**INTRODUCTION:**

The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security.

**LITERTURE SERVERY:**

**TITLE:** A survey on enabling technologies, protocols, and applications

**AUTHOR:** A. Al-Fuqaha

**Description:** This paper provides a comprehensive study of Federated Learning (FL) with an emphasis on enabling software and hardware platforms, protocols, real-life applications and use-cases. FL can be applicable to multiple domains but applying it to different industries has its own set of obstacles. FL is known as collaborative learning, where algorithm(s) get trained across multiple devices or servers with decentralized data samples without having to exchange the actual data. This approach is radically different from other more established techniques such as getting the data samples uploaded to servers or having data in some form of distributed infrastructure. FL on the other hand generates more robust models without sharing data, leading to privacy-preserved solutions with higher security and access privileges to data. This paper starts by providing an overview of FL.

**TITLE:** Divertible protocols and atomic proxy cryptography,

**AUTHOR:** M. Blaze, G. Bleumer,

**DESCRIPTION:**  we introduce the notion of divertibility as a protocol property as opposed to the existing notion as a language property We give a definition of protocol divertibility that applies to arbitrary party protocols and is compatible with Okamoto and Ohta's definition in the case of interactive zero-knowledge proofs. Other important examples falling under the new definition are blind signature protocols. We propose a sufficiency criterion for divertibility that is satisfied by many existing protocols and which, surprisingly, generalizes to cover several protocols not normally associated with divertibility (e.g., Diffie-Hellman key exchange). Next, we introduce *atomic proxy cryptography*, in which an *atomic proxy function*, in conjunction with a public *proxy key*, converts ciphertexts (messages or signatures) for one key into ciphertexts for another. Proxy keys, once generated, may be made public and proxy functions applied in untrusted environments. We present atomic proxy functions for discrete-log-based encryption, identification, and signature schemes

**TITLE;** “Identity-based cryptosystems and signature schemes

**AUTHOR:** A.sharmic

**DESCRIPTION:**

we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other’s signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period.

**TITLE:** Secret handshakes from pairing-based key agreements,

**AUTHOR:** D. Balfanz

**Description:** Consider a CIA agent who wants to authenticate herself to a server but does not want to reveal her CIA credentials unless the server is a genuine CIA outlet. Consider also that the CIA server does not want to reveal its CIA credentials to anyone but CIA agents - not even to other CIA servers. We first show how pairing-based cryptography can be used to implement such secret handshakes. We then propose a formal definition for secure secret handshakes, and prove that our pairing-based schemes are secure under the Bilinear Diffie-Hellman assumption. Our protocols support role-based group membership authentication, traceability, indistinguishability to eavesdroppers, unbounded collusion resistance, and forward repudiability.