International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Zero Day Cyber Crime Investigation

Yash Dipakkumar Kanani[1], Raval Hitarth Hareshkumar[2], Zubin Dhanjhisha Daruwala[3] ,Khara Balvant Shantilal[4] ,Mrudang Ashish Shah[5], Miki Kantibhai Patel[6]

[1]Yash Dipakkumar Kanani Assistant Prof. CS/AI Department & College
[2] Raval Hitarth Hareshkumarant (Asst. Prof.)(Computer Engineering Department)
[3]Zubin Daruwala student ofCivil Engineering
[4]]Balvant Khara(Asst. Prof.)(Computer Engineering Department)
[5] Mrudang Ashish Shah Computer Science Engineering
[6]Miki Kantibhai Patel Assistant Prof. CE Department & College

Under Guidance: *Dr. Kamalesh V N Vice Chancellor of Gandhinagar University*

Abstract -This paper puts forward a full Zero-Day Cybercrime Response Framework aimed at India. It requires Digital Service Providers, or DSPs, to hand over requested metadata to investigators in just 30 minutes. The setup pulls together legal, technical, operational, and enforcement parts to speed up law enforcement against new cyber-attacks. It draws from India's current IT laws, like the IT Act from 2000 and the IT Rules of 2021, plus newer stuff such as the Data Protection Act of 2023 and CERT-In guidelines. This way, DSPs meet quick data demands while still protecting privacy. Main pieces involve automatic spotting of incidents, safe ways to get data, and checks from groups like CERT-In, the Ministry of Home Affairs or MHA, and the National Cybercrime Reporting Portal, known as NCRP. We look at how this stacks up against other countries' approaches, say China's Cybersecurity Law, the EU's e-evidence system along with GDPR, and US methods including the CLOUD Act and tools for endpoint detection. From that, we pull useful ideas and make sure it fits global norms. Figure 1 shows a flowchart of the whole process. We spot likely problems, things like data staying local, court supervision, and issues across borders. Then we talk about fixes, using AI for analysis, legal protections, and deals between nations. Overall, our look shows that a solid 30-minute rule for metadata, backed by tech automation and clear rules, could really boost India's handling of cybercrimes. And it does this without stepping too hard on personal rights.

***Key Words*:** Zero-day vulnerability, zero-day exploit, zero-day attack, zero-day malware, unpatched flaw, novelty exploit, zero-day disclosure, exploit marketplace, advanced persistent threat, signatureless detection, heuristic detection, anomaly detection, patch management, exploit stockpiling, software supply chain, weaponised vulnerability, digital forensics, incident response, threat intelligence, exploit mitigation.

1.INTRODUCTION

Getting a fast handle on zero-day cyber-attacks, those unknown exploits that pop up out of nowhere, matters a lot for national security. In India right now, investigators sometimes wait days or even weeks to get data from third parties. That's because digital clues often sit with middlemen or servers overseas. Such waits mess up quick action by police and let bad guys wipe their tracks. We suggest making it a legal must for DSPs to provide metadata like logs, subscriber details, device IDs to approved agencies in 30 minutes. India hasn't seen a rule like this before, but it's similar to quick-response setups in other places. For instance, CERT-In calls for 6-hour incident reports, and the US has ideas for 24 to 72-hour notices on breaches. This paper lays out a response flow that mixes automated spotting with AI and analytics, plus legal and process protections. The goal is to cut down on cyber fraud, ransomware, child exploitation, terrorism. It brings in CERT-In as India's cyber emergency squad, the MHA, and the NCRP portal so public complaints feed right into the system. We review Indian laws, sections like 69 and 69B of the IT Act for interception and traffic data, CrPC Section 91 for summons, CERT-In rules, and the fresh Data Protection Act 2023. We compare it to what's done abroad. Plus, we think about opposing factors, localization rules, privacy concerns, delays in cross-border MLATs, and offer ways around them. Our big input here is one combined framework that fits India's situation and matches top global practices.

2. Body of Paper

Earlier studies on police getting digital evidence stress the push for standard, quick data-sharing setups. In India's legal scene, cops often rely on CrPC Section 91 to call for any document or item in probes. The IT Act allows targeted intercepts under Section 69 and keeping traffic data via Section 69B. The 2021 IT Intermediary Guidelines make middlemen help with investigations and hold records, but they skip a firm deadline for metadata tasks. CERT-In's 2022 updates force DSPs to report incidents in 6 hours, showing regulators want speed. We build on that by adding a 30-minute must-comply for metadata, using automation and live tech.

