INDEX

LIST OF FIGURES

CHAPTER-1

INTRODUCTION:

An identity is a set of information which can be used to identify an entity. If an identity matches an entity, there is only one such entity, i.e. there are not two different entities that have the same identity. This implies that identities are unique. The uniqueness of identities can be used as keys in cryptographic schemes. Applying this property to the public-key cryptography, Adi Shamir proposed a scheme called Identity-Based Encryption (IBE). In this scheme, the public key of the receiver can be created based on his identity, and then the sender can use the key to encrypt and send messages to the receiver. The sender needs to know the identity, e.g. names or email addresses, in order to send to the receiver. Thus, the identity, in this case, is public. However, applying that property to secret-key cryptography is another problem. In secret-key cryptography, the keys are secret, so the identities are also secret.

To protect the secret, a cryptographically secure pseudorandom number generator is used to generate keys, but cannot be applied to identity information in the same way, because it is predetermined and unchanged. For that reason, instead of generating, we design a scheme that selects at random the information from the private identity through a questionnaire. To ensure the safety of the questionnaires, we also propose security scenarios and prove that our method is secure under them. After all, we construct an application using our scheme for key management. In the application, the keys do not need to be stored, but only the information to remind users of the generating process is stored. Therefore, the application can be built in a decentralized manner.

Various decentralized systems are designed based on Blockchain technology such as Bitcoin, Ethereum. To create transactions on Blockchain, and user need to have an address associated with a public/secret key pair. But in our application, the key pair is used one time to create only one transaction, and then the user does not need to keep it. Hence, the key pair is considered as a one-time account. In summary, we make the following contributions: A scheme uses questionnaires to get private identities to create keys for a secret-key encryption. Security scenarios are used to evaluate the security of the scheme is based on questionnaires. A decentralized application based on the schemeis used for key management.

1.1 EXISTING SYSTEM:

In the existing system, a sender can encrypt a message or information for a receiver knowing just the identity of the receiver and importantly, without obtaining and verifying the receiver’s public-key certificate. Applying that property to secret-key cryptography is another problem. To protect the secret, a cryptographically secure pseudorandom number generator is used to gene generates, but cannot be applied to identity information in the same way, because it is predetermined and unchanged.

1.1.1. DISADVANTAGES OF EXISTING SYSTEM:

- Consequently, with a standardized public-key string format, an IBE scheme completely eliminates the need for public-key certificates.
- The identity, in this case, is public. However, applying that property to thsecret-key cryptography is another problem.

1.2. PROPOSED SYSTEM:

In the proposed system, a private key generator will generate the public key and private key for the certified users. So that the users will receive each other’s public key for identification and the data has been encrypted through private key. We Propose security scenarios and prove that our method is secure under them. After all, we construct an application using our scheme for key management. In the application, the keys do not need to be stored, but only the information to remind users of the generating process is stored. Therefore, the application can be built in a decentralized manner.

1.2.1 ADVANTAGES OF THE PROPOSED SYSTEM:

- Scheme uses questionnaires to get private identities to create keys for a secret-key encryption.
- A decentralized application based on the scheme is used for key management.

