ABSTRACT

This research project (Private MD) implements a modified version of PriView, a privacy-preserving technique for querying third-party services from mobile devices. Classical private information retrieval (PIR) schemes are difficult to deploy and use, since they require the target service to be replicated and modified. To avoid this problem, PriView utilizes a novel, proxy-mediated form of PIR, in which the client requests dummy query responses to the proxy server. This way the proxy server does not know the actual request made by the user. The proxy then sends the query requests to the target web server which handles queries. This technique provides both confidentiality and anonymity with respect to the target service, which knows neither the identity of the client device or the exact query it issued. Our application, Private MD, will allow the user to enter symptoms in order to get a preliminary diagnosis. Further work will be done to implement a more accurate diagnosis, which utilizes SNOMED-CT, include a feature which allows the user to find a doctor based on their profile, and allow the user to use their voice to describe their symptoms. Furthermore, more privacy-preserving techniques will be implemented and tested for security and usability.

BACKGROUND

Other Health Applications
- iTriage
- WebMD
- Aida

Drawbacks
1. Gather personal information and use it for many purposes, such as advertisement.
2. Don’t assist in finding a doctor.
4. Don’t take preventative measures to secure privacy.

PROBLEM & OBJECTIVE

Problem
- Web services are able to capture the user’s information whenever you use their service.
- Web Services are also able to capture the user’s request which can contain sensitive information.
- Third-party services are able to use this sensitive information for purposes such as advertisements.

Objective: The main objective of our project is to successfully allow a user of our application to query information while hiding that query and the user’s information. This will be achieved using our modification of the PriView.

Our research project will assist the user in:
- Self Diagnosis
- Privacy Preservation
- Assisting locating doctors’ office

EXPERIMENTAL ENVIRONMENT

Devices Used for Development and Testing
- Samsung Galaxy S8
- LG G6
- Mac for testing
- Various windows laptops for development

Tools and Databases Used
- Android Studio
- Heroku
- Django
- Amazon EC2
- Wireshark
- Columbia Medical Database
- Pen Testing (OWASP, Zap, Jenkins, Vega)

METHOD

System Overview

Privacy Test

Proposed Algorithm

1. Create dummy queries, and place it in a random sequence to obfuscate the real data being transmitted.

2. Encrypt the request using SSL and send it to the proxy server (using the http protocol handled by android automatically). This step is done so that we don’t accidentally leak information.

3. From the proxy send a request to the web application, to hide the user’s information from the Cloud Service.

4. Query the information and send it back through the proxy to the client.

Implementation of the System

Analysis of the Results

Test of the privacy

CONCLUSIONS

Future Work
- Implement more security techniques and analyze their security
- Increase the accuracy of the diagnosis using wordnet and SNOMED-CT
- Locate a doctor specific to the user

REFERENCES


ACKNOWLEDGEMENT

The project is funded by National Science Foundation Grant No. CNS-1559692 and New York Institute of Technology.

DISCUSSIONS

Usability and user privacy are two fundamental requirements for medical applications. Our framework allows users to map symptoms to diseases using online services, without revealing any of their symptoms to the service provider. Instead of using two proxy servers, we used one to act as the middleman between the user and the internet service. The framework also hides the user’s identity, which means the online service will not know who is accessing or querying their database. Particularly, this technique provides both confidentiality and anonymity with respect to the target service.

Future improvements and potential downsides of implemented system
- Sending queries only to proxy allows for increased confidentiality.
  - This system is more susceptible to an outside attacker since there is only one proxy server.
  - Our focus is hiding the user’s identity and query requests from the internet service not an outside attack by a third-party

FUTURE WORK

REFERENCES

ACKNOWLEDGEMENT

The project is funded by National Science Foundation Grant No. CNS-1559692 and New York Institute of Technology.