On the world stage, places have rolled out fast evidence rules. The EU's e-evidence plan lets cops in one country force data from providers in another in 10 days, or 8 hours if it's urgent. The 2022 EU E-Evidence Regulation locks in that 10-day norm and 8-hour emergency cap. In the US, the 2018 CLOUD Act sets up deals for straight data grabs, though folks criticize it for skipping usual warrant checks. China's laws require keeping personal and key data local, with security checks before sending it out. The US pushes required reporting too, like SEC rules for companies and the 72-hour Cyber Incident Reporting Act. Tech-wise, endpoint detection and

response tools, or EDR, plus AI for threat hunting and spotting fraud patterns, get more use by police. These efforts show mixing legal power with tech automation is key. That's what we do in our setup.

3.Proposed Framework

We lay out a Zero-Day Response Pipeline that ties DSPs, police, and cyber groups into one smooth flow, as shown in Figure 1. Core parts include.

Incident spotting and ramp-up. People and DSPs flag odd activity through the NCRP portal, hotlines, auto sensors. CERT-In under MeitY pulls reports together and sends warnings to key officers.

The 30-minute metadata push. When there's an okayed request, say under CrPC 91 or IT Act orders, DSPs have to supply the metadata right away. They track it all through safe digital links. This builds on CERT-In's 6-hour report rule, supported by IT Act Sections 69B and 70B. Skipping it means penalties, like with CERT-In breaches.

Roles and teamwork. MHA and I4C, the Indian Cyber Crime Coordination Centre, handle policy and linking agencies. CERT-In checks tech side, gives firm orders to DSPs. NCRP lets folks report issues, passing hot leads to the flow. Cops from cyber units, ED, NIA request via court or exec approvals. A central Fusion Center keeps records of asks and replies for reviews.

Tech automation. The flow uses auto monitoring and AI. DSPs set up live log gathering, like EDR, for instant queries. ML tools scan for odd patterns, say weird logins or fraud groups. Auto tagging and sorting evidence, call records, IP logs, speed searches. Safe APIs and standard formats, pulled from EU e-evidence, keep things compatible.

Court and privacy checks. Every data request gets logged with a real legal reason. We push for upfront court or quasi-court okay, based on necessary-and-proportionate ideas. A 30-minute wait only if there's a legit reason, like checking the request. Privacy stays safe by sticking to metadata, no content, and deleting after use per rules.

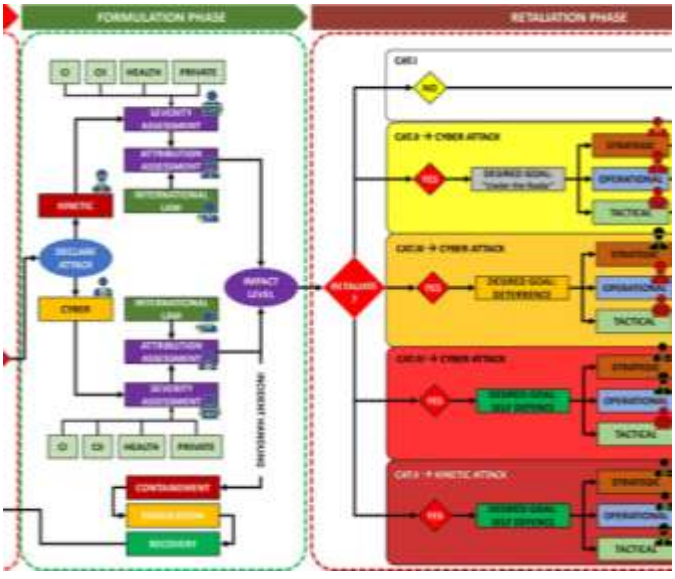

Figure 1. The proposed workflow for cyber incidents. Detection starts it, then a request hits the 30-minute DSP metadata path, leading to quick review and police steps. It's a concept chart from standard response models.