1.3. SYSTEM SPECIFICATION

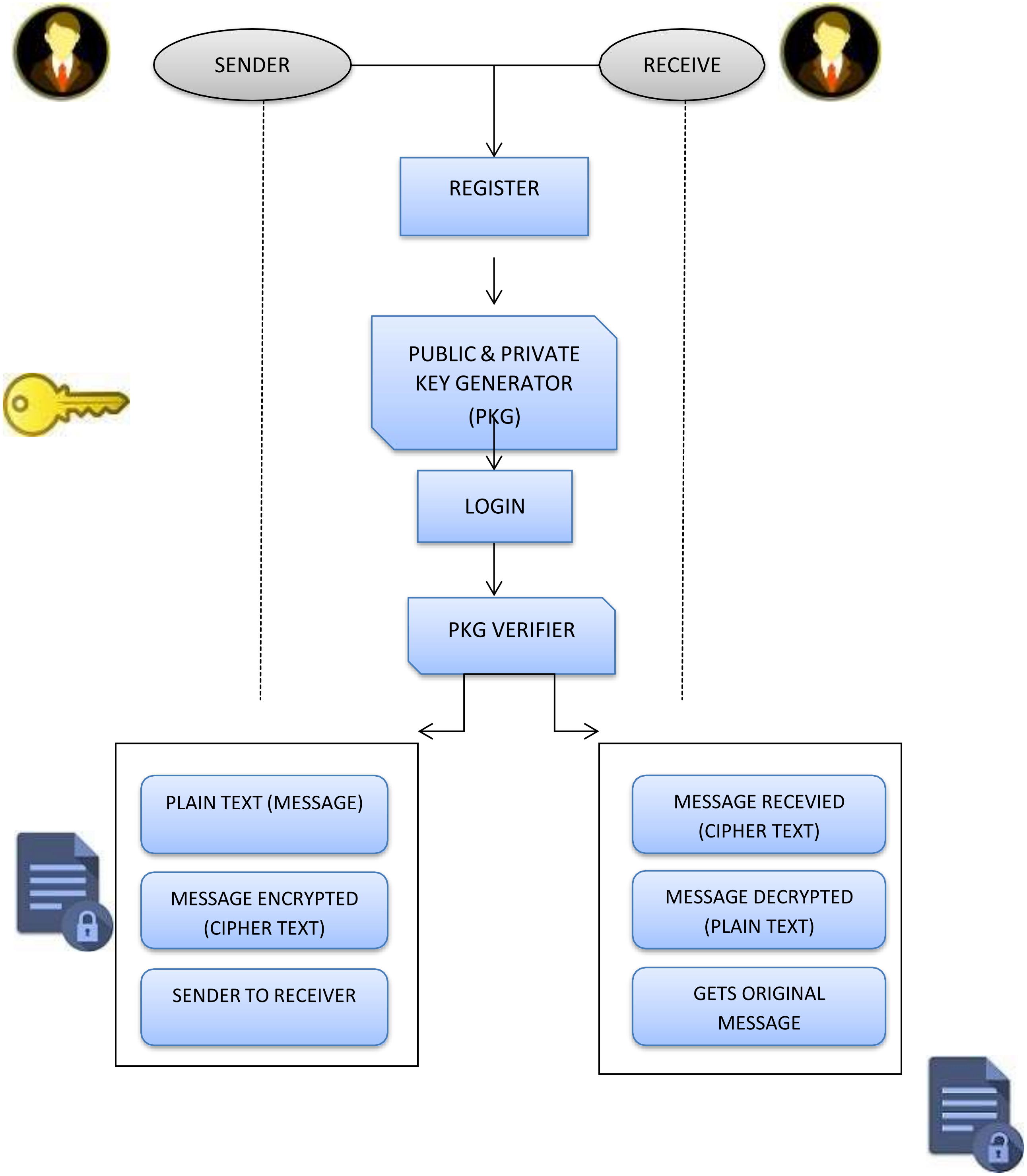
1.3.1. HARDWARE REQUIREMENTS:

Processor:		Intel Core i3 Processor
Speed:		2.5 GHz
RAM	:	2GB(min)
Hard Disk:		500MB
Key Board:		Standard Windows Keyboard
Mouse:		Two or Three Button Mouse
Monitor	:	LCD

