Secure and Fast Remote Application–Based Authentication Dragonfly using an LED Algorithm in Smart Buildings

1st Batool Mohammed Radhi
Department of Computer Science
College of Education for Pure Sciences
University of Basrah, Basrah 61004, Iraq
batool.mohammed@uobasrah.edu.iq

2nd Mohammed Abdulridha Hussain
Department of Computer Science
College of Education for Pure Sciences
University of Basrah, Basrah 61004, Iraq
mohammed.abdulridha@uobasrah.edu.iq

3rd Zaid Ameen Abduljabbar
Department of Computer Science
College of Education for Pure Sciences
University of Basrah, Basrah 61004, Iraq
zaid.ameen@uobasrah.edu.iq

4th Vincent Omollo Nyangaresi
Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya
vnyangaresi@joust.ac.ke

2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) | 979-8-3503-4434-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICAIIC60209.2024.10463470

***Abstract*— The proliferation of the internet of things (IoT) has led to the emergence of a wide range of intelligent devices, creating a broad domain with significant security concerns. These concerns impose a high level of security; unfortunately, IoT devices usually have limited resources in terms of little memory, low computing power, and a short battery life. Therefore, IoT application developers must use lightweight cryptographic tools to achieve a trade-off between performance and security. The storage and high computation capacity of cloud computing is often exploited to manage the vast amount of data produced by such gadgets. Some methods still suffer from attacks, and others cannot achieve low complexity. We propose a secure and low-complexity system for smart buildings in transferring data between the local server, the cloud, and users authorized by the owner. The LED encryption algorithm, which is lightweight and requires limited resources and less energy, was used to create a mobile application system characterized by confidentiality, authentication, and privacy. For further security, the owner's biometrics were used and derived as the key to decrypt data from the cloud. We have leveraged Dragonfly authentication technology to transfer data from the local server to the users. The owner can add authorized persons in the cloud database and local server to enjoy using the application. Moreover, we successfully balance security complexity and performance in our work. As a result, we achieve good results with a computation cost of 0.281 s and a communication cost of 1472 *bit*.**

***Keywords*— *authentication, confidentiality, lightweight LED, dragonfly technology, mobile application*.**

I. INTRODUCTION

The internet of things (IoT) grew quickly and is expected to continue growing over the next years. There is projected to be approximately 25 billion connected IoT devices and sensors by 2025 [1]. These devices can move and produce data via a network without the assistance of a human, which is in line with the expectation that IoT devices and their applications will reach and connect every element of our daily lives. These days, a wide range of fields and applications, including smart homes, smart cities, water, electricity, green energy, traffic congestion, waste management, disaster alerting, recycling, agriculture, breeding, and healthcare, have adopted connectivity, cloud computing, and big data analytics due to significant advancements in IoT-enabling technologies [2],[3],[4]. These sensors and devices generate data that may include private or sensitive patient information, such as medical records, photos of people, and license plate numbers from IoT surveillance cameras in checking zones. All of this has made the security and privacy of such data increasingly important. Furthermore, IoT devices must be secured, and their data must be shielded from unwanted access because attackers might leverage any weakness [5],[6]. Thus, robust and enhanced encryption techniques should be considered to safeguard the transfer of sensitive information. In the context of IoT, lightweight cryptographic primitives are advised while considering the trade-off between security assurance and performance [7],[8]. The data many smart devices produce is one of the biggest concerns with IoT. With so many various types of IoT devices producing such a large database store, cloud computing (CC) has emerged as a critical technology for managing it [9],[10].

WPA3, released in June 2018, is the most recent security system, created to improve security on existing Wi-Fi networks and address issues with earlier iterations. It uses WPA3 password-based simultaneous authentication equality (SAE) technology for client authentication. Originally designed for usage in mesh WLANs, the SAE protocol has been modified and shown to deliver the promised protection [11]. This resistance is achieved using a Dragonfly handshake to take advantage of logarithms and a discrete ellipse curved encoder. One of the most basic tasks in the IoT is to protect data transmitted over the local or global network and check who can access the data [12],[13]. In this work, an LED is used to protect data in motion, while Dragonfly protocols are used as a switch for a lightweight LED algorithm. One of its weaknesses is its static key, so by using Dragonfly's technology to authenticate users, we could use it for a single session key [14]. The proposed scheme also has powerful features, such as secure authentication and a lightweight, confidential, and secure algorithm for changing key sessions every time. User privacy is also important. Therefore, we use the owner's biometric key to decrypt the data received from the cloud