iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75129

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

Global Threat Intelligence Network to Collect and Display Terrorist Profiles at a Single Platform

Bhavya Sharma[1], Abhinand T[2], Kalidindi Sowmya[3]
SSET, Sharda University, Greater Noida

Abstract: ***This project presents the development of a centralized, web-based platform titled Global Terrorism Database, aimed at compiling and providing comprehensive information on known terrorists across the world. The website serves as a unified intelligence interface where verified data—including names, photographs, affiliations, criminal history, and bounty details—are organized and made accessible to both security agencies and the general public. A key feature of the platform is its public reporting system, which allows individuals to submit tips, sightings, or relevant information regarding the listed terrorists. These reports are securely forwarded to concerned law enforcement or intelligence agencies. In cases where a reward is officially declared for information on a particular terrorist, the platform enables a transparent system for informers to claim such incentives, creating a mutual benefit model for both agencies and civilians. By reducing duplication of effort across nations and encouraging crowd-sourced intelligence, the website seeks to support global counter-terrorism initiatives through better coordination, public participation, and rapid information exchange. This project integrates technology with security efforts, offering an innovative tool in the fight against terrorism.***

Keywords: Terrorism, Intelligence, Cyber-Security, NIA, FBI, InterPol

I. INTRODUCTION

In an era marked by transnational extremism and decentralized terror networks, timely access to credible information on known terrorists has become both a strategic necessity and a global security imperative. Despite the existence of various institutional watchlists and classified intelligence systems, a significant void remains in the public-accessible domain—especially concerning centralized, real-time information dissemination and public cooperation. Bridging this gap is critical for strengthening counter-terrorism frameworks through collective vigilance and actionable civilian participation.

The Global Threat Intelligence Network (GTIN) is conceptualized as a web-based intelligence platform that consolidates detailed profiles of globally wanted terrorists. It offers a structured interface where users can access high-value data such as name, aliases, organizational affiliation, criminal charges, last known location, and bounty information—all in one centralized location. Designed to simulate the aesthetic and functionality of a real-world intelligence dashboard, the system incorporates search, filtering, and partial access control mechanisms to model real agency workflows. One of the defining features of this platform is its public reporting mechanism, allowing citizens to submit sighting reports or intelligence leads. In return, they may claim official rewards (where applicable), thereby creating a mutually beneficial exchange between the public and national security agencies. Although currently implemented as a front-end prototype with static data, the platform is structurally scalable to integrate backend databases, authentication layers, geo-tagging APIs, and automated verification pipelines. This project merges principles from cybersecurity, civic intelligence, and web systems design, offering a conceptual foundation for future real-world deployment. It represents a step toward a more open yet secure model of threat intelligence—where governments and citizens collaborate digitally to confront the evolving landscape of terrorism.

II. LITERATURE REVIEW

The study of terrorism from a systems and information science perspective has evolved significantly over the past two decades, particularly with the proliferation of digital infrastructures for intelligence management. Existing research underscores the necessity for centralized, interoperable databases capable of aggregating and disseminating threat-related information across jurisdictions and user groups (Feldman & O'Leary, 2011).

Global Terrorism Database (GTD) maintained by START at the University of Maryland. GTD is widely cited in academic and policy-oriented literature and provides incident-level data on terrorist activities dating back to 1970 (START, 2023). However, the GTD is primarily designed for retrospective research and lacks interactive, real-time capabilities or support for individual terrorist profiling and public reporting. This limitation creates a disconnect between scholarly databases and operational counter-terrorism needs.

FBI's Most Wanted Terrorists List and INTERPOL's Red Notices focus on individual profiles but are regionally constrained, non-interactive, and largely inaccessible to external agencies or the general public (FBI, 2023; INTERPOL, 2023). Moreover, there is little to no integration with crowd-sourced intelligence—a growing domain of interest in intelligence studies.

According to Schmid (2011), the success of modern counter-terrorism operations increasingly depends on horizontal information sharing and multi-actor participation, including the engagement of civilians. This is supported by empirical studies that highlight the role of open-source intelligence (OSINT) in threat detection and mitigation (Weimann, 2016; Zegart, 2022). Despite this, most public platforms either lack formalized reporting mechanisms or fail to integrate user-submitted intelligence into structured verification workflows.

