**Paper No: PU-ECE- 04**

**An Efficient Secure Authentication Scheme for Personalized Healthcare System**

Kamalanathan Chandrana, Sunitha Pandab & **Bhaskara Sreenivasc**

a. Department of Electrical, Electronics & Communication Engineering, GITAM School of Technology, GITAM University, Bengaluru 561203

b. Department of Electronics & Communication Engineering, GITAM School of Technology, GITAM University, Bangalore 561203

c. Department of Electronics & Communication Engineering, School of Engineering, Presidency University, Bangalore 560 064

**Abstract**

Health care applications are pondered as propitious fields for wire-less sensor networks (WSN), in which patients can well be monitored utilizing wire-less medical sensor networks (WMSNs). Presently, hospitals are employing applications to admittance physical condition data of the patient. Therefore, the cost for user’s uniqueness executive is increased and also the security protection is decreased. The existent works presented the authentication scheme intended for the healthcare sector, but that’s techniques provides low security. To trounce the existing work loss, here, a proficient secure authentication scheme is proposed intended for personalized healthcare system using WMSN. The proposed method comprises 3 phase. Initially, perform an authentication process which consists of 3 steps, (a) registration, (b) login, (d) verification. Registration and login data are combined using Fisher-Yates Shuffled Algorithm (FYSA), thus the combined data are modified as the hash code utilizing RIPEMD hash code algorithm. Secondly, the file is securely transferred using Modified Elliptic Curve Cryptographic (MECC). Thirdly, scheduling with the cloud using parameters like speed, task cost, weight, memory, Number of the request, data size, bandwidth, along with disk space. Thus, the scheduling parameters are optimized using Modified Grey Wolf Optimization (MGWO) algorithm. Experimental outcomes of the proposed secure authentication scheme are contrasted with the existing authentication scheme centered on the encryption time, decryption time, packet delivery ratio (PDR), End-to-End delay (EED), along with throughput.

**Keywords:**

[Fisher Yates Shuffled Algorithm (FYSA)](https://www.tandfonline.com/keyword/Fisher%2BYates%2BShuffled%2BAlgorithm%2B%28FYSA%29), [RACE Integrity Primitive Evaluation Message Digest (RIPEMD)](https://www.tandfonline.com/keyword/RACE%2BIntegrity%2BPrimitive%2BEvaluation%2BMessage%2BDigest%2B%28RIPEMD%29), [Modified Elliptic Curve Cryptography (MECC)](https://www.tandfonline.com/keyword/Modified%2BElliptic%2BCurve%2BCryptography%2B%28MECC%29), [Modified Grey Wolf Optimization (MGWO)](https://www.tandfonline.com/keyword/Modified%2BGrey%2BWolf%2BOptimization%2B%28MGWO%29), [Wireless Medical Sensor Network (WMSN)](https://www.tandfonline.com/keyword/Wireless%2BMedical%2BSensor%2BNetwork%2B%28WMSN%29)

**Publication Details:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Journal Name** | **Vol.** | **Month & Year**  | **Page No.** | **Publisher** | **Scimago Ranking** |
| Journal of Inter Disciplinary Mathematics | 23(1) |  April, 2020 | 215-227 | Francis & Taylor | Q4 |