

The growth of Internet of Things (IoT) took center stage universally due their capability to advance the course of human lives. Consequent upon this, several challenges were thrown up such as security of huge data stored and transmitted through network communication channels. IoT insecurity is partly due to centralization architecture, low computational strength, resource constrained devices, variation in standards and protocols of communication. From this Systematic Literature Review (SLR), the 85 articles reviewed showed that privacy and security solutions are still being proposed or at conceptual levels, though a number of researchers favored the integration of Blockchain technology, cryptographic and hashing schemes into IoT. The Blockchain technology in IoT systems remains an open area of interest for top researchers especially in evolving frameworks to fit into the centralized architecture, functionality, and scalability demands of conventional IoT systems. In this article, we investigate security and privacy concerns of IoT from the lens of current trends, pertinent challenges, security methodologies, applications, and gaps for future research directions. Most specifically, there is prospect of utilizing cryptographic and hashing schemes offered by Blockchain technology in IoT. Then, high performance and scalable cryptographic schemes (that is, those in the class of lightweight approach) are suggested to deal with privacy and security of data in Blockchain-based IoT system. More importantly, this study provides basis for evolving secure and decentralized applications and systems in several domains such as smart farming.