A Novel Method For Linking Existing Health-Related Data and Maintaining Participant Confidentiality

Project By:
Mayuri D. Patil
Vrushali S. Patil
Rupali S.baviskar
Swati S.Patil
Guided by: Mr.Manoj E. Patil

SSBT's College of Engineering & Technology,
Bambhori, Jalgaon - 425 001, Maharashtra, India

Outline

Introduction

- A novel method is develop for a record linking of existing individual health care data and maintaining participant confidentiality.
- Strong security is provided through standard Encryption Algorithm (i.e. AES) and by maintaning a Lock Table.

Literature Survey

Existing system faces several problems:

- Either a unique personal identifier,like social security number, is not available or non-unique person identifiable information, like names, are privacy protected and cannot be accessed.
- Unfortunately, encrypted hash codes of two names differ completely if the plain names differ only by a single character.

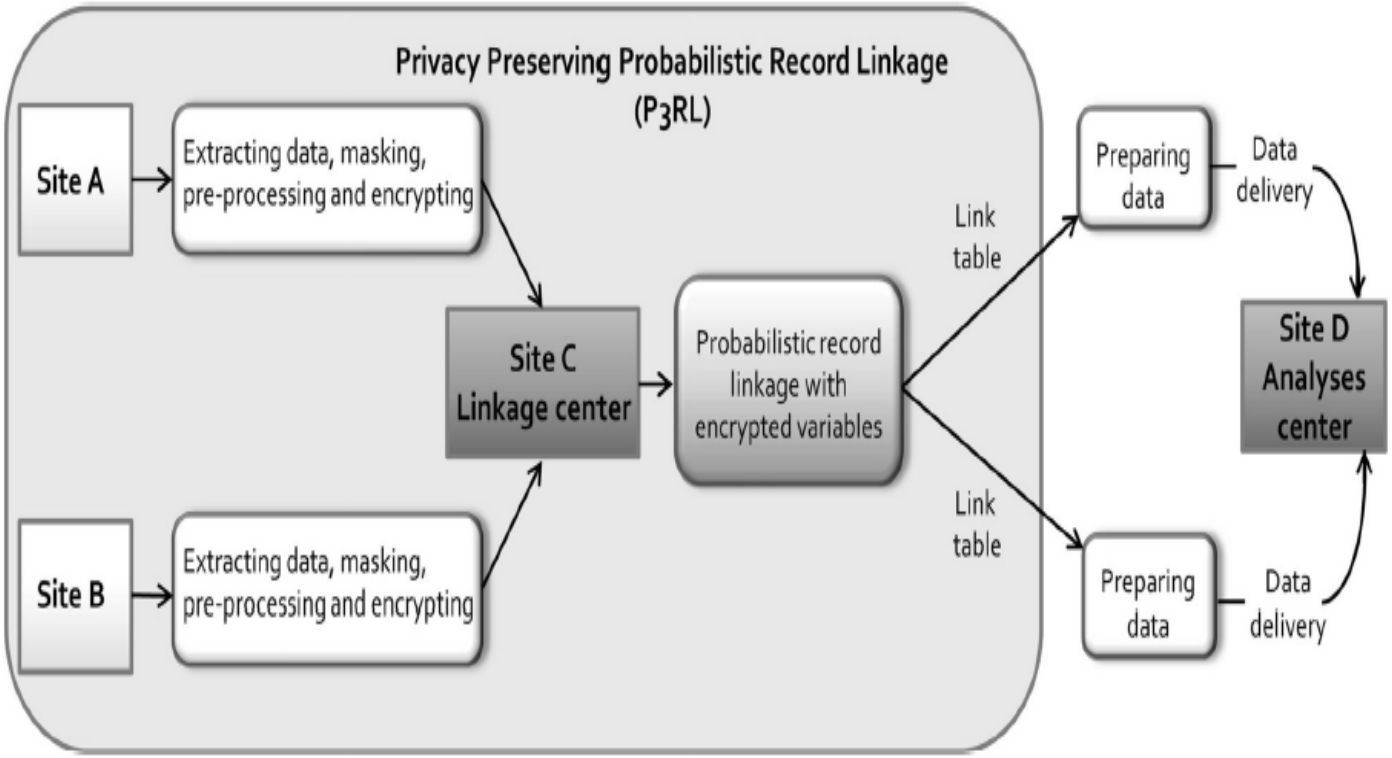
Therefore, standard encryption methods be applied to overcome these challenges.

Proposed system

- In our system we apply a three-party protocol, with two sites collecting individual data and an independent trusted linkage center as the third partner.
- Our method consists of three main steps: Pre-processing, encryption and probabilistic record linkage.