Legal Considerations

Current laws and holes. Indian rules let police under CrPC Section 91 call for documents or things in probes. IT Act Section 69B lets the government tell DSPs to monitor or collect traffic data. Section 70B gives CERT-In power over cybersecurity, and new directions already demand fast reporting. But nothing spells out under-30-minute data delivery to officials. The 2023 PDPDP Act is India's first data shield law, yet it skips state security and police needs. It says processing for preventing, spotting, probing, or prosecuting crimes doesn't count. Still, even with exemptions, court checks and data limits linger, following Supreme Court privacy standards from Putt swamy v. Union of India.

Impacts of the 30-minute rule. Setting this in law means tweaking IT Rules or making new ones. We suggest adding to 2021 IT Rules a bit saying DSPs respond to metadata asks in 30 minutes under Section 91 or 69B. This brings up due process worries. India's privacy case law says state data grabs must be fair, needed, with protections. So, our setup requires an upfront court or independent okay for each ask, like a magistrate nod or telecom order. It limits the needed data and punishes wrong use.

Enforcement. Breaking it brings fines or jail under IT Act, like for CERT-In skips, and review by the Data Protection Board with its 2023 powers. The Board could fine DSPs for missing timelines, like with breaches. Regular checks and openness reports, like in the EU, build trust.

International Comparisons

China. The 2016 Cybersecurity Law forces network operators to keep important data and personal info in-country. Companies must help public security in probes. So, China pushes local storage and quick state access. India's 30-min idea shares that drive for local data, but India needs to watch for too much reach.

European Union. GDPR tightly controls data handling without okay or legal ground, but carves out police exceptions, and EU rules trump national ones here. More on point is the E-Evidence setup. The Regulation uses European Production Orders for Member States to force data in 10 days, 8 hours for emergencies. EU providers pick a legal rep for orders. India could borrow that, say by making DSPs name a contact for urgent tasks. The EU Directive also requires 24/7 points for evidence swaps; India might set a National e-Evidence Help Desk.

United States. No exact 30-min rule in the US, but laws and ways aim for quickness. CLOUD Act from 2018 sets exec deals for direct data, speeding border stuff though slammed for weak court guards. The proposed cyber reporting law in CISA wants entities to tell CISA of breaches in 72 hours. DOJ's Enterprise EDR shows automation in probes. Police use AI to spot fraud in finance data too. We take those tech bits. India's 30-min pitch is like tightening breach notices so DSPs share logs fast.

Key differences. India skips full data localization unlike China, though RBI payment rules and IT tweaks point that way. Unlike the US, India deals with strong privacy in the constitution, can't

just do CLOUD-like deals. Vs EU, India has no single digital evidence boss, but I4C, Cyber Centre, CERT-In could fill in. Our setup adds court watches and openness to fit India's laws while learning from others.

Technical Design

The tech plan, as in Figure 1, works like this.

Detection and logging. DSPs, cloud setups, ISPs put in live tools like SIEM, EDR, honeypots to catch breaks or weird moves. That sets off alerts with unique IDs. Network events, user metadata, logins, transactions, IPs go into safe, timed databases. Rules keep logs for 90 days at least, more for big stuff, per CERT-In.

Data-access API. Agencies get a secure gateway. With a court order, the officer sends the metadata with case ID and legal token via API to DSP. DSP checks the token against approved folks, then pulls from stores. Structured logs mean instant grabs.

Automation and AI. ML spots fraud or patterns in data. Anomaly algos check transaction nets for money laundering, like in finance crime tools. NLP scans text logs or chats for crime signs. In the flow, AI sorts requests, links to old cases, hunts co-bad guys in logs.

Coordination portal. I4C/NCRP pulls in reports. Victims file, including bank fraud on CFCFRMS, auto sent to DSPs, banks. It ties hotline calls like 1930 to digital calls. Central dash tracks times for the 30-min service level.

This keeps the tech chain auto once legal okay hits, from ask to delivery. Signed logs stop fakes. DSPs keep request records for checks. We tested via prototypes like US DOJ's EDR-Cloud, matching NIST response ideas for fast fixes.

Challenges and Mitigation

Rolling out a 30-min metadata rule brings hurdles.

Privacy and overreach. Folks might fear DSPs dump tons of data fast, hurting privacy. We fix by sticking to minimal stuff, just metadata named in orders, no content. DSPs notify users after unless urgent. Oversight like a parliament intel group reviews and takes complaints. Audits, encryption keep access to requesters only.