From a technological standpoint, the use of web-based interfaces for public safety and intelligence reporting has been implemented in localized crime tracking systems, such as India's Crime and Criminal Tracking Network and Systems (CCTNS). These systems demonstrate the feasibility of public-facing platforms but are typically limited in scope, lacking global reach or integration with international watchlists (MHA, 2022).

Jain and Sharma (2019) argue that while crowd-sourced security systems are theoretically beneficial, they require robust moderation, authentication protocols, and legal frameworks to avoid misuse. Similarly, Bjelopera (2013) emphasizes the need for digital counter-terrorism tools to balance public access with national security imperatives.

Emerging studies on machine learning in terrorism detection show promise in clustering behavioral patterns, identifying communication networks, and flagging anomalous reports from public sources (Feldman & O'Leary, 2011). These findings align with the proposed future extensions of the Global Threat Intelligence Network, which aims to integrate AI modules for report validation and threat analysis.

In summary, the current literature reflects a fragmented ecosystem where data is abundant but operationally siloed. While individual systems offer incident tracking or suspect profiling, there is a noticeable absence of integrated platforms that combine open-access intelligence, real-time reporting, and reward-based civilian engagement. The proposed system directly addresses this gap by offering a prototype that consolidates global terrorist profiles and facilitates public reporting through a secure, extensible digital framework.

III. IMPLEMENTATION

The platform has been implemented as a client-side static web application, optimized for responsiveness and modularity. Below is a breakdown of core functional modules:

A. Search Engine

The platform supports case-insensitive, substring-matching search functionality. It parses user input and dynamically highlights or renders cards that match either names, aliases, or organizational tags. The logic is implemented using JavaScript array traversal and basic string-matching algorithms.

B. Filter Module

Each card is assigned category tags such as INDIA, INTERPOL, or MOST WANTED. Clicking these tags triggers a filter function that toggles the display of cards with matching classifications. This logic is modular and can be extended to handle multiple tag combinations.

C. Profile Rendering

Each terrorist profile is rendered as a card containing:

1) A headshot or silhouette
2) Full name and aliases
3) Organization or group affiliation
4) Criminal record or known charges
5) Location of last sighting
6) Reward amount (if any)

"CLASSIFIED" profiles are masked using CSS overlays and color cues to represent redacted information.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

D. Simulated Intelligence Features

The interface includes buttons and elements such as “Analyze” and “Access Level: Top Secret” to simulate future features like:

1) Threat clustering algorithms
2) Geo-mapping of sightings
3) Authentication-based data unlock

These components act as functional placeholders and can be activated once backend systems and AI models are integrated.

IV. RESULT DISCUSSION

The *Global Threat Intelligence Network (GTIN)* project successfully delivers a functional web prototype that consolidates global terrorist profiles into a centralized, searchable, and user-friendly interface. The platform enables keyword-based searches and tag-specific filtering, allowing users to efficiently navigate detailed profile cards containing essential information such as name, affiliation, known charges, location, and bounty status. The system also simulates access control via “CLASSIFIED” overlays, reflecting real-world data privilege mechanisms. While the current version operates entirely on the front end with static data, its architecture is modular and scalable, laying the groundwork for future backend integration, authentication systems, and secure civilian reporting mechanisms. A key innovation is the inclusion of a reward-based public reporting model, encouraging civilian participation in intelligence workflows—an approach that enhances both agency efficiency and public engagement. Although features such as real-time verification, dynamic data fetching, and AI-based threat analytics remain conceptual, the results affirm the technical feasibility and societal relevance of such a platform. Overall, GTIN demonstrates how digital infrastructure can bridge the gap between public access and national security in a controlled and extensible manner.

In terms of interpretative insights, the outcomes of the prototype lead to several observations regarding design feasibility, practical scope, and real-world applicability:

1) Centralized Intelligence Access: The GTIN system provides a unified platform for aggregating data that would traditionally remain siloed across multiple agency portals. Existing systems such as the FBI Most Wanted List or INTERPOL Red Notices are individually useful but do not offer a unified interface or interactive search and reporting functionalities. GTIN demonstrates that such centralization is not only achievable but also scalable with proper backend integration.
2) Public Engagement and Civilian Intelligence Channels: A central innovation in this project lies in the proposed model for crowdsourced intelligence. The platform’s conceptual infrastructure supports user-submitted reports, which can be tied to bounty systems for verified sightings. This creates a two-way communication channel between state institutions and the public—an area often overlooked in conventional counter-terrorism infrastructure. Though this component remains non-functional in the current prototype, its inclusion demonstrates readiness for future implementation of user form modules and reporting validation pipelines.
3) Information Security and Access Simulation: The use of visual redaction mechanisms (e.g., "CLASSIFIED" overlays) offers an intuitive model for conditional content access. While actual authentication systems are not yet implemented, the interface anticipates user-specific privilege differentiation, which is critical in any system handling sensitive national security data. This simulation of controlled access further reinforces the realism and deploying ability of the proposed system in secure environments.
4) Limitations and Present Constraints: Despite its successful interface functionality, the current system is limited in several respects. The most significant limitation is its reliance on static content; all terrorist profiles are hard-coded in the HTML layer with no support for backend operations. Additionally, the platform lacks encryption, session management, and formal input verification mechanisms—all of which are essential for field deployment. Moreover, the AI-assisted threat clustering, geospatial mapping, and evidence upload capabilities remain conceptual at this stage.
5) Forward Compatibility and Technical Extensibility: Importantly, the structural codebase and component hierarchy are conducive to future upgrades. The interface logic is cleanly separated from content, allowing seamless integration with RESTful APIs, NoSQL or SQL-based data stores, and cloud-based authentication services. The placeholder features, such as “Analyze” and “Report Sighting” modules, have been intentionally included as extension points for future iterations of the platform.

