issued appreciation letters to the staff.

❖ The event was followed by breakfast and special screening for the families and children of staff in the Seminar Hall of Training Block.

Photo of Flag hoisting on 15.08.2025 at CDTI, Hyderabad

CryptoSherlock X: Advanced Multi-Chain Cryptocurrency Forensics Platform for Detection and Mitigation of Digital Financial Crimes

Celebrated Independence Day on 15.08.2025 with the CDTI Staff and their family members. Director, CDTI, Hyderabad hoisted the national flag and issued appreciation letters to the staff.

The event was followed by breakfast and special screening for the families and children of staff in the Seminar Hall of Training Block.

TEAM MEMBERS

Team Lead

Sneh Singh

Contact Information: Email: sneh2105@gmail.com

LinkedIn: www.linkedin.com/in/sneh-singh-cs/

Team Members

Preksha Joshi
Contact Information: Email: jpreksha18@gmail.com
LinkedIn: www.linkedin.com/in/preksha-joshi18

Aarushi Taneja
Contact Information: Email: aarushitaneja777@gmail.com
LinkedIn: www.linkedin.com/in/aarushitaneja

ORGANIZATION

School of Cyber Security and Digital Forensics,
National Forensic Sciences University

SUMMARY

CryptoSherlock X is an advanced multi-chain cryptocurrency forensics platform designed to detect and mitigate digital financial crimes through innovative pattern recognition and cross-chain analysis capabilities. The system addresses the critical gap in cryptocurrency forensics by implementing the first operational explainable cross-chain detection system with real-time multi-blockchain integration.

The platform employs a sophisticated eight-layer modular architecture that transforms raw blockchain data into actionable intelligence and compliance-ready reports, utilizing Python's data science ecosystem with NetworkX for graph analysis, Pandas for data processing, and Plotly for visualization. The system achieves 85% detection accuracy across seven distinct money laundering patterns including peel chains, structuring/smurfing, rapid movement, layering, CoinJoin mixing, terrorist financing crowdfunding, and cross-chain laundering.

CryptoSherlock X pioneers automated cross-chain detection with 90% accuracy by correlating Bitcoin-to- Ethereum transactions through known exchange addresses within 24-hour windows, addressing the primary money laundering technique used to break audit trails across blockchain networks. The platform delivers comprehensive compliance-ready forensics with SAR-style reporting, audit trails, watchlist management, and multi-threshold alert systems, providing 70-80% cost savings over foreign alternatives while supporting up to 1,000 cryptocurrency addresses for continuous surveillance.

KEYWORDS

Cryptocurrency Forensics, Cross-Chain Analysis, Blockchain Analysis, Pattern Recognition, Risk Assessment, Explainable AI, Compliance Reporting, Real-time Monitoring.

BACKGROUND

The swift expansion of cryptocurrency transactions has fundamentally altered the sphere of financial crime, presenting unique challenges for detection and investigation. Criminals are increasingly taking advantage of digital assets to engage in intricate money laundering operations, fraud schemes, and unauthorized financing activities, which makes cryptocurrency forensics an essential area for research and development. The shift from traditional rule-based detection methods to machine learning techniques highlights the shortcomings of standard investigative approaches when faced with the complexities of modern blockchain networks. Significant hurdles include the pseudonymity characteristics, sophisticated obfuscation methods, and the complicated nature of multi-layered transactions that enable offenders to effectively mask the flow of funds. Industry evaluations showcase advanced laundering methods, such as smurfing tactics that target threshold-based detection frameworks, while cross-chain transactions and DeFi protocols further complicate investigative processes. The limitations of current forensic techniques have created an urgent need for more flexible and scalable detection systems capable of recognizing new criminal patterns in real-time.

Graph Neural Networks have surfaced as the leading technological solution for cryptocurrency forensics, showing better performance compared to traditional machine learning methods in anti-money laundering detection. Studies have demonstrated GNNs' remarkable ability to understand complex cross-entity relationships and non-linear dependencies in diverse financial networks, with models such as N2V-GCN and HexGIN establishing new standards for detection accuracy. Nevertheless, the volume of illicit activity continues to rise sharply, with inflows in 2024 projected to reach $40.9 billion, potentially surpassing $51 billion upon revision, marking one of the highest years on record. This ongoing growth, in spite of technological advancements, highlights the sophisticated evolution of criminal networks and their capacity to exploit new vulnerabilities in decentralized systems. Significant challenges remain, including scalability issues in managing the rapidly increasing transaction volumes, gaps in cross-chain analysis that criminals exploit through chain-hopping techniques, and the lack of explainability in black-box GNN models that hinders regulatory acceptance. The disjointed nature of evaluation metrics and datasets further obstructs systematic advancement, while the rise of quantum-inspired methods and continuous learning frameworks indicates a shift toward increasingly advanced detection capabilities.

LITERATURE REVIEW

The rapid proliferation of cryptocurrency transactions has created unprecedented challenges for financial crime detection and investigation. Criminals exploit digital assets for money laundering, fraud, and illicit financing, making cryptocurrency forensics a critical area of research. This literature review examines methodologies, challenges, and technological advances, with particular emphasis on graph neural network (GNN) approaches for anti-money laundering (AML) detection.

Paper Title	Contribution	Methodology	Limitations	Relevance to CryptoSherlock X
The Current State of Cryptocurrency Forensics (Dudani, 2023)	Traces evolution from rule-based to ML-based forensic methods	Survey & analysis of forensic approaches	Lacks focus on graph- based detection and scalability	Motivates shift toward advanced graph/ML models
Blockchain and Crypto Forensics: Investigating Crypto Frauds (Agarwal, Kumar & Singh, 2024)	Identifies challenges in investigating pseudonymous fraud	Case study & analysis of crypto fraud techniques	Provides problem framing but no technical solution	Highlights need for innovative forensic frameworks
What Is Smurfing? Tactics, Use Cases, and Detection (Merkle Science, 2024)	Explains structuring/smurfing laundering typologies	Rule-based thresholds and typology analysis	Industry report, no ML integration	Informs rule- based detector design for structuring
Finding Money Launderers Using Heterogeneous Graph Neural Networks (Johannessen & Jullum, 2023)	First large-scale GNN applied to AML detection	Heterogeneous Graph Neural Networks (HGNN, MPNN extension)	Focused on banking data, not blockchain	power for financial crime detection
A Graph-Based Deep Learning Model for the Anti-Money	Proposes N2V-GCN model for AML	GCN with node2vec embeddings;	Limited dataset scope;	Provides strong baseline GCN for AML detection
Laundering System (Bakhshinejad, Shokri & Yazdi, 2024		benchmarked vs classical ML	imbalance issues	
An Analysis of Novel Money Laundering Data Using HexGIN (Wójcik, 2024)	Applies HexGIN to FinCEN Files AML data	Heterogeneous GIN architecture	Restricted to banking datasets	Demonstrates superiority of advanced GNN architectures
Financial Fraud Detection Using Graph Neural Networks: A Systematic Review (Motie et al., 2024)	Provides taxonomy of GNN methods in fraud detection	Systematic review	Theoretical, no new datasets	Positions GNNs as state-of-the-art for fraud detection

Graph Neural Networks for Financial Fraud Detection: A Review (Cheng et al., 2024)	Surveys 100+ studies on GNNs in finance	Comprehensive review framework	Broad but not blockchain-specific	Confirms potential of GNNs for AML detection
Detecting and Preventing Money Laundering Using Deep Learning and Graph Analysis (2024)	Proposes hybrid GNN+LSTM AML system	Combines GraphSAGE + LSTM; 95.4% accuracy	Limited real-world validation	Inspires hybrid temporal + relational modeling
Financial Fraud Detection Using Quantum Graph Neural Networks (Innan et al., 2024)	Introduces QGNNs for fraud	Quantum- inspired GNN	Still experimental, resource- heavy	Indicates future potential for high-dimensional analysis
Advances in Continual Graph Learning for Anti- Money Laundering Applications (2024)	Reviews continual GNN learning for AML	Survey of adaptive graph learning	Lacks large- scale blockchain evaluation	Informs adaptive design for evolving laundering patterns
Anti-Money Laundering by Group- Aware Deep Graph Learning (2024)	Proposes group-aware detection	Group-aware deep GNNs	Early stage, limited benchmarking	Relevant for organized laundering detection (cartels, groups)

Challenges and Future Directions

Despite progress, persistent challenges remain:

- **Scalability:** handling exponentially growing transaction volumes.
- **Cross-chain analysis:** most works remain chain-specific, neglecting chain-hopping and DeFi-based laundering.
- **Explainability:** black-box GNNs limit adoption in regulatory and law enforcement contexts.
- **Standardization:** evaluation metrics and datasets remain fragmented, hindering comparison across studies.

