The Rise of Blockchain Internet of Things (BIoT): Secured, Device-to-Device Architecture and Simulation Scenarios

ABSTRACT

Most Internet of Things (IoT) resources are exposed to security risks due to their essential functionality. IoT devices, such as smartphones and tablets, have a limited network, computation, and storage capacity, making them more vulnerable to attacks. In addition, the huge volume of data generated by IoT devices remains an open challenge for existing platforms to process, analyze, and discover underlying trends to create a convenient environment. As a result, to deliver acceptable services, a new solution is necessary to secure data accountability, increase data privacy and accessibility, and extract hidden patterns and usable knowledge. Moving the Internet of Things to a distributed ledger system might be the most effective way to solve these issues. One of the most well-known and extensively utilized distributed ledger systems is the blockchain. Due to its unique properties, such as privacy, accountability, immutability, and anonymity, blockchain technology has recently attracted a lot of interest. Using IoT in conjunction with blockchain technology can bring several benefits. This paper reviews the current state of the art different BIoT architectures, with a focus on current technologies, applications, challenges, and opportunities. The test findings prove that the decentralized authentication platform-based blockchain-based IoT (BIoT) device-to-device architecture has a significantly higher throughput than the gateway-based architecture. To encrypt the elliptical curve cryptographic (ECC) and to generate keys, the Chinese remainder theorem (CRT)-based scheme is proposed and compared with the secure hash algorithm (SHA-256). Finally, ECC-CRT is used to access system performance in terms of latency, throughput, and resource consumption, simulated through the Contiki Cooja (CC) simulator, and alter orderer and peer nodes for performance study in BIoT. A comprehensive analysis and simulation results show that the proposed scheme is secure against a variety of known attacks, including the man-in-the-middle (MiM) attack, and outperforms the SHA-256 cryptographic algorithm. Moreover, the significance of blockchain and IoT, as well as their analysis of proposed architecture, is discussed. This paper will help readers and researchers understand the IoT and its applicability to the real world.