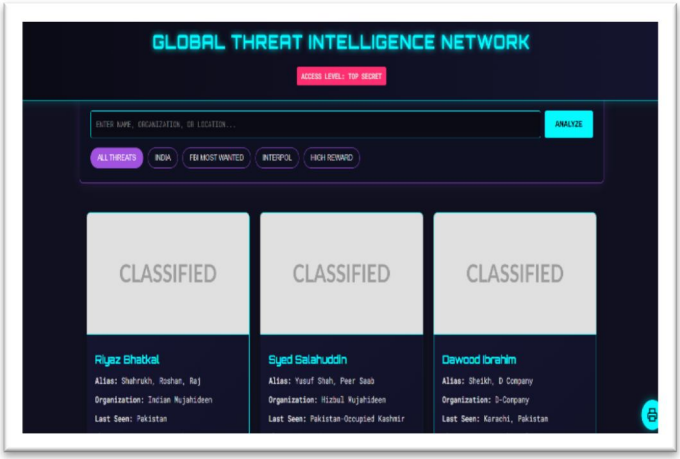


Fig. 1 Terrorist's profile filtered region wise

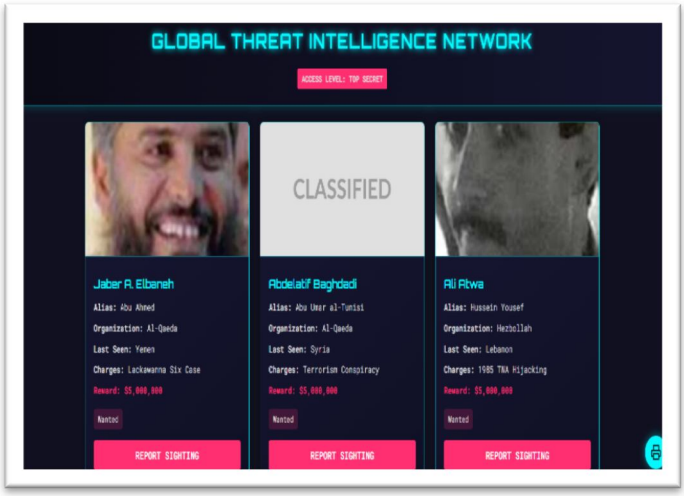


Fig. 2 Terrorist and their profile

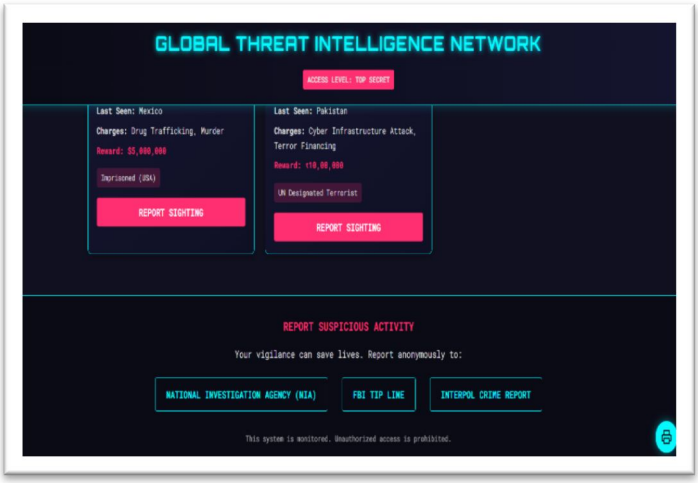


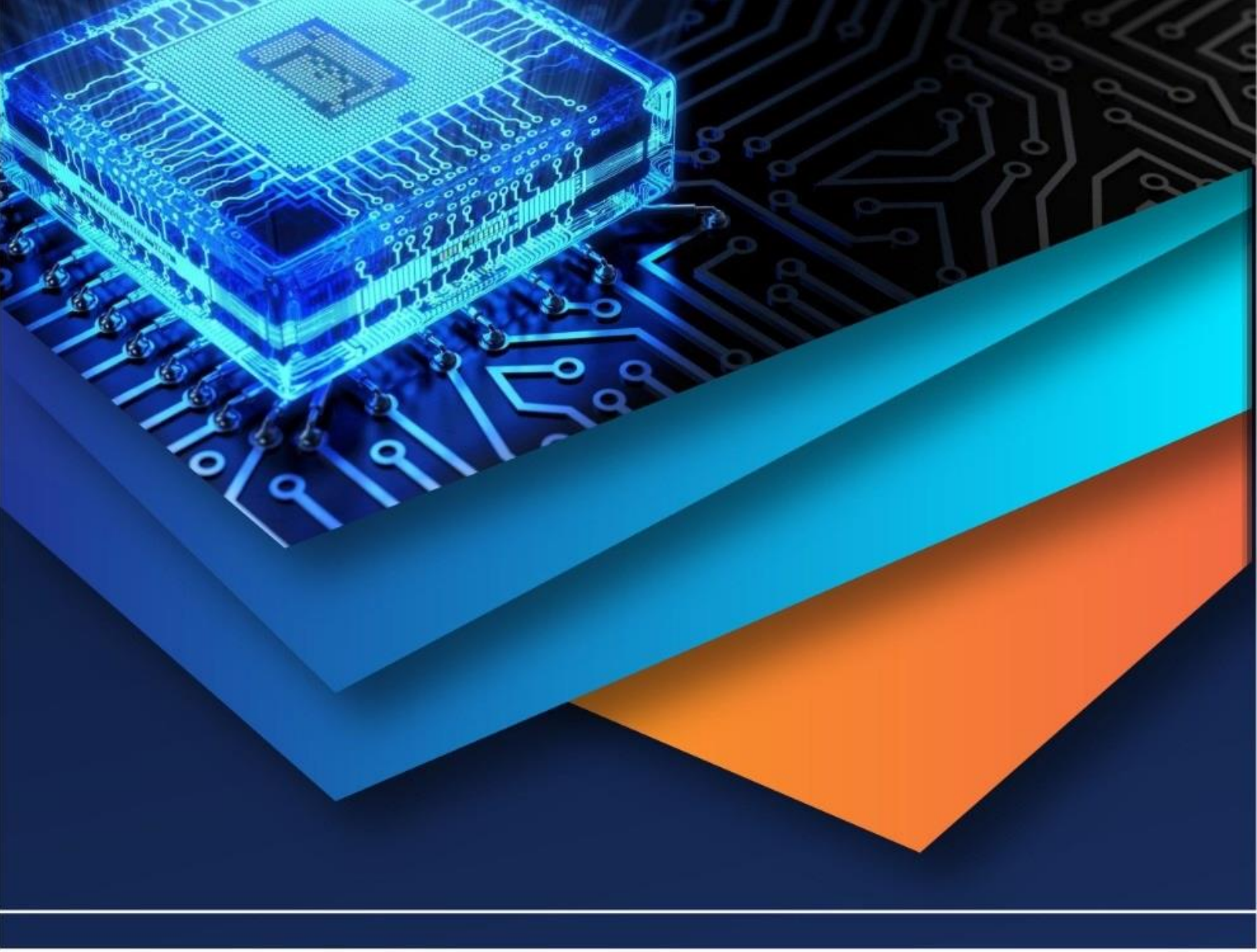
Fig. 3 Sightings can be reported

V. CONCLUSION

The *Global Threat Intelligence Network (GTIN)* represents a forward-thinking approach to digital counter-terrorism infrastructure by consolidating decentralized intelligence into a single, interactive, and civilian-accessible platform. Through the development of a dynamic, searchable interface that simulates real-world intelligence dashboards, the project demonstrates the technical feasibility of integrating public reporting systems with structured terrorist profiling. The design successfully models essential functionalities such as keyword filtering, profile-based visualization, and access-restricted data presentation. While currently implemented as a front-end prototype with static content, the system architecture is purposefully modular—enabling seamless transition to a fully integrated, database-driven, and secure reporting environment. Importantly, the project introduces a participatory intelligence model wherein civilians can contribute information in exchange for potential rewards, fostering a cooperative ecosystem between agencies and the public. In doing so, GTIN addresses existing gaps in transparency, accessibility, and real-time responsiveness found in traditional threat monitoring systems. This work lays the conceptual and technical foundation for future development of scalable, secure, and ethically responsible public-facing counter-terrorism platforms.

REFERENCES

[1] Eldridge, C., Hobbs, C., & Moran, M. (2018). Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'. Intelligence and National Security, 33(3), 391-406.
[2] Chaudhary, M., & Bansal, D. (2022). Open source intelligence extraction for terrorism-related information: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(5), e1473.
[3] Weimann, G. (2015). Terrorism in cyberspace: The next generation. Columbia University Press.
[4] Hatfield, J. M. (2024). There is no such thing as open source intelligence. International journal of intelligence and CounterIntelligence, 37(2), 397-418.
[5] Mashechkin, I. V., Petrovskiy, M. I., Tsarev, D. V., & Chikunov, M. N. (2019). Machine learning methods for detecting and monitoring extremist information on the internet. Programming and Computer Software, 45(3), 99-115.