1.3.2. SOFTWARE REQUIREMENTS:

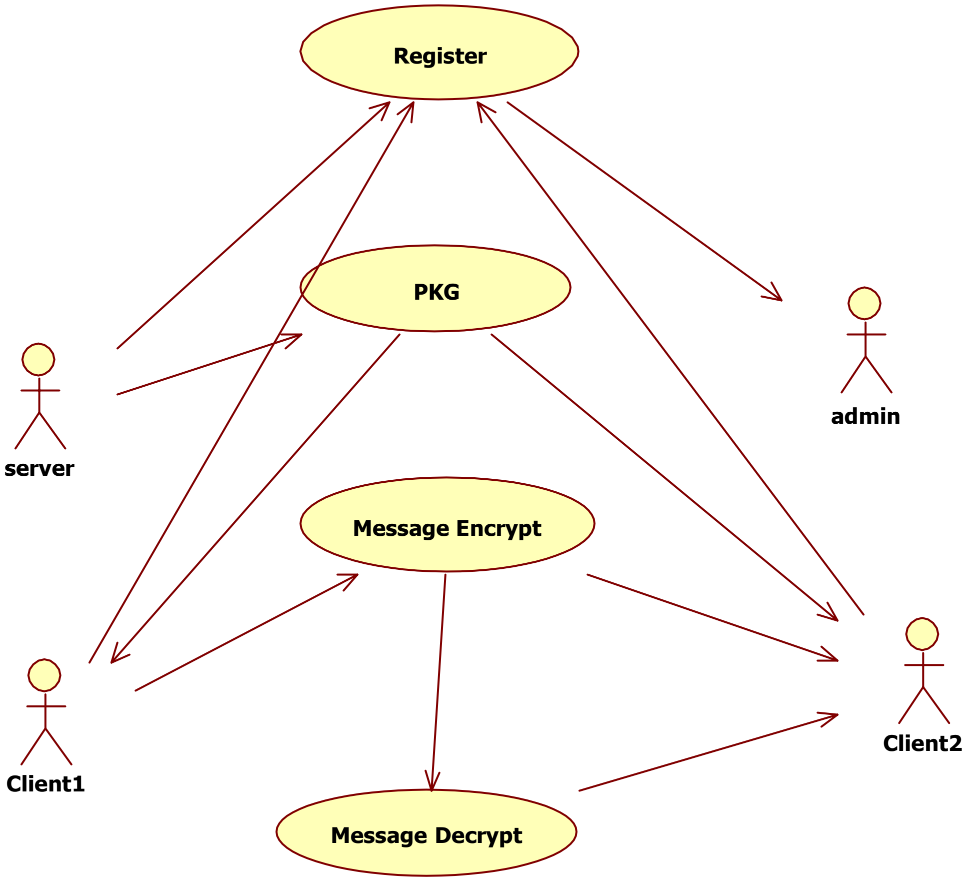
Operating System	:	Windows7/10.
Application Server	:	Tomcat6.0/7/8.X.
Front End	:	Java , HTML,CSS
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
IDE	:	Net beans
Back End	:	MYSQL 5.0/ Heidi SQL 8.1
Database Connectivity	:	JDBC

1.1 ARCHITECTURE DIAGRAM:

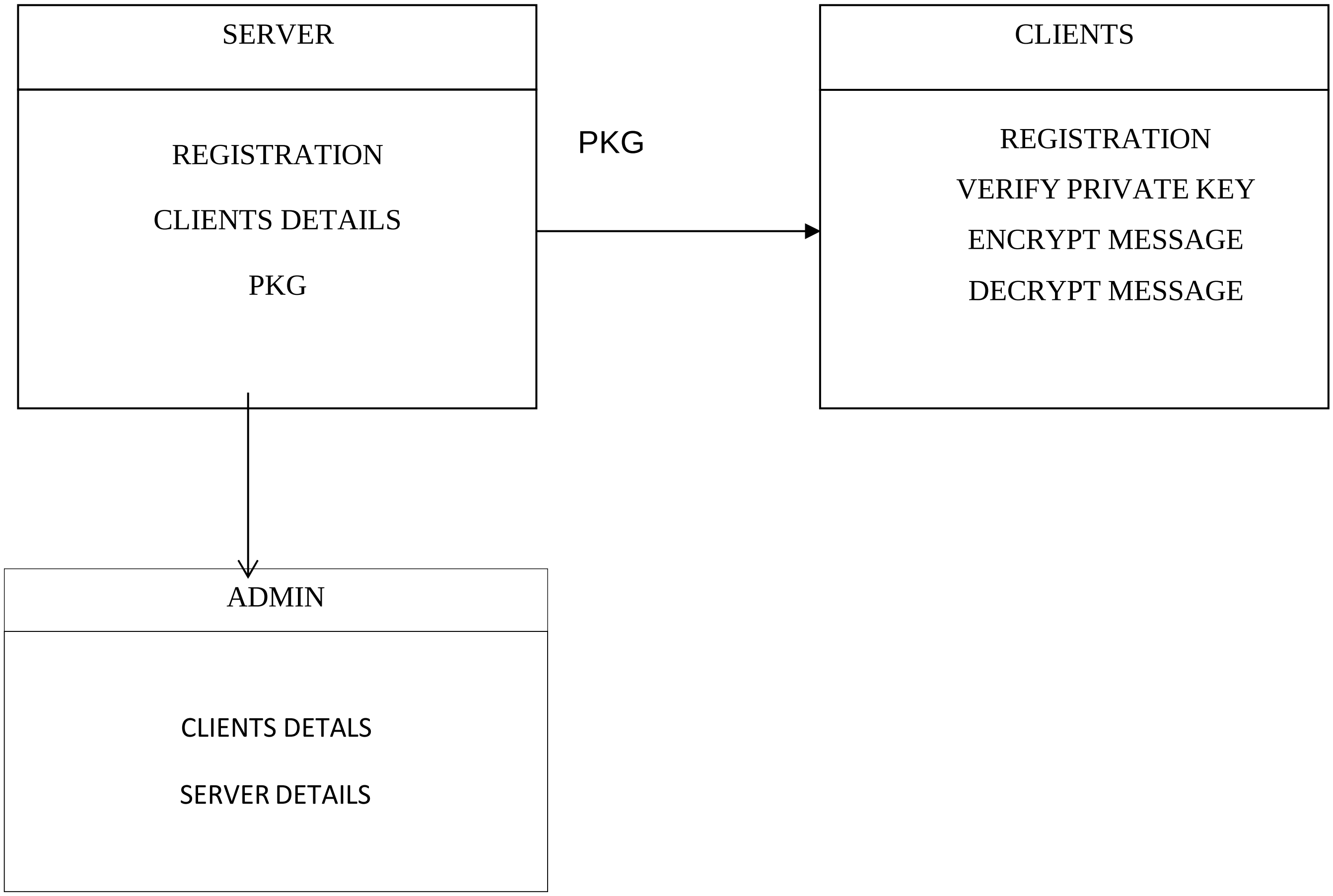

SENDER
RECEIVE
REGISTER
PUBLIC & PRIVATE KEY GENERATOR (PKG)
LOGIN
PKG VERIFIER
PLAIN TEXT (MESSAGE)
MESSAGE ENCRYPTED (CIPHER TEXT)
SENDER TO RECEIVER
MESSAGE RECEVIED (CIPHER TEXT)
MESSAGE DECRYPTED (PLAIN TEXT)
GETS ORIGINAL MESSAGE

1.2 UML DIAGRAMS:

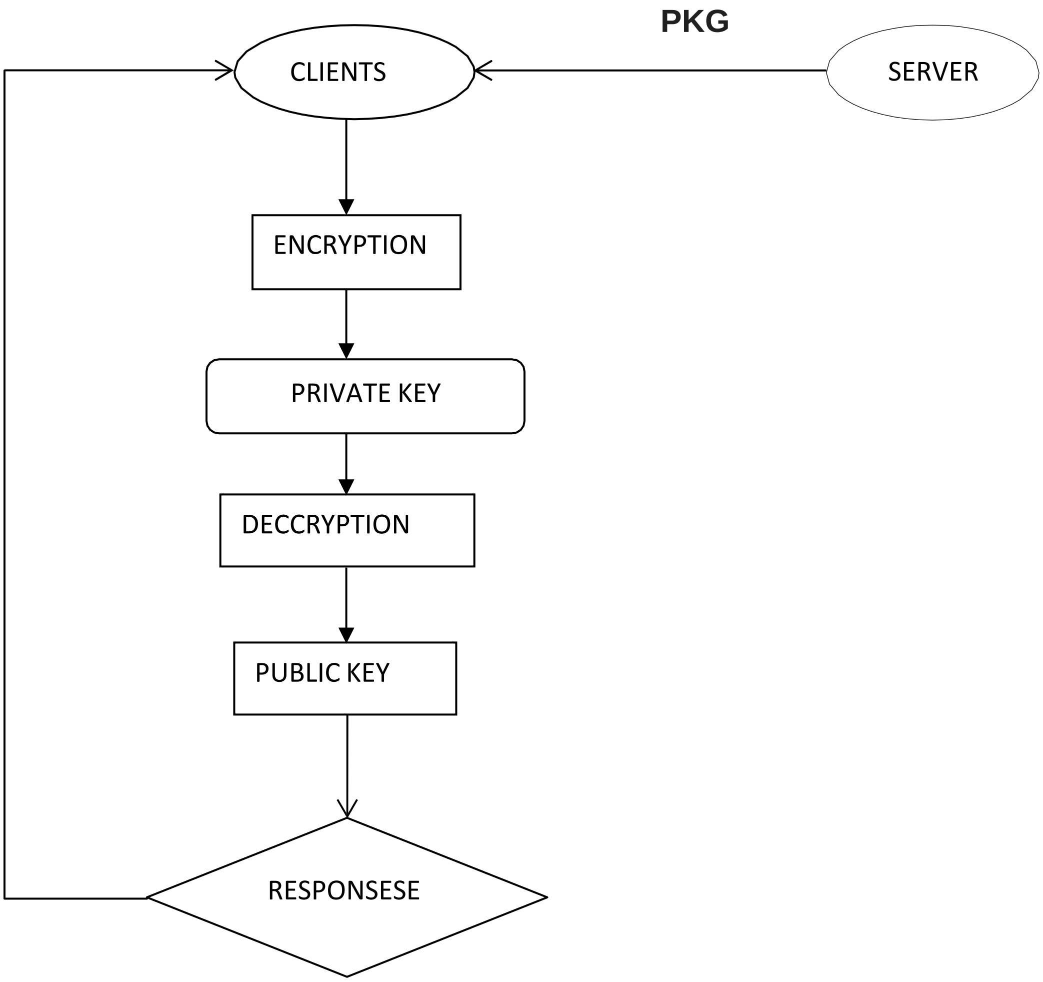
1.2.1 USECASE DIAGRAM:



1.2.2 CLASS DIAGRAM:-



1.2.3 DATA FLOW DIAGRAM:-



CHAPTER-2

LITERATURE SURVEY

TITLE: Secure Key-Reduplication with Identity-Based Broadcast Encryption.

YEAR OF PUBLISHING: 2021

AUTHOR NAME: Ling Liu, Yuqing Zhang.

ABSTRACT:

For the purpose of ensuring data confidentiality, they are usually encrypted before beingoutsourced. Traditional encryption will inevitably result in multiple different ciphertexts produced from the same plaintext by different users' secret keys, which hinders data deduplication. Convergent encryption makes deduplication possible since it naturally encrypts the same plaintexts into the same ciphertexts. One attendant problem is how to reliably and effectively manage a huge number of convergent keys. Several deduplication schemes have been proposed to deal with the convergent key management problem. However, they either need to introduce key management servers or require interaction between data owners. In this paper, we design a novel client-side deduplication protocol named KeyD without such an independent key management server by utilizing the identity-based broadcast encryption (IBBE) technique. Users only interact with the cloud service provider (CSP) during the process of data upload and download. Security analysis demonstrates that KeyD ensures data confidentiality and convergent key security, and well protects the ownership privacy simultaneously.

TITLE: Identity-Based Hybrid Format-Preserving Encryption Scheme.

YEAR OF PUBLISHING: 2020