

(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :06/01/2026

(21) Application No.202641001312 A

(43) Publication Date : 23/01/2026

(54) Title of the invention : Secure Multi-Factor Authentication Using Behavioural Biometrics and Blockchain

(51) International classification	:H04L 9/32, G06F 21/32, H04L 29/06, H04L 9/06, H04L 9/08	(71)Name of Applicant : 1)Sqn Ldr R Giri Address of Applicant :AP(SG), Department of EEE, Hindustan University No 1,Rajiv Gandhi salai, padur, kelambakkam, chengalpet dist. Chennai 603103 Chengalpet Tamilnadu India Tamil Nadu India 2)Dr. P. Kanchanamala 3)Archana Sachin Patil 4)Kandasamy V 5)Suyog Sudam Medhe 6)Manisha Das 7)Dr Annadurai S 8)Dr G Manjula (72)Name of Inventor : 1)Sqn Ldr R Giri 2)Dr. P. Kanchanamala 3)Archana Sachin Patil 4)Kandasamy V 5)Suyog Sudam Medhe 6)Manisha Das 7)Dr Annadurai S 8)Dr G Manjula
(31) Priority Document No	:NA	
(32) Priority Date	:NA	
(33) Name of priority country	:NA	
(86) International Application No	:	
Filing Date	:01/01/1900	
(87) International Publication No	: NA	
(61) Patent of Addition to Application Number	:NA	
Filing Date	:NA	
(62) Divisional to Application Number	:NA	
Filing Date	:NA	

(57) Abstract :

Secure Multi-Factor Authentication Using Behavioural Biometrics and Blockchain Abstract The suggested methodology encompasses a collection of tactics and instruments designed to safeguard user-sensitive information, including passwords, from illegal access, exploitation, or loss. Its objective is to detect unauthorized users, typically attackers who have acquired passwords, attempting to alter the passwords of authorized users. Authentication is critically important to cybersecurity. Nonetheless, the majority of traditional authentication systems operate in a centralized manner, which may lead to issues such as single-point failure, personal information exposure, and the threat of identity theft. Standard verification methods, including passwords and PINs, are very susceptible to phishing, brute-force assaults, and social engineering tactics. This study introduces a novel authentication approach that integrates biometric characteristics with behavioral biometrics to enhance user authentication processes. The immense popularity of technology-driven solutions and innovations for daily procedures has greatly facilitated the rise of smart cities. where millions of interlinked devices and sensors produce and disseminate vast quantities of data. The accessibility and abundance of both personal and public data produced in these digitalized and automated ecosystems make smart cities susceptible to both intrinsic and external security breaches. In the current era of rapidly advancing technologies, traditional login and password methods are insufficient to protect important data and information from hackers.

No. of Pages : 10 No. of Claims : 6