International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 48-67

A CRYPTOGRAPHIC AUTHORIZATION MODEL FOR SECURE EHRS IN HEALTHCARE CLOUD INTEGRATING MAC VERIFICATION WITH HASHING METHODS

S. Prathima[1] Dr. R. Durga[2]

[1]Research Scholar, Department of Computer Science, School of Computing Sciences

[2]Associate Professor, Department of Computer Science, School of Computing Sciences

Vels Institute of Technology and Advanced Studies (VISTAS), Chennai, India

Email: prathismanian@gmail.com[1], drrdurgaresearch@gmail.com[2]

ABSTRACT:

In the current era of rapid technological advancement, electronic/digital health records are increasingly used by medical institutions. These electronic health records require a safer cloud to store and process data. Nonetheless, establishing a cloud-based medical data centre comes with hefty construction expenses and specialized technological assistance. Hence, we suggest a cryptographic authorization model using MAC verification and hashing (CAEHRMH). At first, patient registration is done and then the nodes are initialized. After that, the test packet is transmitted to create the authenticated path by calculating the cipher text using CRROT13. Then, the doctor's appointment is booked and the consultation is done. After the successful consultation, parameters are extracted and converted into hash code using DF-ASH512 while the secret key is generated using LDH. With this key, the MAC address is generated using the LDH-TDES-MAC algorithm. Next, the data is converted into encrypted formats at a double time using CREDCC. Then, the doctor will log in with the system and the parameters are extracted and converted into the hash code for generating the MAC address. The MAC address is matched with the patient's MAC address. Upon matching, the doctor downloads the encrypted data and decrypts it. The experimental findings demonstrated that the suggested methodology is significantly more secure than the current methods.

KEYWORDS: *Electronic Health Records (EHRs), Digit Folding-based Algorithm for Secure Hashing (DFASH512), Log Diffie Hellman (LDH), Log Diffie Hellman (LDH) based Triple Data Encryption Standard MAC (LDH-TDES-MAC), Cube Root Edwards Curve Cryptographic (CREDCC).*