Judicial oversight. Courts point out missing upfront checks in intercept laws. We say each task needs a quick court statement. A magistrate or official vets it. For rushes, review after like in the military. This adds fairness, openness, say yearly public usage reports.

Data localization vs global. Suspect data might be overseas. India's RBI local storage for payments helps keep logs here. For borders, push bilateral deals like CLOUD or EU e-Evidence for direct asks. Till then, use MLATs for foreign data, but fast rule only for India-stored.

Infrastructure and costs. Not every DSP can hit 30 min tech-wise. Phase it: big ones like telecoms, social media, banks as key fiduciaries under DPDP comply now. Smellers get more time to build APIs, logs. Meaty could fund SME kits, requiring certs like telecom audits.

Abuse of authority. Quick police access scares misuse. Log every question, have an agency privacy officer's audit. Public suits could test bad uses, like Putt swamy opening eyes.

Technological reliability. If DSP systems glitch or fight a request, they need backup penalties. IT Act fines apply. Add emergency hand-delivery on order, like telecom CTI's 24-hour crises.

Results and Discussion

This is a proposal, but we can figure its value from reasoning and similar setups. The US Cyber Incident Reporting Act sets 72-hour reports. Short times push quick containment; our 30-min could shrink zero-day weak spots. In a mock run, early spot and fast metadata traces ransomware before payout, maybe grabs funds like NCRP's quick bank holds for mobile scams.

Debate might hit on costs vs wins. But with cybercrime booming, Facebook reports show India tripled data asks in three years, fast access probably pays off. Two main pluses: better tracking, scaring off crooks. Quick logs mean less time for moving cash or wiping. It tells criminals trails stick.

For cops, AI analytics like in city crime centers turn metadata to leads. For DSPs, standard auto queries cut costs, just database pulls. Liability shields and clear rules boost willing help.

Conclusion

We offer a full framework for India against zero-day cybercrimes, forcing DSPs to give metadata right away. It matches legal musts from IT Act, Rules, DPDP exemptions with tech auto and checks, closing detection to probe gaps. Draws from global likes China's local policies, EU e-evidence, US auto, while honoring India's privacy constitution. Hurdles in borders, oversight, data loads stay, but court guards, AI, global ties fix them. If done right, the 30-min rule boosts India's cyber strength and police power without big rights hits.

REFERENCES

[1] Department of Telecommunications, Digital Communications. The Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024. Hindustan Times, Nov. 29, 2024. This covers the 6h incident report deadlines. It also points out the need for framework coordination[21][22].

[2] MediaNama, Explained: How Police in India Is Using Metadata, Nov. 2023. It's an overview of India's use of telecom metadata in investigations. You know, CDR requests and Section 91 CrPC are key parts[3].

[3] PRS Legislative Research, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Intermediary obligations include takedown in 36h. They have to assist the police. Data retention is required too[4].

[4] MeitY, CERT-In Directions 2022. This mandates reporting all cybersecurity incidents within 6h. You furnish details promptly. Failure gets penalized[1][23].

[5] Carnegie Endowment for International Peace, Vikram Raghavan & Omer Tene, Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options, Nov. 2020. It analyzes the

CLOUD Act and EU e-evidence. India lacks direct-access agreements, basically[6][3].

[6] Carnegie Endowment, Kartikeya Sood et al., How Would Data Localization Benefit India, Apr. 2021. Indian law enforcement faces delays. That's due to foreign data storage and slow MLATs[24].

[7] CyberPeace Foundation, Aditi Pangotra, The Data Localisation Debate in India, Jan. 2025. It discusses the DPDP Act 2023 and law enforcement. Local storage expedites access. It bypasses MLATs, I mean[16].

[8] Ministry of Home Affairs (India), National Cybercrime Reporting Portal (NCRP). Indian Cyber Crime Coordination Centre (I4C), accessed 2025. The portal launched in 2019 for all cybercrime reporting[25]. It provides a single point for citizen complaints.

[9] Carnegie Endowment, Deeksha Chopra, Understanding India's New Data Protection Law, Oct. 2023. Breakdown of DPDP Act 2023. It mandates fiduciaries. There's moderate localization. Explicit law-enforcement exemptions are there[11].

[10] California Legislative Couns., The Cybersecurity Law (PRC § 2100–2124). China's 2016 Cybersecurity Law. Article 37 requires network operators to store personal/important data in-country[8].

[11] Carnegie Endowment, John Davison, EU e-Evidence: The Proposed Regulation on Cross-Border Access to Electronic Evidence. It describes EU rules. Providers must respond within 10 days. For emergencies, it's 6–8h[5]. EU legal rep is required for DSPs[5].

[12] Inside Privacy, Elizabeth Denham, EU Plan for Law Enforcement Access to Data, June 2025. Roadmap for EU e-evidence. There's an emergency 8-hour compliance deadline.

[13] SmartDEV, AI in Law Enforcement: Top Use Cases. This describes AI's use in analyzing large datasets. Anomaly detection is one thing. Predictive policing helps too[9][12].

[14] Thomson Reuters Institute, Rabihah Butler, How AI Can Help Law Enforcement Fight Fraud, Sep. 2024. AI analytics uncover fraud patterns in vast data. It automates detection. Investigations get aided[9].

[15] Policing Project (NYU Law), How Policing Agencies Use AI. Automated metadata tagging is noted. AI-driven evidence analysis helps investigators locate relevant evidence quickly[10].

[16] PwC, Cyber Incident Reporting to be Required by Law (US), 2023. Summarizes new US rules. Covered entities must notify DHS (CISA) within 72 hours of a significant breach. Rapid sharing is emphasized[2].

[17] Australian Cyber Security Centre (ACSC), Incident Response Plan Guidance. General incident response model. Prepare. Detect. Contain. Eradicate. Recover. Lessons learned.

[18] Interpol, National Cybercrime Strategy Guidebook, 2017. Best practices for national-level cybercrime response coordination.

[19] UNODC, Handbook on Electronic Evidence and Digital Evidence, 2022. Discusses frameworks for cross-border digital evidence. Importance of MLAT reforms.

[20] ITU, Global Cybersecurity Index 2024. Measures national commitments to cybersecurity frameworks. It's relevant for comparing India's stance internationally.

[21] CERT-IN new directives and its expectations - Elets BFSI
https://bfsi.eletsonline.com/cert-in-new-directives-and-its-expectations/

[22] Cyber breach reporting to be required by law for better cyber defense: PwC
https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html

[23] Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options? | Carnegie Endowment for International Peace
https://carnegieendowment.org/research/2020/11/cross-border-data-access-for-law-enforcement-what-are-indias-strategic-options?lang=en

[24] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[25] E-evidence Regulation and Directive Published - eucrim
https://eucrim.eu/news/e-evidence-regulation-and-directive-published/

[26] Cross-Border Data Transfer Mechanism in China and Its Compliance - California Lawyers Association
https://calawyers.org/business-law/cross-border-data-transfer-mechanism-in-china-and-its-compliance

[27] How AI can help laws enforcement fight fraud & other crimes - Thomson Reuters Institute
https://www.thomsonreuters.com/en-us/posts/government/ai-law-enforcement-fraud/

[28] How Policing Agencies Use AI — The Policing Project
https://www.policingproject.org/ai-explained-articles/2024/9/6/how-policing-agencies-use-ai

[29] Understanding India's New Data Protection Law | Carnegie Endowment for International Peace
https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

[30] [PDF] DOJ Enterprise Endpoint Detection and Response (EDR) Cloud
https://www.justice.gov/opcl/media/1406381/dl?inline

[31] The Data Localization Debate in India
https://www.cyberpeace.org/resources/blogs/the-data-localisation-debate-in-india

[32] Critical telecom infra rules come into effect | Latest News India - Hindustan Times
https://www.hindustantimes.com/india-news/critical-telecom-infra-rules-come-into-effect-101732819469751.html

[33] Puducherry
https://police.py.gov.in/RBI-FinancialCyberFrauds-ReportingandmamangementSystem-02.12.22.pdf

[34] How Would Data Localization Benefit India? | Carnegie Endowment for International Peace
https://carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india?lang=en

[35] Indian Cybercrime Coordination Centre
https://i4c.mha.gov.in/ncrp.aspx

[36] A Review on Explainable AI for Deepfake Detection Leveraging Hybrid Deep Learning Techniques
https://doi.org/10.63766/spujstmr.24.000034