Conclusion

The literature reveals a clear trajectory: from rule-based heuristics to ML classifiers and finally to GNN- based detection systems that model complex, dynamic financial networks. While GNNs have demonstrated superior detection performance, unresolved gaps in scalability, cross-chain tracing, and explainability persist.

Future work should focus on developing scalable, explainable, cross-chain forensic systems. Hybrid models (e.g., GraphSAGE + LSTM) and continual learning approaches show promise, but need operational integration. Interdisciplinary collaboration among computer scientists, investigators, and regulators is essential for building investigator-ready AML platforms.

NOVELTY

❖ **The First Operational Explainable Cross-Chain Detection System:** CryptoSherlock X features the first fully functional explainable pattern detection system, utilizing seven unique algorithms that incorporate Shannon entropy analysis for identifying layers and temporal correlation analysis for tracking cross-chain activities between Bitcoin and Ethereum networks, offering transparent, investigator-ready justifications unlike existing opaque solutions.

❖ **Real-Time Multi-Blockchain Integration with Live API Monitoring :** The platform effectively enables cross-chain analysis through correlation databases with real-time API integration via Blockstream and Etherscan, fulfilling a significant need not met by single-chain detection tools by allowing for simultaneous monitoring of Bitcoin-Ethereum transactions and detection of chain-hopping behaviors.

❖ **Comprehensive Compliance-Ready Forensics Platform:** CryptoSherlock X delivers all-encompassing SAR-style compliance reporting complete with audit trails, watchlist management, and multi-threshold alert systems, now operational as a fully functional platform for financial institutions and law enforcement, connecting academic research to applicable investigative efforts.

❖ **Future Hybrid GraphSAGE-LSTM and Continual Learning Framework**: The future plan includes groundbreaking hybrid GraphSAGE-LSTM models that merge temporal sequence learning with spatial analysis via graph neural networks, alongside advanced continual learning frameworks that facilitate real-time adjustments to new money laundering strategies, as well as quantum-inspired GNN architectures for analyzing complex financial networks innovations that are currently nonexistent in any other cryptocurrency forensic system.

OBJECTIVES

1. Comprehensive Illicit Activity Detection

   Detect and analyze suspicious cryptocurrency addresses with automated risk scoring, identifying seven distinct money laundering patterns (peel chains, structuring/smurfing, rapid movement, layering, CoinJoin mixing, terrorist financing crowdfunding, and cross-chain laundering) using advanced pattern recognition algorithms that achieve 85% detection accuracy while processing 1,000 transactions per hour.

2. Cross-Chain Analysis

   Pioneer automated cross-chain detection with 90% accuracy by correlating Bitcoin-to-Ethereum transactions through known exchange addresses within 24-hour windows, addressing the primary money laundering technique used to break audit trails across blockchain networks

3. Explainable AI and Transparency

   Generate audit-ready forensic evidence with human-readable explanations, structured evidence packages, confidence scores, pattern-specific analysis, and comprehensive trails meeting Indian Evidence Act 2023 standards for regulatory compliance and legal proceedings

4. Real-Time Monitoring and Compliance

   Enable continuous surveillance of up to 1,000 cryptocurrency addresses with automated alert generation within 60 seconds, producing regulatory-ready SAR-style reports with detailed findings and evidence to streamline AML investigations and compliance workflows

5. Interactive Visualization and User Experience

   Deliver interactive network visualizations with color-coded nodes, variable edge thickness, and time-slider functionality across multi-tab pattern-specific interfaces to enhance investigative training and make complex money laundering patterns visually comprehensible

6. Scalable and Lightweight Architecture

   Develop cost-effective indigenous solution delivering 70-80% cost savings over foreign alternatives through laptop-deployable architecture using free/open-source tools, supporting multiple data sources including live blockchain APIs, synthetic datasets, and CSV uploads for flexible enterprise scaling

7. Advanced Risk Assessment

   Implement sophisticated risk scoring using weighted maximum approach with three-tier classification (LOW/MEDIUM/HIGH) and evidence-based recommendations, coupled with entity clustering to identify real economic actors behind multiple cryptocurrency addresses

METHODOLOGY

1. System Architecture

CryptoSherlock X employs an eight-layer modular architecture that transforms raw blockchain data into actionable intelligence and compliance-ready reports. Built on Python's data science ecosystem with NetworkX for graph analysis, Pandas for data processing, and Plotly for visualization, orchestrated through a Streamlit web interface.

Layer 1: Data Ingestion and Processing Framework Multi-Source Data Integration Engine

Real-time Bitcoin Integration: Leverages Blockstream API for live blockchain data with intelligent caching mechanisms to minimize API calls and respect rate limits, providing comprehensive transaction history access with automatic retry logic.

Ethereum Network Support: Integrates with Etherscan API for cross-chain analysis, accessing transaction history, smart contract interactions, and ERC-20 token transfers with rate limiting compliance.

File Processing Capabilities: Robust CSV upload system with format validation, flexible column mapping, data quality checks, and support for large file processing through chunked reading.

Synthetic Data Generation System: Advanced generator creates realistic patterns across seven money laundering typologies: peel chains (8-hop decreasing sequences), structuring (25+ coordinated deposits), CoinJoin mixing (3-8 equal outputs), cross-chain routes (Bitcoin-to-Ethereum), rapid movement (sub-60- minute chains), complex layering (6+ hop dispersion/consolidation), and crowdfunding (15+ micro- donations). Each includes accurate address formats, timestamps, hashes, and comprehensive metadata.

Layer 2: Graph Construction and Entity Analysis Engine NetworkX-Based Graph Builder

Constructs directed graphs where nodes represent cryptocurrency addresses with attributes (label classification, transaction count, volume, activity timestamps) and edges represent payment flows with attributes (amount, timestamp, transaction hash, block height, fees). Handles complex multi-input/multi- output transactions through proper edge decomposition.

Entity Clustering Algorithm: Implements common input ownership heuristics: when multiple addresses appear as inputs in the same transaction, they're clustered as belonging to the same entity. Applies transitive closure to build complete clusters with confidence scoring, producing address-to-entity mappings, collapsed entity graphs, aggregated entity risk scores, and temporal entity evolution tracking.

Temporal Graph Filtering: Provides custom date range selection, sliding window analysis for pattern detection, time-series decomposition, event-based filtering (before/after specific transactions), and multi-resolution temporal views (hourly/daily/weekly/monthly).

Layer 3: Advanced Pattern Detection Engine Algorithm 1: Peel Chain Detection (Weight: 0.8)

Identifies sequential fund transfers with progressively decreasing amounts. Uses graph path analysis with minimum 3-hop chains, requiring 50% decreasing hops and 40% dominant outputs. Confidence calculated based on fraction of decreasing hops and dominant output patterns. Evidence includes chain length, amount decrease percentages, dominant output ratios, and temporal spacing.

Algorithm 2: Structuring/Smurfing Detection (Weight: 0.9)

Detects coordinated efforts to evade reporting thresholds through multiple small transactions. Uses time window clustering with deposits below 0.01 BTC threshold from minimum 15 distinct donors within 24- hour windows. Confidence based on effective donor count relative to minimum threshold, with penalties for rapid onward movement. Evidence includes donor count, time window, individual amounts, and onward movement analysis.

Algorithm 3: Cross-Chain Laundering Detection (Weight: 0.95)

Identifies sophisticated laundering across blockchain networks using database of 200+ exchange addresses. Correlates Bitcoin outflows to exchanges with Ethereum inflows within 24-hour windows, validating amount similarity (±10% tolerance). Confidence weighted heavily toward hop patterns with time-based scoring for rapid movements. Evidence includes source/destination addresses, exchanges involved, amount correlations, and time gaps.

Algorithm 4: Rapid Movement Analysis (Weight: 0.7)

Detects unusually fast money flows indicating automated operations. Analyzes timestamp gaps between transactions with 60-minute threshold, requiring minimum 5 transactions. Confidence increases with higher proportion of fast movements and transaction count. Evidence includes transaction count, individual time gaps, and average gap across chain.

