

ABSTRACT

TABLE OF CONTENTS

Personal health records possess the patient's medication details and their health history. The health records attract the attention of the attackers as it possesses invaluable information. Loss of electronic health record leads to a wrong medication or surgery. PHR generally contains highly-sensitive and critical data related to patients, which is frequently shared among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for effective diagnosis and treatment. Key exchange protocols enable two or more parties to establish a shared encryption key that they can use to encrypt or sign data that they plan to exchange. As key exchange schemes with certificates require some trusted authority to verify integrity of the received messages, the extension to a larger system may be difficult. They need a large storage for certificates and more bandwidth for the verification of the signature as the number of user's increases. The authentication method requires that the client and server are each pre-provisioned with a unique asymmetric Elliptic Curve Cryptography (ECC).

2.11 EFFICIENT IDENTITY-BASED
DISTRIBUTED DECRYPTION
SCHEMES FOR HETEROGENEOUS
PERSONAL HEALTH RECORD
SHARING SYSTEM

2.12 BLOCKCHAIN TECHNOLOGY
FOR HEALTHCARE
EMERGENCY SHARED
ELECTRONIC HEALTH