ABSTRACT

Today's Internet of Things (IoT) transforms our lives and is witnessed as a prominent part of various communities. It allows the interaction of physical objects, smart vehicles, and buildings by wireless connectivity and enables data exchange among them. As a result, we are surrounded by numerous smart devices. On the contrary, this growing number of devices is exposed to security threats and energy unproductiveness. Providing an energy-efficient secured path remains a greater challenge in such systems. This intended research examines the significance of data protection and energy conservation practices in IoT networks by identifying the limitations in existing mechanisms, including fragmented security, limited processing power, and reduced network scalability. The proposed research presents a holistic approach to enhancing security and energy efficiency in IoT networks. The approach involves the development of comprehensive frameworks that encompass all aspects of security and energy efficiency. Cellular Automata Based Key Management Scheme (CABKMS) comprising Key preloading, shared key establishment, and rekeying is identified as essential steps for achieving security in IoT networks.

A novel local forwarding approach called FPSO-FFSC (Fast Particle Swarm Optimization – Fast Far and Slow Closer) is proposed to improve energy efficiency. The research focuses on a three-layered architecture for IoT networks, where cryptographic keys are loaded into sensors in the device layer. A Time seeded Linear Congruential Generator (T-LCG) generates a random probability value. Next, the interval [0-1] is divided

into equal subintervals; each assigned a CA rule using Interval Partitioning Approach (IPA). The CA rule used in each time step depends on the random value generated during the previous step. The automaton runs for several steps, and a different CA is used at each iteration. By selecting a subset from the cells, the automaton's final state generates the cryptographic keys, which are then loaded into the sensors' memory for secure communication within the IoT. More interestingly, the research incorporates the FPSO-FFSC method to enhance energy efficiency. The energy-intensive task, generating and processing random probabilities for key creation, is performed on nodes located farther from the sink and with greater energy reserves. This optimization helps to avoid energy depletion in nodes closer to the sink, leading to a longer lifespan for the IoT system and increased energy efficiency. Simulation experiments conducted using MATLAB R2022a demonstrate that the residual energy is maximized and transmission delay is significantly reduced compared to other routing optimization approaches.

Furthermore, the proposed research introduces the FFSC-BMO (Fast Far and Slow Closer - Barnacles Mating Optimizer) approach as an optimization technique for IoT networks. The approach builds upon the traditional FPSO algorithm but incorporates an enhanced Barnacles Mating Optimizer from the BSO algorithm. By integrating the Mutated Barnacles Mating Optimizer (MBMO), the FFSC-BMO approach facilitates better solution space exploration, preventing premature convergence to suboptimal solutions and enabling faster convergence to optimal global solutions. The primary goals of the FFSC-BMO approach are to increase the lifespan of IoT networks and accelerate convergence to global optimal solutions, ultimately optimizing energy resource usage and improving energy efficiency and sustainability. The proposed system mainly focuses on comprehensively

analysing a secured energy-efficient path that utilizes the FFSC-BMO approach against existing optimization mechanisms to assess its performance. Simulations are performed, and the results state that the proposed approach provides a better exploration rate and enhanced network lifetime. More significantly, this research offers a cutting-edge strategy by addressing research challenges such as energy efficiency, security, and convergence rate in finding global optimal solutions.