ABOUT TECHNOLOGY

CENTRAL TRAINING COLLEGE

TELECOM & INFORMATION TECHNOLOGY



AI IN MAHA KUMBH

LET'S TALK ABOUT THE FUTURE...

February 2025

ctcit@crpf.gov.in @ctctitranchi CTC(T&IT)_CRPF_RANCHI ctctitcrpfranchi

INDEX

Chief Patron

Sh. Harjinder Singh, DIGP,Principal

Editorial Advisory Board cum R&D Team Chairman

Sh. Brijish Kumar Dubey, Dy. Comdt,Vice Principle

Members

Sh. Aman Deep , Dy. Comdt.
Insp/C Praveen Sagar
Insp/T Harish Prasad
Insp/RO Ramdas K B
Insp/T Biju S T
Insp/RO N.Anil
SI/T Virender Bisht
ASI/T Saneesh S
ASI/Ro Satender Singh Suhag
HC/RO Pradeep Kumar Singh

Editor

Smt. Gauri Singh, Asst. Comdt
Sh. Vinod Kumar Choudhary, Asst. Comdt

Proof Reader

Insp/T R.A. Mishra
Insp/RO Vijay Kumar Sharma

Designing & Layout

SI/T Rajesh Kumar Rajput
ASI/T Deepak

Photography Preceis Cell

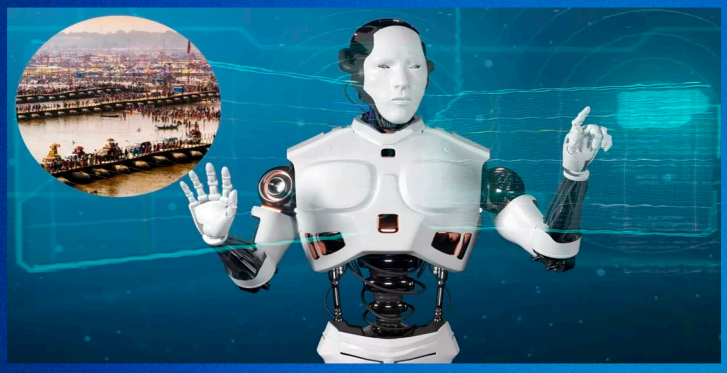
Contents

1. AI CHANGING THE KUMBH MELA
2. NEW CYBER THREATS 2025

Published by:-
CTC(T&IT),RANCHI

AI Changing the Kumbh Mela Experience

Attracting millions of pilgrims looking for spiritual comfort, Kumbh Mela is the biggest religious assemblage in the planet. Organizing an event of size where human traffic, logistics, security, and services call for careful coordination is an amazing difficulty. Artificial Intelligence (AI) here helps to revolutionize the conventional methods of planning and running the Kumbh Mela into a more seamless, safe, and efficient experience for pilgrims and organisers alike



How artificial intelligence is being used in Kumbh Mela to tackle difficult chores such crowd management, public safety, logistics, healthcare, and customized pilgrim services. This is one of the best examples of Goverment Technical.

Monitoring and crowd control

Managing millions of guests in a small area presents a major difficulty, as crowding increases the danger to security. Real-time crowd analytics and artificial intelligence-driven computer vision technologies are tracking crowd density in several event zones. AI-powered cameras on drones record aerial imagery, which is real-time processed to identify possible congestion areas and support fast response. Advanced heat-mapping technology, for example, enables officials to locate regions where big gatherings of pilgrims are occurring and direct the pilgrim flow, therefore preventing stampedes.



Improving public security

Public safety during the Kumbh Mela depends much on artificial intelligence. Common concern in such big events, missing people are identified using facial recognition technology. By means of collaborations with law enforcement authorities, artificial intelligence technologies connect real-time video feeds with a database of missing persons to enable rapid family reunion. Moreover, predictive analytics-powered artificial intelligence systems can highlight odd activity patterns, enabling security agencies to react early on possible hazards.



Waste Management and Logistics

For millions of people, managing logistics entails supplying basics such food, drink, shelter, and sanitation. By means of demand pattern analysis and guaranteed timely resource distribution among several camps, AI-driven solutions maximize supply chain management. By forecasting waste-generating quantities and streamlining waste-collecting paths, artificial intelligence also helps with waste management. This guarantees better surroundings, thereby supporting the sustainability of the event.

Customized Pilgrim Services

Personalized advice from AI-driven mobile apps gives pilgrims real-time knowledge on paths, ceremonies, and facilities as well as direction. Natural language processing (NLP) driven chatbots answer questions in several regional languages, therefore ensuring that pilgrims from several linguistic backgrounds obtain correct information. Moreover, AI-powered navigation tools enable guests to make their way throughout the large grounds of Kumbh Mela, therefore lowering uncertainty and improving the whole experience.



AI in Healthcare Assistance

Healthcare services have to be strong and responsive given millions of people visiting one location. By means of health surveillance systems analyzing environmental variables and population behavior, artificial intelligence aids by forecasting possible disease outbreaks. AI-powered telemedicine booths provide first diagnoses and treatment recommendations, therefore relieving on-ground medical workers of some of their load. Additionally being used are wearable sensors tracking vital indicators that notify medical staff should an emergency strike

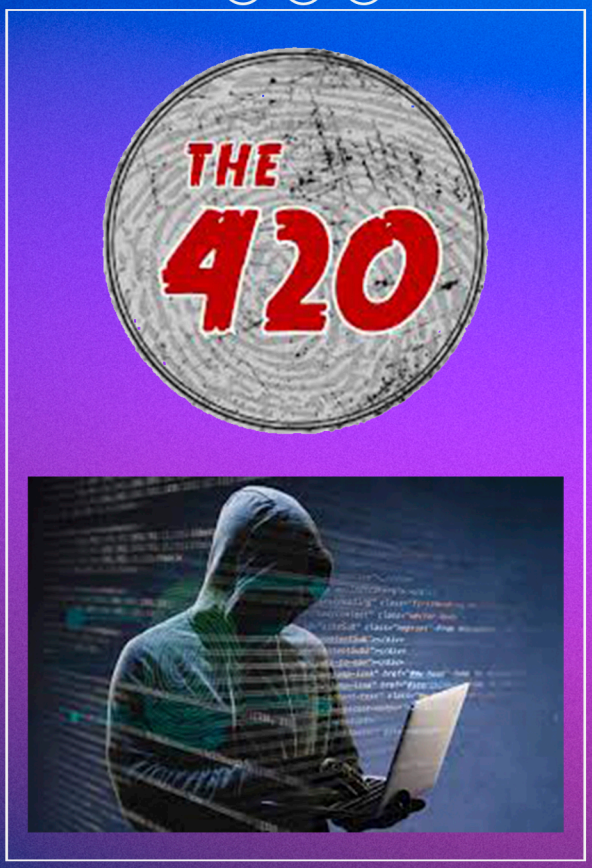


NEW CYBER THREATS 2025

Hackers are actively exploiting outdated versions of WordPress and its plug-ins to compromise thousands of websites, tricking visitors into downloading and installing malware, according to security researchers. The cyberattack, which remains ongoing, was discovered by web security firm c/side. Its founder and CEO, Simon Wijckmans, told TechCrunch on Tuesday that the hackers' objective is to distribute malware capable of stealing passwords and personal data from both Windows and Mac users. Some of the affected sites rank among the most visited on the internet. Security researcher Himanshu Anand, who detailed the findings, described the attack as "spray and pay", meaning it indiscriminately targets any visitor rather than focusing on specific individuals or groups. When a user visits a compromised WordPress site, the page content swiftly changes to display a fake Chrome browser update prompt, urging the visitor to download an update to continue viewing the website. If the visitor accepts, they are prompted to install a malicious file that varies depending on whether they are using Windows or macOS. C/side researchers identified over 10,000 compromised websites. By conducting reverse DNS lookups and crawling malicious domains, they traced several in terconnected sites hosting the attack.

Pakistan-based cybercrime network dismantled by US, Dutch authorities (The Record)

U.S. and Dutch law enforcement agencies have seized dozens of domains linked to a Pakistan-based cybercrime network operated by a group known as Saim Raza. The group, also tracked under the name Heart Sender, has been using these websites since at least 2020 to sell hacking tools — including phishing kits, scam pages and email extractors — to thousands of customers worldwide, according to a statement from the Justice Department. "A cybercriminal can use these tools to send large amounts of spam or phishing emails or to steal someone's login credentials," the Dutch police said, adding that Saim Raza's marketplaces also sold access to compromised infrastructure, including email servers, WordPress accounts, and web hosting control panels such a cPanel. "With stolen cPanel or WordPress accounts, criminals can take control of a website or server's management system," the police warned.



NEW CYBER THREATS 2025

Cyber Criminals Luring Citizens with Aadhaar Update Scams (Kashmir Observer)

With the rise of digital scams and cyber attacks in India, Aadhaar — a government-issued identity document that over a billion people depend on — has become a prime target for cybercriminals. Whether you've seen the notification, "Your Aadhaar needs an update," or received texts offering easy, quick fixes, it's essential to be wary. These scams are increasing, and they leverage the trust people put in official communications. The reality is that these scammers are getting slicker with their approach. If you've been using the internet for long enough, you'll know the good old phishing emails with typos and dodgy links. Now? These cyber fraudsters are upgrading their tactics, creating legit-looking websites, and messages that could fool the most prudent of online users. To keep yourself and your personal data safe, here's what you need to know about Aadhaar update scams, and how to dodge these digital traps

Ransomware attack forces Brit high school to shut doors (THE REGISTER)

A UK high school will have to close for at least two days, today and tomorrow, after becoming the latest public-sector victim of ransomware criminals. Blacon High School in the historic city of Chester, in north west England, said yesterday the attack hit on January 17, and didn't rule out having to shut its doors to students for additional days this week. Students have not been given the day off, however. Teachers set work for them to complete on Google Classroom over the two days, although they can still visit the school to collect lunch. No ransomware crew has claimed responsibility for the attack at the time of writing, and the school is unwilling to comment on whether any data was compromised as a result of the incident. "We have an independent cybersecurity company working in school to understand exactly what has happened," headteacher Rachel Hudson said in a statement. "Until this is completed, I will not be able to provide any further details on any potential data breach." Many of the school's IT systems are down, although Hudson said senior staff are working to create systems that will enable operations to continue