Algorithm 5: Complex Layering Detection (Weight: 0.85)

Identifies multi-hop fund dispersion followed by reconsolidation using Shannon entropy analysis to measure transaction distribution complexity. Requires minimum 6 hops with high entropy distribution. Confidence weighted toward entropy scores with additional consideration for dispersion-then-consolidation trends. Evidence includes dispersion/consolidation points, entropy values, and amount flow analysis.

Algorithm 6: CoinJoin Privacy Mixing Detection (Weight: 0.6)

Identifies privacy mixing services through equal output patterns. Requires minimum 3 identical outputs with input diversity validation. Confidence weighted heavily toward output patterns with consideration for input diversity. Evidence includes number of equal outputs, input diversity, script type analysis, and mixing service identification.

Algorithm 7: Terrorist Financing Crowdfunding Detection (Weight: 0.6)

Identifies micro-donation patterns potentially supporting illicit financing. Requires minimum 15 unique

based on contributor patterns with bonuses for rapid onward movement. Evidence includes contributor count, donation amounts/timestamps, aggregated total, and onward movement analysis.

Layer 4: Risk Assessment and Scoring System Weighted Maximum Approach

Implements sophisticated scoring using weighted maximum rather than averaging: the final risk score is determined by the highest weighted pattern confidence score. This prevents dilution of strong signals by weaker patterns, ensuring single severe indicator triggers high-risk classification.

Three-Tier Classification Framework

Low Risk (≤0.4): Basic suspicious indicators requiring monitoring and watchlist addition
MEDIUM Risk (0.4-0.7): Significant patterns warranting detailed investigation and preliminary SAR preparation
Hight Risk (≥0.7): Severe indicators demanding immediate SAR filing, account freeze, and law enforcement notification

Evidence Compilation System

For each pattern, compiles comprehensive packages including quantitative metrics (confidence scores, transaction counts, total values, temporal spans), supporting data points (addresses, hashes, timestamps, amounts), explanatory narratives (pattern descriptions, activity reconstruction, typology comparisons), and compliance integration (FATF alignment, PMLA categories, Evidence Act 2023 standards).

Layer 5: Real-Time Monitoring and Alert Infrastructure Automated Surveillance System

Supports up to 1,000 cryptocurrency addresses simultaneously with multi-blockchain monitoring, import/export capabilities, and categorization by risk level. Continuous polling (5-60 minute intervals) with incremental transaction retrieval, automatic re-analysis against all seven patterns, and queue-based processing. Generates alerts within 60 seconds with persistent storage, deduplication, and severity-based prioritization.

Multi-Threshold Alerting Engine

Volume-Based: Default 10 BTC/100 ETH threshold for single transactions or 24-hour cumulative volume. **Transaction Count-Based:** Default 50 transactions in 24-hour window detecting velocity anomalies. **Risk Score-Based:** Default 0.7 threshold with graduated levels (0.4, 0.7) for different notification channels.

Smart Threshold Management

Features dynamic adjustment using ML-based optimization, historical false positive/negative analysis, address behavior profiling, multi-channel notifications (email, SMS, webhook), role-based distribution, escalation workflows, and complete audit trail with alert history, analyst actions, and compliance-ready reports.

Layer 6: Interactive Visualization and User Interface

Streamlit-Based Web Platform Multi-tab interface featuring dashboard overview, transaction analysis with address lookup and history tables, seven pattern-specific visualization tabs, network canvas, monitoring & alerts management, and reports & export functionality.

Dynamic Network Graphs Color-coded nodes (Green: licit, Red: illicit, Gray: unknown, Yellow: investigating) with size proportional to volume and hover tooltips. Variable edge thickness representing transaction amounts, color-coded by age, with directed arrows for large transactions. Interactive controls enable click highlighting, double-click expansion, right-click menus, and path highlighting.

Temporal Analysis Capabilities Time-slider with animated playback, adjustable speed controls, date range selection, and frame-by-frame stepping. Supports cumulative view, sliding window, event-based highlighting, and temporal heatmaps with smooth animations and risk score evolution tracking.

Pattern-Specific Visualizations Peel Chains use linear path layouts with bar charts; Structuring employs radial layouts with target-centered donors; Cross-Chain displays side-by-side blockchain views with flow diagrams; Layering shows multi-level hierarchical layouts with entropy heatmaps; Entity Clustering presents collapsed entity interactions with risk metrics.

Layer 7: Compliance Reporting & Export Framework

The SAR engine automates reports with subject details, suspicious patterns, evidence, transaction data, and recommended actions. It produces summaries, risk assessments, detailed findings, appendices, visualizations, and analyst notes, ensuring FATF, PMLA Sec. 12, Evidence Act 2023, and FIU-IND compliance.

Exports support JSON for APIs, CSV for transaction data and risk scores, PDF for formatted reports with visuals and signatures, and ZIP bundles for graphs, raw data, and manifests.

The framework integrates FATF risk-based reporting, CDD/EDD, STR filing, CVR support, and 10-year retention. It maintains Evidence Act 2023 standards through hash validation, custody tracking, audit trails, expert reporting, and immutable logs.

Layer 8: Cross-Chain Analysis and Correlation Module

Exchange Bridge Detection System: The exchange bridge system tracks 200+ exchange and bridge addresses across Bitcoin and Ethereum, covering hot/cold wallets and deposit addresses for major platforms. It detects Bitcoin outflows and correlates Ethereum inflows using ±10% amount matching within 24 hours, with support for wrapped tokens, cross-chain bridges, atomic swaps, and Layer 2 protocols.

Temporal Correlation Analysis: Temporal analysis extracts precise timestamps, scores gaps (<1h very rapid, 1 6h rapid, 6 24h moderate), and assigns confidence levels: High (>0.8) for strong matches, Medium (0.5 0.8) for partial, and Low (<0.5) for weak correlations.

Multi-Blockchain Integration Architecture: The integration framework currently supports Bitcoin and

Ethereum APIs with ERC-20 tracking, using a plugin model for standardized detection and address normalization. The roadmap includes UTXO chains (Litecoin, Bitcoin Cash), EVM chains (BSC, Polygon), privacy coins (Monero, Zcash), and account-based chains (Ripple, Stellar).

Core Technology Components

- Backend: Python 3.10+ with NetworkX, Pandas, NumPy Web Framework: Streamlit for interactive dashboard
- Visualization: Plotly for dynamic network graphs
- Machine Learning: Scikit-learn, PyTorch Geometric (optional) Database: SQLite for caching, JSON for configuration
- APIs: Blockstream (Bitcoin), Etherscan (Ethereum)

Deployment Architecture

- Hardware Requirements: Standard server with 8GB RAM, 4-core CPU minimum
- Operating System: Linux/Windows compatible
- Cloud Deployment: Docker containerization ready with AWS/Azure architecture

2. Implementation Phase Plan

Phase 1: Core Development (Months 1 2)

Goal: Build the functional backbone of the system.

- **Blockchain Data Ingestion**

1. Integrate APIs for Bitcoin, Ethereum, and stablecoins.
2. Normalize transactions into a cross-chain schema.

- **Clustering & Entity Resolution**

3. Implement heuristics (multi-input, change address, deposit address detection).
4. Integrate known entity labels (CEX, mixers, DeFi bridges).

- **Rule-Based Detectors**

5. Peel chain detection (progressive decay).
6. Structuring/smurfing detector.
7. Chain-hopping identification.

- **Risk Scoring Engine**

8. Combine rule-based indicators with entity tags into a composite score. Deliverable: Running backend pipeline producing risk-scored clusters from raw blockchain data.

Phase 2: Advanced Analytics (Months 3 4) Goal: Add intelligence and scalability.

- **Graph Neural Networks (GNN)**

9. Train GCN/GraphSAGE models on AML-labeled data (Elliptic, FinCEN Files).
10. Benchmark against classical baselines.

- **Explainability Layer**

11. Integrate SHAP/LIME edge-importance scoring for flagged clusters.
12. Store audit trails for each score.

- **Continual & Group-Aware Learning**

13. Prototype adaptive models that evolve with new laundering patterns.
14. Group-aware clustering to identify coordinated laundering rings. Deliverable: ML-enhanced detection engine with explainable alerts.

Phase 3: User Interface & Visualization (Months 5 6)

Goal: Make system usable for investigators & compliance officers.

- **Visual Dashboards**

15. Transaction graph visualization (flows, hops, cluster interactions).
16. Risk heatmaps & timeline of suspicious activity.

- **Case Management Module**

17. Generate automated case reports (PDF/HTML).
18. Allow tagging, notes, and export for investigators.

- **Integration APIs**

19. REST/GraphQL endpoints for third-party compliance systems (e.g., SIEM/SOAR). Deliverable: End-to-end user-facing product with dashboards, case reports, and API access.

Phase 4: Testing & Deployment (Months 7 8)

Goal: Ensure robustness, scalability, and compliance readiness.

- **Performance Testing**

20. Benchmark throughput (transactions/sec) & scalability (graph size).
21. Stress-test under live blockchain feeds.

- **Security & Compliance Testing**

22. Verify alignment with FATF, AUSTRAC, BPRD guidelines.
23. Implement secure data storage & access controls.

❖ **Pilot Deployments**

24. Partner with law enforcement / compliance teams for pilot feedback. Deliverable: Stable, compliant system validated in real-world pilot.

Phase 5: Full Product Launch (Month 9+)

Goal: Transition from prototype to production-ready product.

❖ **Cloud Deployment** (AWS/Azure/GCP with scalable microservices).

❖ **Continuous Monitoring & Updates** (detect new laundering typologies, integrate new entity labels).

❖ **Training & Documentation** (user manuals, investigator training sessions).

❖ **Commercialization** (licensing, SaaS model, partnerships with regulators and exchanges). Deliverable: Production-grade CryptoSherlock X deployed with full operational support.

3. Evaluation Metrics

Primary | Performance | Metrics

Detection Accuracy

- ❖ Overall Detection Accuracy: ≥ 85% across all seven money laundering patterns
- ❖ Pattern-Specific Precision: Correctly identified illicit transactions per algorithm
- ❖ Recall Rate: Percentage of actual illicit activities successfully detected
- ❖ F1-Score: Harmonic mean of precision and recall
- ❖ False Positive Rate: ≤5% for minimal legitimate transaction disruption

System Performance

- ❖ Processing Throughput: 1,000 transactions/hour with real-time analysis
- ❖ Response Time: Alert generation within 60 seconds
- ❖ System Uptime: 99% availability for continuous monitoring
- ❖ Scalability: Support for 5,000 nodes simultaneously

Cross-Chain Analysis Metrics

- Cross-Chain Correlation Accuracy: 90% in Bitcoin-to-Ethereum tracing
- Temporal Window Efficiency: 24-hour correlation with 0.95 confidence
- Exchange Detection Coverage: 200+ known exchange addresses
- Multi-Hop Identification: Track up to 3 cross-chain hops

Risk Assessment Metrics

- Risk Level Classification Accuracy: LOW/MEDIUM/HIGH precision
- Weighted Scoring Effectiveness: Maximum-weighted vs. averaging validation
- Evidence Quality: Legal admissibility of generated packages
- Audit Trail Integrity: 100% traceability of detection decisions

Real-Time Monitoring Metrics

- Watchlist Capacity: 1,000+ cryptocurrency addresses
- Alert Generation: Instant triggering upon threshold breaches
- Threshold Accuracy: Volume (10 BTC), transaction (50), risk score (0.7)
- Continuous Analysis: 24/7 monitoring with automatic re-analysis

User Interface Metrics

- Graph Rendering Speed: Real-time network visualization
- Interactive Response: Smooth time-slider, zoom, filter operations
- Multi-Tab Efficiency: Seamless pattern analysis navigation
- Export Functionality: SAR-style JSON report generation speed

Compliance Metrics

- SAR Generation: Suspicious Activity Report format compliance
- Legal Standards: Indian Evidence Act 2023 admissibility
- PMLA Integration: Prevention of Money Laundering Act alignment
- Documentation: Complete analytical process audit trails

Technical Robustness

- Error Handling: API limitations and network issue management
- Cache Performance: API response and computation efficiency
- Resource Utilization: Laptop-class hardware optimization
- Data Integrity: Zero corruption across processing stages

EXPECTED OUTCOME

Prototype Forensic Tool

A lightweight Streamlit-based application that detects suspicious wallets and clusters, identifies laundering patterns, and assigns risk scores with clear explanations.

Data Visualisations & Network Maps

Interactive time-slider graphs with color-coded nodes and variable edge thickness to highlight suspicious money flows, making laundering patterns visually obvious.

Risk Scoring & Reporting

Addresses and clusters are given [LOW/MEDIUM/HIGH] risk levels with explicit reasons. A SAR-style JSON export and watchlist mock enable investigators to generate compliance-ready reports.

Detection of False Positives

Multiple indicators must align before an address/cluster is flagged as HIGH risk. Explainable rules, supporting evidence, and human-readable justifications help investigators distinguish genuine illicit activity from benign transactions.

Advanced Hybrid ML Architecture

Implementation of GraphSAGE-LSTM hybrid models will enable dynamic pattern evolution detection with 95%+ accuracy in identifying sophisticated money laundering schemes across temporal sequences, addressing current limitations in static pattern recognition.

GNN Bases Analytics Platform

Deployment of GNN architectures will provide unprecedented high-dimensional analysis capabilities, processing complex multi-chain transactions with exponentially improved computational efficiency and pattern detection accuracy.

Enterprise-Grade RegTech Integration

Development of containerized microservices architecture will enable seamless integration into existing compliance workflows, supporting automated real-time monitoring across multiple financial institutions with standardized API interfaces and regulatory reporting protocols.

Comprehensive Multi-Blockchain Ecosystem Support

Extension to Layer-1 and Layer-2 networks including Solana, Polygon, and emerging DeFi protocols will provide complete coverage of cross-chain money laundering activities, supporting complex bridge tracking and smart contract analysis for advanced obfuscation techniques.

LIMITATION

❖ Limited blockchain coverage focusing only on Bitcoin and Ethereum, excluding major cryptocurrencies like Litecoin, Monero, Zcash, Ripple, and thousands of altcoins, creating blind spots for comprehensive financial crime investigation

❖ Reliance on external APIs (Blockstream, Etherscan) creates single points of failure vulnerable to rate limiting, API changes, or service outages

❖ Inability to effectively analyze privacy-focused cryptocurrencies like Monero, Zcash, or Dash that use advanced cryptographic techniques to obscure transaction details

❖ Streamlit-based interface may not meet sophisticated visualization and analytical needs of professional investigators, compliance officers, and forensic analysts in enterprise environments

❖ Primary testing limited to synthetic data and Elliptic research dataset with limited real-world validation through actual criminal cases and law enforcement collaboration

FUTURE SCOPE

Advanced Blockchain Integration:

❖ Comprehensive multi-chain ecosystem expansion with support for Layer 1 blockchains including Solana, Cardano, Polkadot, Avalanche, and emerging networks with chain- specific analysis algorithms

❖ Integration with Layer 2 scaling solutions like Lightning Network, Polygon, Arbitrum, and Optimism for high-value transaction monitoring

❖ Advanced integration with DeFi protocols including Uniswap, SushiSwap, Compound, Aave, and yield farming platforms to understand automated market makers, liquidity pools, and flash loans

❖ Development of NFT-specific analysis modules for detecting money laundering through digital art, collectibles, and gaming assets

Artificial Intelligence and Machine Learning Enhancement:

❖ Implementation of unsupervised algorithms including isolation forests, autoencoders, and generative adversarial networks for detecting unknown money laundering patterns and zero-day financial crimes

❖ Integration of Graph Convolutional Networks and Graph Attention Networks for sophisticated relationship analysis detecting subtle patterns invisible to rule-based systems

❖ Development of machine learning models analyzing user behavior patterns over time to identify suspicious changes in transaction habits, timing patterns, and network relationships

❖ Implementation of predictive analytics to forecast potential money laundering activities based on historical patterns, network evolution, and external risk factors

Privacy-Preserving Investigation Technologies:

❖ Zero-knowledge proof systems enabling privacy-preserving investigations analyzing transactions without revealing sensitive financial information

❖ Homomorphic encryption techniques allowing analysis of encrypted transaction data while maintaining privacy protections and regulatory compliance

❖ Advanced research into privacy coin analysis techniques including timing correlation attacks, network analysis, and side-channel analysis methods

Enterprise and Institutional Features:

❖ Comprehensive integration with law enforcement case management systems, financial intelligence units, and institutional compliance platforms

❖ Development of secure multi-tenant deployment capabilities supporting multiple organizations with isolated data environments and role-based access controls

❖ Implementation of secure collaboration features enabling information sharing between law enforcement agencies, financial institutions, and regulatory bodies while maintaining confidentiality

Budget

Category	Details	Monthly Cost ₹	Annual Cost ₹
Cloud & Infrastructure	AWS/GCP/Azure compute + storage (datasets, dashboards, reports)	8,000 - 15,000	1,20,000 - 1,80,000
Blockchain Data Access	Paid APIs / Node hosting (ETH, BTC, stablecoins)	5,000 - 8,000	60,000 - 1,00,000
Software & Tools	IDEs, GitHub, visualization, AML datasets/licenses	2,000 - 3,000	25,000 - 40,000
Testing & Security	Freelance penetration testing, audits, backups	-	40,000 - 70,000
Documentation & Reporting	Report generation, UI templates, compliance documentation	1,500 - 2,500	20,000 - 30,000
Miscellaneous	Domain, SSL, internet, hackathon fees, small hardware/network costs	-	30,000 - 50,000
Team Salaries	2 technical devs (backend + ML) , full-stack dev , compliance & security role , QA	75,000	9,00,000

CRYPTOLABS: AI-POWERED ADVANCED BLOCKCHAIN INTELLIGENCE

Effortless Blockchain Intelligence & Investigation. /~ By DarkFriday

Description

CryptoLabs is an AI-based Advanced Blockchain Intelligence solution that aids Law Enforcement Agencies in Block Chain Intelligence and Investigation. CryptoLabs also has capabilities for AML & KYC for Businesses.

Features

- **Public Exchange Detection:** Detects Public cryptocurrency exchanges for an address.
- **Real-Time Address Monitoring:** Continuously monitor specific blockchain addresses for any events (Transactions, mixing/suspicious movement activity etc.).
- **AI-NLP Investigation Assistant:** Instantly ask AI to investigate, for example, "Where did funds from wallet X go?" and receive immediate answers.
- **Transaction Mapping:** Visualize intricate transaction flows to uncover hidden connections and patterns.
- **Interactive Visualization:** Gain a clear understanding of complex blockchain data through graphical representations.
- **Wallet Profiling/Overview:** Obtain detailed insights into individual cryptocurrency wallets, including their history and associated entities.
- **Case Management and secure intel sharing:** Manage cases and get actionable exports.

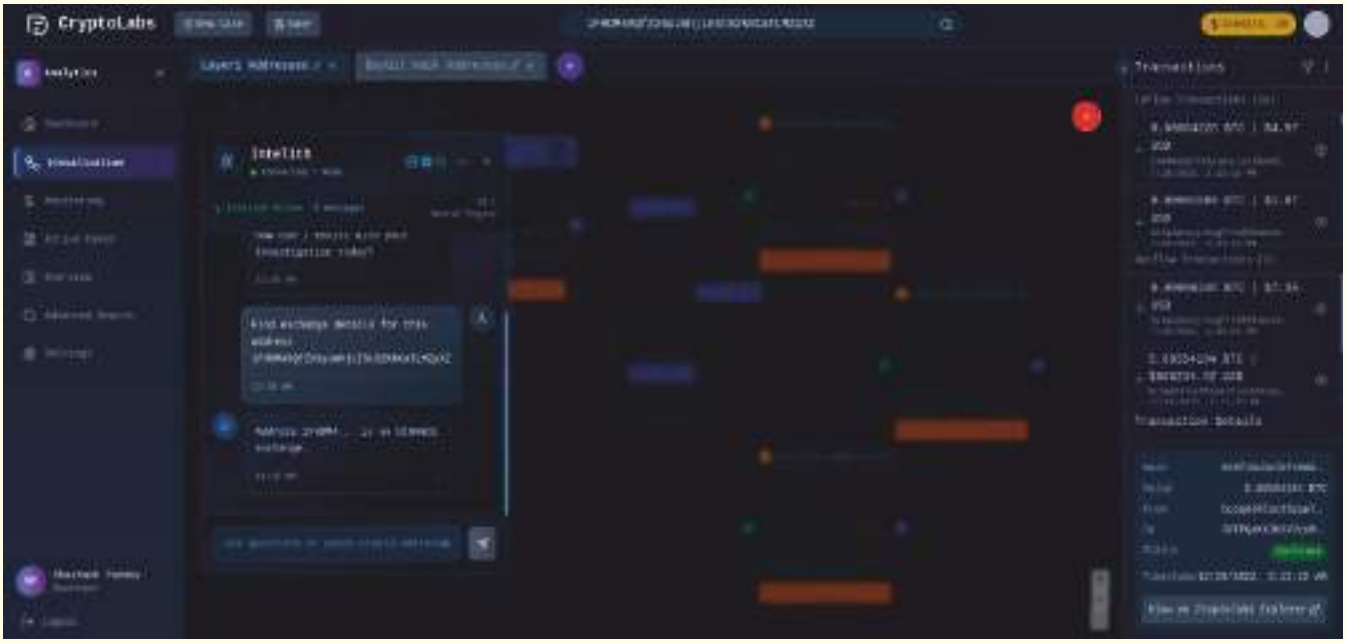
Product Demonstration

1. Dynamic Visualization and In-Depth Analysis

- In this visualization environment, users can:
  - -Visualize Address Inflow and Outflow
  - - Map All Transactions
  - - Organize Investigations with Tabs
  - - Leverage Toolbar Features
  - - Other various things

2. AI Investigation Assistant

This allows users to reduce the time spent on investigation significantly yet keeping the accuracy intact.



3. Realtime Monitoring and Alerting

CryptoLabs provides real-time monitoring capabilities, allowing users to keep eye on specific addresses or patterns of activity.

❖ Within the monitoring section, users can:

-Monitor Any Address

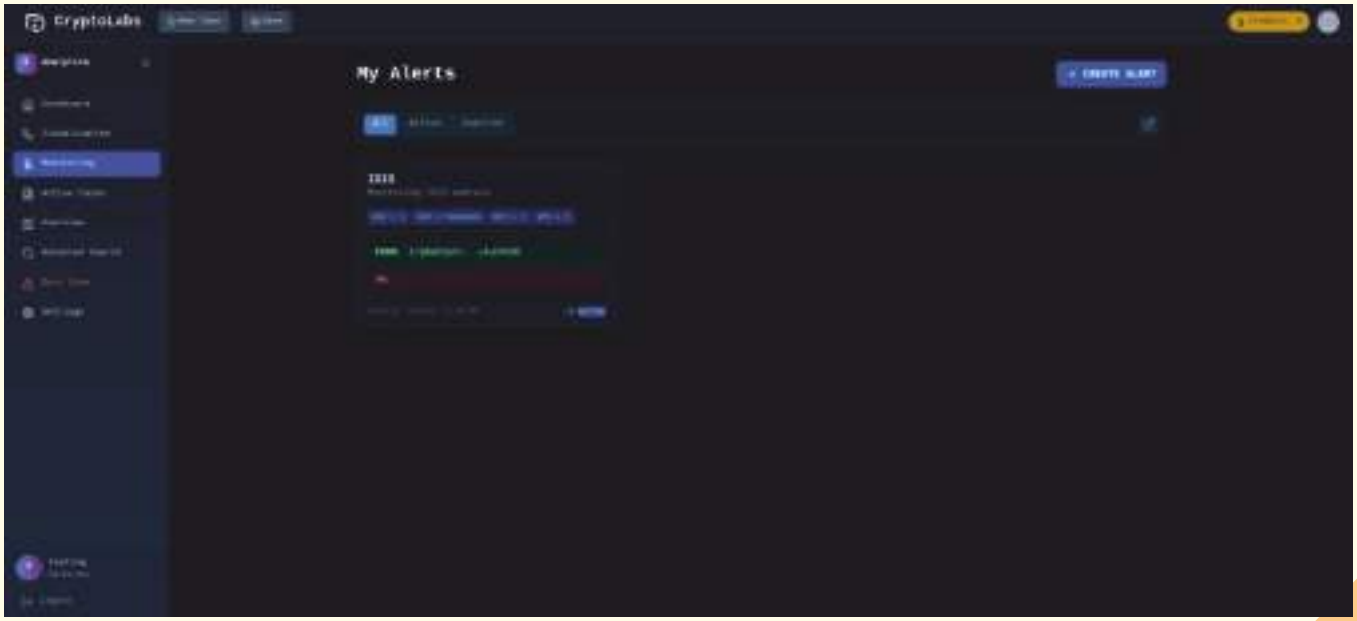
-Granular Filtering for Alerts

Amount Transferred/Received

-Specific Address Interaction

-Transaction Type

Customizable Email/Telegram/WhatsApp Notifications



4. Comprehensive Address Overview

❖ In the "Overview" section, users can:

- Quick Exchange Identification
- Transaction Summaries
- Interactive Sankey Graph of Transactions
- Surface and Darkweb Intelligence
- AI Summary

5. Advanced Timeline Analysis (Under Development)

CryptoLabs is continuously evolving and developing. While working with our own advanced Research & Development techniques. Timeline analysis will allow users to get a complete timeline on an event including an AI Articulated Summary.

Example- Address x interacted with a mixer on 12th Jan 2024 then with an exchange [Coinbase] on 30th Jan 2024.

❖ The “Timeline" section offers:

View Specific Address Timeline: A chronological record of all transactions for a selected address.

Exchange Mode: Filters the timeline to show only interactions with known cryptocurrency exchanges, aiding asset tracing.

-Suspicious Mode: Flags suspicious transactions with known suspicious wallets or entities for immediate investigation.

HOP Mode: Analyzes intermediary transactions between an address and exchanges, helping understand money laundering patterns.

Tron Investigation

- **Exchange Detection:** Automatically identify interactions with global and Indian crypto exchanges for real-world attribution.
- **Linked Addresses:** Map and visualize all addresses connected to a target wallet to uncover hidden relationships.
- **Labeling:** Tag addresses with custom intelligence (e.g., "Scammer," "Mixer," "Exchange") for quick identification and reporting.
- **Clustering:** Group multiple addresses belonging to a single entity to de-anonymize complex operations.
- **Transaction Money Flow:** Visually trace the complete path of funds with amounts between all involved wallets.
- **Multi-Hop Analysis:** Automatically detect and map intermediary transactions between a source and destination, revealing money laundering patterns.
- **Timeline Analysis:** Filter and search all transaction history based on specific dates and times for precise event reconstruction.

Darkweb & surface co-relation

- **Shadow intelligence:** scrap GitHub, telegram, social media, or all surfaces we things.
- **Darkweb co-relation:** onion links, crypto address, label APT, DRUGS, ONION addresses, hidden service ss(optional), keyword search, cluster, address, entity. (username, email, contact) [optional]
- **AML/KYT**
- **Demixing**

Use Cases

- Crypto Investigation
- Blockchain Intelligence
- National Security - Terror Funding Cases
- Advanced Monitoring - Police/Other causes
- Finance - ED, SEBI
- Businesses - KYT/AML/Compliances

Future Plans

Features (Working on):-

- Complete social media & Dark web correlation
- De-mixing / swaps
- Multi hops detection
- Complete AI Automation - Enter an address and relax ai will do everything
- KYT/AML
- Multichain monitoring (BTC TO ETH/USDT/USDC)
- Cross chain investigation

We have tried our best to explain the gist of what we have and what we are working on.

[Plans can't be explained on a doc]

However, it is not possible to explain everything in just one PDF.

For further queries / opportunities / early access contact us via phone/email.

Thank You!

PROPOSAL FOR COLLABORATION ON TRAP (THREAT RECON & ATTRIBUTION PLATFORM)

Submitted to: Bureau of Police Research & Development (BPRD)
Division: Cyber Division - CDTI
Submitted by: Team TRAP

1. Background & Context

At the CipherCop Hackathon organized by BPRD, TRAP (Threat Recon & Attribution Platform) secured 3rd place nationally, recognizing its innovation, investigative relevance, and potential to strengthen capabilities in tackling crypto-enabled and cyber-facilitated crimes.

With the rapid rise in cryptocurrency-driven frauds, darknet activities, and anonymized financial flows, law enforcement requires indigenous, investigator-friendly, and scalable solutions. TRAP has been built specifically to empower Indian LEAs with actionable intelligence and to reduce dependency on foreign investigative tools.

2. About TRAP

TRAP (Threat Recon & Attribution Platform) is a SaaS-based investigative suite designed for law enforcement and cybercrime investigation units. Its core features include:

- Crypto Tracing - Tracking wallets, exchanges, mixers, and illicit fund flows.
- Darknet & Telegram Monitoring - Automated reconnaissance of illicit forums, markets, and groups.
- OSINT Profiling - Digital footprint analysis of phone numbers, emails, and accounts for attribution.
- Wallet Risk Scoring - Behavioral tagging, transactional pattern analysis, inbound/outbound volume monitoring.
- Investigation-Ready Reports - Exportable reports suitable for case files and prosecution.

The platform is modular, automation-driven, and requires minimal training, making it suitable for adoption by cyber labs and field investigation units.

3. Alignment with BPRD & CDTI Mandate

TRAP directly supports CDTI's mandate by:

- Strengthening investigative capacity in cryptocurrency and darknet crimes.
- Offering operational independence through an indigenous alternative to foreign tools.
- Providing scalable deployment options across state cyber cells and district units.
- Supporting knowledge transfer through integrated training workflows and investigator handbooks.

4. Proposed Collaboration Model

1. Pilot Deployment

Deployment of TRAP at CDTI on a pilot basis with access for select investigators.

Evaluation of performance on real case datasets such as cryptocurrency wallets and darknet intelligence.

2. Feedback & Customization

Refinement of platform features based on officer feedback.

Integration with existing cyber forensic and investigative systems.

3. Capacity Building

Specialized training modules for CDTI investigators.

Development of a TRAP-aligned investigator handbook on cryptocurrency and darknet crimes.

4. National Scale-Up

Based on pilot outcomes, explore structured scale-up via BPRD for adoption by state and district-level cybercrime units.

5. Expected Outcomes

- Strengthened CDTI capability to investigate crypto-enabled and darknet crimes.
- Reduced reliance on foreign vendor solutions.
- Creation of standardized, investigator-ready workflows for crypto attribution and forensic reporting.

Contribution towards Atmanirbhar Bharat in the domain of cyber enforcement technologies.

6. Way Forward

We request BPRD's support to:

- Initiate a formal pilot of TRAP at CDTI.
- Nominate a nodal officer for coordination.
- Establish a joint working group for evaluation and roadmap planning for scale-up.

7. Contact Details

Lakshit Verma

Founder - TRAP (Threat Recon & Attribution Platform)

+91-9303556894

Proposal for
The Cipher Cop 2025
National Police Hackathon Compendium

1. Proposal Title: CyberVajra

1. Introduction

The digital threat landscape is growing more complex, with phishing, fraudulent apps, defacements, and zero-day attacks eroding trust and endangering national security. Traditional tools often fall short limited to known signatures, lacking context, and offering little investigative depth.

Cyber Vajra was built to change that. It makes cybersecurity simple and accessible -

enabling citizens to scan and verify suspicious websites or apps in seconds, while equipping law enforcement with a powerful, field-ready investigative tool.

Designed as a **first line of defence,** CyberVajra helps users "check before they click" and connects them directly to official complaint portals. It transforms cybersecurity from passive alerts into a complete cycle of **awareness, detection, and action.**

2. Problem Statement

India is among the **prime global targets** for phishing campaigns, fraudulent websites, malicious domains, and rogue mobile applications. Adversaries deploy convincing clones of trusted services to harvest data, spread malware, and exploit user trust often slipping past conventional defences.

Current solutions are **reactive and fragmented**: they rely on user complaints or slow takedowns, miss zero-day threats, lack behavioural context, and fail to deliver investigation-ready intelligence.

What's needed is a **next-generation AI/ML-driven system** that proactively detects, classifies, and explains fraudulent online content from phishing domains and scam applications to cloned websites by analyzing WHOIS, DNS, SSL, app metadata, network behaviour, and visual similarity. Leveraging NLP to flag suspicious language, computer vision to detect UI cloning, and machine learning to categorize risks, such a system can provide clear, actionable intelligence tailored for both citizen safety and law enforcement investigations.

3. Proposed Solution - Cyber Vajra

CyberVajra is a next-generation, AI-powered mobile and web security platform that bridges the gap between citizen safety and law enforcement investigations. Built with a Flutter frontend and a Python (FastAPI/Flask) backend, it performs deep analysis of websites, domains, and Android applications to detect malicious behaviour and deliver actionable intelligence.