[6] Huamaní, E. L., Alva, M. A., & Roman-Gonzalez, A. (2020). Machine learning techniques to visualize and predict terrorist attacks worldwide using the global terrorism database. International Journal of Advanced Computer Science and Applications, 11(4).
[7] Baby, A., & Sruthi, A. (2023, November). Machine learning models for prediction of terrorist attacks: A comparative analysis in terrorism prone regions. In 2023 Annual international conference on emerging research areas: International conference on intelligent systems (AICERA/ICIS) (pp. 1-6). IEEE.
[8] LaFree, G., & Gill, P. (2024). Strengths and weaknesses of open source data for studying terrorism and political radicalization. Studies in Conflict & Terrorism, 1-17.
[9] Renard, T., & Demuynck, M. (2025). Migration-related Terrorism: Trends, Challenges, and Policy Implications.
[10] Index, G. T. (2020). Global Terrorism Index: Measuring the impact of terrorism. Institute for Economics and Peace. Retrieved June, 29, 2022.
[11] Chen, H., Reid, E., Sinai, J., Silke, A., & Ganor, B. (Eds.). (2008). Terrorism informatics: Knowledge management and data mining for homeland security (Vol. 18). Springer Science & Business Media.
[12] Chaudhary, M., Vashistha, S., & Bansal, D. (2022). Automated detection of anti-national textual response to terroristic events on online media. Cybernetics and Systems, 53(8), 702-715.
[13] Iliou, C., Tsikrika, T., Vrochidis, S., & Kompatsiaris, Y. (2017, February). Evasive focused crawling by exploiting human browsing behaviour: a study on terrorism-related content. In Proceedings of the 1st International Workshop on Cyber Deviance Detection co-located with the Tenth International Conference on Web Search and Data Mining CyberDD@ WSDM.
[14] Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. Big Data and Cognitive Computing, 8(8), 91.
[15] Conway, M., Jarvis, L., & Lehane, O. (Eds.). (2017). Terrorists' use of the Internet: Assessment and response (Vol. 136). Ios Press.
[16] Tinnes, J. (2024). Risk Assessment of Terrorism. Perspectives on Terrorism, 18(1), 144-207.
[17] Pai, Y., & Krishna Prasad, K. Open Source Intelligence and its Applications in Next Generation Cyber Security-A.
[18] Bjelopera, J. P. (2013). American jihadist terrorism: Combating a complex threat. DIANE Publishing.
[19] Singh, A. K., Ashok/Ali Siddiqui Kumar Singh (Zeesha), & Singh, S. (2024). Recent advances in computational intelligence and cyber security.3



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY