**INTRODUCTION**

**T**HE Internet of Things (IOT) has emerged as a technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others [1]. The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy. IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of data.

A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users.

Although simple, the traditional encryption schemes involve complex key management protocols and, hence, are not apt for data sharing. Proxy re-encryption (PRE), a notion first proposed by Blaze *et al.* [2], allows a proxy to transform a file computed under a delegator’s public key into an encryption intended for a delegatee. Let the data owner be the delegator and the data user be the delegate. In such a scheme, the data owner can send encrypted messages to the user temporarily without revealing his secret key. The data owner or a trusted third party generates the re-encryption key. A proxy runs the re-encryption algorithm with the key and revamps the cipher text before sending the new cipher text to the user. An intrinsic trait of a PRE scheme is that the proxy is not fully trusted (it has no idea of the data owner’s secret key). This is seen as a prime candidate for delegating access to encrypted data in a secured manner, which is a crucial component in any data-sharing scenario. In addition, PRE allows for encrypted data in the cloud to be shared to authorized users while maintaining its confidentiality from illegitimate parties. Data disclosures can be minimized through the use of encryption since only users delegated by the data owner can effectively access the outsourced data.

Motivated by this scenario, this article proposes an improvement in IOT data sharing by combining PRE with identity based encryption (IBE), information-centric networking (ICN), and block chain technology. Shamir [3] first presented the notion of IBE, in which a sender encrypts a message to a recipient using the identity (email ) as the public key. It is a very powerful primitive used to combat numerous key distribution problems and has consented to the development of several cryptographic protocols, including public-key searchable encryption [4], [5], secret handshakes [6], and chosen cipher text attack (CCA) secure public-key encryption [7]. IBE is preferred over attribute-based encryption (ABE) because ABE involves heavy computations on data encryption, decryption, and key management, and these processes are not convenient for the resource-constrained IoT devices. The strength of this article is increased by borrowing the idea of ICN to cater for the growth in information sharing.

The appeal for low-latency applications introduced the notion of ICN [8] [11], where data owners can distribute and assign unique names to their data which can be replicated and saved in network caches [12], [13]. This ensures that there is an efficient data delivery and utilization of network bandwidth, which is a prerequisite for the IOT ecosystem regardless of the enormous growth in network volumes. On issues of trust, a decentralized, distributed system that can smoothen secure and trusted data sharing was introduced by Nakamoto [14]. This is the block chain technology, and it has gained much attention due to its ability to preserve data privacy. Although there exist optimization issues when storing vast sizes of data, emerging system applications have used the block chain for access control in database management. Data confidentiality and user revocation can also be achieved using block chain. PRE, together with IBE and the features of ICN and block chain, will enhance security and privacy in data-sharing systems.

PRE and IBE will ensure fine-grained data access control, while the concept of ICN promises a sufficient quality of service in data delivery because the in-network caching provides efficient distribution of data. The block chain is optimized to prevent storage and data-sharing overheads and also to ensure a trusted system among entities on the network. In our article, the data owner propagates an access control list which is stored on the block chain. Only the authorized users are able to access the data. The contributions of this article are summarized as follows.

1) We propose a secure access control framework to realize data confidentiality, and fine grained access to data are achieved. This will also guarantee data owners’ complete control over their data.

2) We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.

3) To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IOT devices and as such provide high performance networking.

4) The security analysis of our scheme is presented, and we also test and compare its performance with existing schemes.

This article is structured as follows. Section II reviews some literature on PRE, IBE, ICN, and block chain for data sharing and access control. Security definitions and preliminaries are formally described in Section III. In Section IV, we define a data-sharing problem and present the system model. The implementation of our model is illustrated in Section V and the formal security analysis is outlined in Section VI. Section VII evaluates and discusses our proposed scheme, while Section VIII concludes the article.