System Architecture

- System Architecture



AES Algorithm

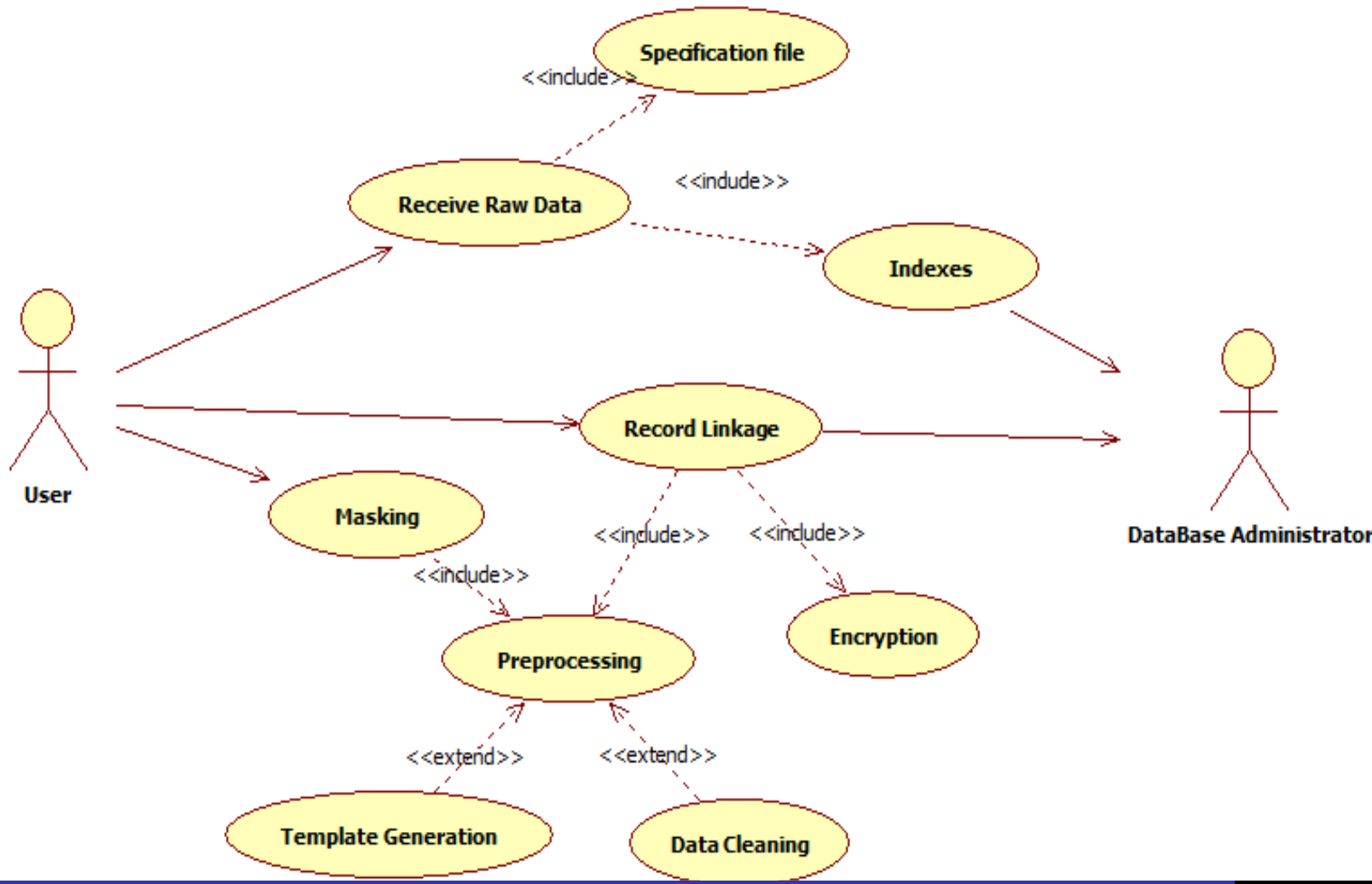
- Encryption steps:

1. Convert string data to ASCII format.
2. Convert ascii to binary format
3. Right shift the bit by 256 bit.
4. Convert the shifted bits to unicode formate.
5. Generate string from unicode.

- Decryption steps:

1. Get string and convert to unicode.
2. Convert unicode to binary format
3. Left shift the bit by 256 bit.
4. Convert to ascii formate.
5. Convert ascii format to string data.

Usecase diagram



Requirement Specification

Software Requirement:

- Operating system
- Jdk1.6
- WAM Server
- Dream Viewer

Hardware Requirement:

- A Windows-compatible LAN Network
- Processor P4
- At least 512 megabytes (MB) RAM
- Automated pre-processing and encryption fully protect sensitive information ensuring participant confidentiality. This method is suitable not just for epidemiological research but also for any setting with similar challenges.

References

- Schmidlin et al. BMC Medical Research Methodology (2015) 15:46
- CBS — 2014 Record Linkage in Health Data: a simulation study

Thank You...