Unlike conventional scanner, CyberVajra doesn't just raise red flags - it explains the "why" behind the threat, using a fusion of machine learning, natural language processing, computer vision, and dynamic runtime analysis. This multi layered approach exposes phishing domains, fraudulent apps, and malicious websites that traditional tools often miss.

Designed for real-world impact. CyberVajra enables citizens to scan suspicious websites or APKs within seconds and instantly file complaints through official government channels. For investigators, it functions as a field-ready forensic companion, capable of scanning seized devices or apps on-site, drastically reducing manual effort. Beyond investigations, it also serves organizations and educational institutions as a preventive and awareness-building platform, strengthening internal defences and cultivating cyber hygiene

4. System Architecture

The platform is designed with modular components to ensure scalability, performance, and investigative depth:

Frontend (Flutter):

1. Cross-platform mobile interface with a single codebase.
2. Delivers fast, consistent experience for citizens and investigators.

Backend (FastAPI/Flask):

1. Lightweight, high-performance API layer for real-time processing.
2. Seamlessly integrates with external services and government portals.

AI & ML Engine (Scikit-learn, LightGBM, Pandas):

1. Performs accurate classification and behavioural modelling.
2. Provides explainable intelligence for investigative insights.

Image Processing (OpenCV + Perceptual Hashing):

1. Detects cloned interfaces, fake logos, and visual anomalies.
2. Catches threats that text- or signature-based tools miss.

Version Control (Git/GitHub):

1. Ensures secure and collaborative development.
2. Supports scalability, transparency, and maintainability.

Unique Advantage: Combines **citizen accessibility with forensic-grade investigative depth,** enabling real-time threat detection and actionable intelligence in one platform.

5. Core Capabilities and Features

5.1 Website Threat Analysis

Cyber Vajra performs multi-layered assessments of websites and domains:

- Content Analysis:
  1. Detects phishing keywords, urgency cues, and linguistic anomalies.
  2. Identifies social engineering tactics to flag suspicious content.
- Reputation Checks:
  1. Cross-references with trusted and malicious domain lists.
  2. Integrates external threat intelligence for enhanced accuracy.

❖ Network & Header Analysis:

1. Monitors redirects, HTTP headers, and network behavior..
2. Provides context for communication patterns of harmful sites.

❖ Visual Similarity Detection:

1. Uses perceptual hashing and template matching.
2. Detects cloned interfaces and spoofed brand assets.

❖ Domain Intelligence:

1. Collects WHOIS, SSL, DNS records, and hosting history.
2. Assesses authenticity and traces malicious infrastructure.

- Risk Scoring: Consolidates all findings into a **0-100 score** to help investigators prioritize threats by severity and confidence.

5.2 Android APK Analysis

CyberVajra conducts static and dynamic APK analysis to uncover malicious behavior:

❖ Metadata Verification:

3. Checks package names, sources, sizes, and hashes.
4. Detects tampering or repackaging attempts.

❖ Permission Assessment:

1. Flags excessive or dangerous permissions (e.g.. SMS, camera, device admin).
2. Helps identify apps with potential privacy or security risks.

❖ Code Inspection:

1. Detects embedded URLs, obfuscation, and hidden payloads.
2. Uncovers malicious logic or backdoors in the app code.

❖ Behavioral Observation:

1. Runs apps in a controlled environment to monitor runtime actions.
2. Detects anomalies and traces potential command-and-control communication.

❖ AI-Based Classification:

1. Uses machine learning to flag suspicious apps with no prior data.
2. Provides an additional layer of zero-day threat detection.

6. Operational Workflow

CyberVajra's end-to-end workflow is designed for ease of use, speed, and actionable intelligence, ensuring investigators can respond to threats efficiently:

❖ Submission:

1. Investigators submit a suspicious URL or APK via the mobile interface.

2. The platform ensures a simple, intuitive submission process that requires minimal technical effort.

❖ Backend Routing:

1. The FastAPI backend automatically routes each submission to the appropriate analyzer pipeline.

2. This ensures fast, accurate processing while maintaining system scalability and reliability.

❖ Threat Analysis:

1. Specialized modules perform multi-dimensional analysis content, network, domain, metadata, and runtime behavior.

2. AI, NLP, and computer vision work together to detect known and zero-day threats.

❖ Risk Evaluation:

1. Results from multiple analyzers are consolidated into a comprehensive, explainable risk score.

2. The scoring engine prioritizes threats based on severity and confidence. enabling investigators to focus on high-priority cases.

❖ Reporting & Action (Law Enforcement Focused):

1. Findings are presented in a structured, color-coded report. highlighting risk levels, indicators of compromise, and actionable intelligence.

2. Investigators can use these reports forfield operations, evidence collection, and legal proceedings, ensuring a seamless transition from detection to enforcement.

Impact: This workflow transforms CyberVajra into a proactive investigative tool, reducing response times, empowering law enforcement, and deliveringinvestigation-ready intelligence in real time.

7. Artificial Intelligence and Machine Learning Integration

CyberVajra employs AI and ML models throughout the detection pipeline to improve accuracy and extend beyond traditional signature-based approaches. It analyzes linguistic patterns to flag phishing attempts, employs computer vision to detect cloned interfaces, and leverages behavioral modeling to identify previously unseen threats.

By continuously learning from new data and correlating it with open-source intelligence, Cyber Vajra enhances its detection capabilities over time and remains effective against evolving threat landscapes.

8. Distinguishing Features and Advantages

While most existing solutions focus solely on detection, CyberVajra is designed as a complete investigative and citizen-centric platform. Its distinguishing strengths include:

❖ **Dual-Use Design:** A single tool that serves both citizens and investigators from verifying suspicious websites to conducting field investigations.

❖ **Zero-Day Threat Detection:** Identifies unknown threats even without existing signatures by

analyzing behavior, permissions, and communication patterns.

❖ **Behavioral Insight:** Observes runtime activity of URLs and apps to reveal malicious intent that static analysis may overlook.

❖ **OSINT Integration:** Enriches analysis with intelligence gathered from external open sources, supporting attribution and context building.

❖ **Direct Complaint Filing:** Bridges the gap between detection and action by redirecting users to official reporting portals within the app.

❖ **High Accuracy and Speed:** Ensures rapid results with low false positives, critical in active investigations.

❖ **Forensic-Grade Reporting:** Generates structured reports suitable for use as evidence in legal and investigative proceedings

9. Strategic Impact

Cybercrime threatens national security, public trust, and organizational integrity. Cyber Vajra empowers law enforcement agencies with real-time visibility, explainable intelligence, and actionable recommendations, enabling a shift from reactive response to proactive defense.

❖ For Law Enforcement:

- Acts as a field-ready investigative tool, capable of scanning suspicious websites and APKs on-site.

- Provides structured, forensic-grade intelligence, reducing hours of manual analysis and accelerating case resolution.

- Supports evidence collection, legal proceedings, and decision-making with clear, actionable insights.

❖ For Citizens:

1. Serves as a first line of defense, allowing users to "check before they click" and avoid phishing, scams, and malicious apps.

2. Raises awareness and promotes safer digital behavior, reducing the overall cyber risk in the community.

10. Future Enhancements

To expand Cyber Vajra's effectiveness, scalability, and investigative reach, upcoming versions will include:

❖ **PDF & Forensic Reporting:** Generate court-ready, structured reports that consolidate findings, indicators, and risk scores for legal and investigative use.

❖ **Image & Deepfake Detection:** Advanced visual analysis to verify authenticity of media and detect manipulated content in websites, apps, and documents.

❖ **Regional Language Support:** Multilingual interface to ensure broader accessibility across jurisdictions and diverse populations.

❖ **AI Chatbot & Voice Assistance:** Interactive support to guide field officers in real-time

during investigations and threat analysis.

- **SOC/SIEM Integration:** Enable automated alerts and blocking recommendations for enterprise environments, connecting CyberVajra to organizational defense systems.

- **Virtual Sandbox Environment:** Secure, isolated execution of suspicious URLs and APKs, allowing Investigating Officers to analyze malware behavior safely and gather actionable intelligence.

11. Team and Contact Information

- **Tashee Bisht -** Backend Developer & Team Leader
- **Himesh Kumar -** Frontend & UI/UX Developer
- **Gopal Mohan Jee -** Cybersecurity Expert
- **Praharsha Kumar -** AI/ML Developer

Contact: tashee.555@gmail.com

GitHub: https://github.com/Praharsha0333/cyber vajra.git

Demo Video: https://youtube.com/shorts/E-hiYJwh7ik?si=qEoV4aYMx0VCEABU

12. Conclusion

CyberVajra is first and foremost a field-ready investigative tool for law enforcement, providing real-time, explainable intelligence, forensic-grade reports, and actionable insights to detect, analyze, and mitigate cyber threats efficiently. Its AI-driven detection, behavioral analysis, and OSINT integration transform investigations from reactive responses into proactive, evidence-backed operations.

At the same time, CyberVajra empowers citizens as a first line of defense, allowing them to verify suspicious websites and applications, raising awareness and reducing exposure to scams.

In essence, Cyber Vajra bridges citizen safety with law enforcement capability, strengthening India's digital ecosystem and enabling a safer, more trustworthy cyberspace truly a "Made by India, for the World" solution.

PROPOSAL FOR THE CIPHERCOP 2025 NATIONAL POLICE HACKATHON COMPENDIUM

1. Proposal Title:

FraudFence – AI-Powered Scam Shield

2. Team Information:

Team Name: FraudFence
Team Members:

1. Lubna Fatima
2. Diksha Gour
3. Sunanya Nareddy

3. Abstract / Executive Summary:

FraudFence is an innovative, dual-platform solution designed to combat the escalating threat of online scams. It integrates a powerful AI-powered website with a seamless browser extension to proactively protect citizens. By analyzing text, images, and URLs in real-time across multiple languages (English, Hindi, and Spanish), FraudFence detects sophisticated fraud patterns and provides users with immediate risk assessments, educational guides, and trending scam news, fostering a safer online environment for everyone.

4. Problem Statement:

India faces a significant and growing threat from cybercrime. Based on current trends from the Indian Cyber Crime Coordination Centre (I4C), the number of cybercrime cases in India for 2025 is projected to be between 2.4 and 2.5 million. The financial impact is staggering, with average monthly losses from financial cyber fraud in the first half of 2025 reaching approximately □1,000 crore, potentially exceeding □1.2 lakh crore annually. This alarming trend highlights an urgent need for advanced, accessible tools to protect the public from sophisticated online scams.

5. Proposed Solution:

FraudFence addresses this challenge directly with a two-pronged approach:

1. **AI-Powered Website:** A central hub where users can manually check for scams by submitting suspicious content such as text, images, or URLs for instant AI analysis. The site also serves as an essential educational resource, featuring curated scam news and comprehensive guides on fraud prevention and recovery.
2. **Seamless Browser Extension:** This extension acts as a real-time guardian, automatically scanning websites as the user browses. It flags suspicious elements and provides immediate alerts, preventing interaction with malicious content before it can cause harm.

The entire platform is designed with a modern, user-friendly interface (with light and dark modes) and supports multiple languages to ensure broad accessibility and a comfortable user experience.

6. Technical Architecture & Methodology:

The core of FraudFence is an advanced AI model trained to identify sophisticated fraud patterns.

1. Input Analysis: The system accepts and analyzes three types of input: plain text, images (for signs of tampering or malicious content), and URLs (for phishing or malware links).
2. AI Detection: Sophisticated algorithms process the input to detect indicators of fraud, such as phishing language, malicious links, or signs of impersonation in images.
3. Real-time Alerts: The browser extension integrates directly into the user's browsing experience, providing non-intrusive, real-time alerts on potentially harmful pages or links.
4. User Interface: The platform features a clear and actionable UI/UX. Analysis results are displayed with an intuitive "Fraud Meter" and a detailed explanation of the AI's findings to empower the user with knowledge.

7. Key Features and Benefits:

Key Features:

1. **AI-Powered Fraud Detection:** Leverages AI to analyze text, images, and URLs for potential scams.
2. **Real-time Browser Extension:** Provides continuous protection by flagging suspicious elements as you browse.
3. **Trending Scam News**: Keeps users informed about the latest fraud trends with an automatically updated news feed.
4. **Educational Guides:** Offers comprehensive guides on identifying scams, prevention, and recovery steps.
5. **Multi-lingual Support:** Operates in English, Hindi, and Spanish to reach a wider audience.
6. **Analysis History:** Allows users to track their past submissions and results.

Benefits:

1. **Enhances Citizen Safety:** Proactively protects the public from financial loss and data theft.
2. **Increases Public Awareness:** Educates users on the nature of modern cyber threats, turning potential victims into vigilant citizens.
3. **Empowers Users:** Provides clear, actionable information to help users make safe online decisions.
4. **Supports Law Enforcement:** The data on emerging scam trends can serve as a valuable resource for police research and strategic development.

8. Implementation Plan & Scalability:

The FraudFence prototype has successfully demonstrated core functionality. The immediate plan involves refining the AI models with larger, more diverse datasets to improve accuracy and reduce false positives. Future steps include expanding language support and launching a public beta to gather user

feedback for further improvements. The architecture is built for scalability, with the potential for future integration with national cybercrime reporting portals and deployment across government platforms to maximize its protective reach.

9. Conclusion:

FraudFence provides a robust, user-centric solution to the critical issue of online fraud. By combining state-of-the-art AI detection with continuous user education and real-time alerts, it empowers individuals to navigate the digital world safely. This proposal offers a tangible and effective tool that can be immediately valuable in the national effort against cybercrime, aligning perfectly with the mission of the Bureau of Police Research & Development.

S.C.O.U.T. (Secure Cyber Operations for Uncovering Threats)

Introduction

S.C.O.U.T. (Secure Cyber Operations for Uncovering Threats) is a focused, AI-assisted prototype that quickly classifies websites as Legitimate, Suspicious, or Phishing and — crucially — returns clear, human-readable reasons why a site was flagged. The system balances fast metadata heuristics with deeper NLP and computer-vision checks so analysts can act immediately with context.

Problem Statement

Fraudulent websites impersonate trusted brands to steal credentials, push malware, or run scams. Security teams need a compact tool that:

5. Produces a clear verdict: Legitimate, Suspicious, or Phishing.
6. Provides actionable reasoning for each verdict so analysts can prioritize and respond.
7. Integrates with existing CV/NLP modules to strengthen the evidence chain when required.

Methodology

8. Ethical Web Crawling and Data Extraction — Adhere to robots.txt and follow rate limits. Extract HTML content and headless screenshot of webpage.
9. Rapid metadata triage — WHOIS (age/privacy), SSL, DNS, URL heuristics (length, keywords), homograph/ASCII fraud checks.
10. Dynamic checks — headless browser (Selenium/Playwright) for popups, alerts, suspicious login forms, and redirects.
11. Evidence aggregation — combine deterministic rule scores with selective CV/NLP signals and threat-intel (VirusTotal/SafeBrowsing) where available.
12. Enhance explainability — After classification as genuine or fake, use an LLM to add a sub-classification like scam / phishing / malware / clone and a brief description explaining the tags.
13. Final output — single label (Legitimate / Suspicious / Phishing) + normalized risk score + concise reasons explaining the decision.
14. Continuous improvement: To ensure the model remains accurate and adapts to evolving fraud tactics, a human-in-the-loop (HITL) feedback mechanism.

Unique Selling Points (USPs)

15. Triage-first design: Fast metadata checks generate verdicts instantly.
16. Explainable outputs: Every flag includes concise reasons.
17. Selective deep analysis: Apply CV/NLP only where metadata is ambiguous.
18. Practical labels: Single-label output — Legitimate, Suspicious, or Phishing.
19. Extensibility: Easily plug in SafeBrowsing, VirusTotal, or internal blacklists.

Team

20. Krishnan C S
21. Chandralekha P
22. Vishnu Tella
23. Chirayu Mehta

CENTRAL DETECTIVE TRAINING INSTITUTE HYDERABAD

cdtshyderabad@nic.in
cdtihyd@gov.in
040-27038182, 29704150

@bprdcdtihyd
@bprdcdtihyd
@bprdcdtihyd

Address :
CDTI, Ramanthapur,
Hyderabad,Telangana,
Pin-500013

Editor in cheif : Shri Salmantaj Patil, IPS, Director
Editor : Shri V Bheemakrishna Naik, PA (TRG.)