PrivateMD

REU Fellows: Randy St. Fleur and Daler Norkulov
Faculty Mentors: Dr. Helen Gu
Affiliation: School of Engineering and Computing Science, NYIT
Emails: rstfleur@nyit.edu, dnorkulo@nyit.edu, hgu03@nyit.edu

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
- Ada

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

Downfalls of classical PIR
- Downloading the entire database
  - Maximum communication complexity
- Other PIR systems require:
  - Replicating the database on multiple servers
  - Excessive Computation, ex: Quadratic Residue

PriView PIR system
- Eliminates the need to replicate or modify databases
- Can be used with third-party services

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

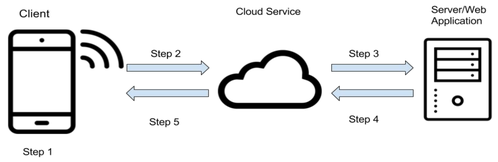
Devices Used for Development and Testing
- Samsung Galaxy S8
- LG G6
- iMac for testing
- Various windows laptops for development

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

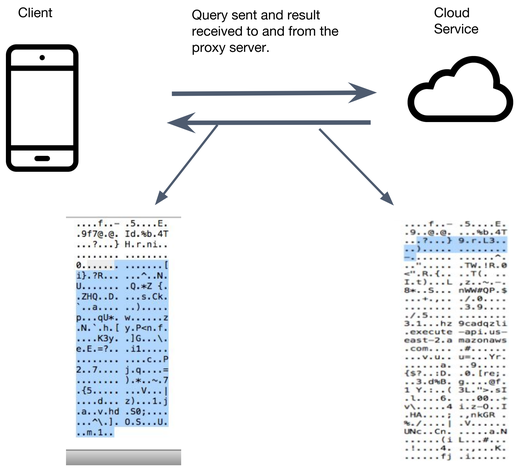
METHOD

Implementation of the System → Test of the privacy → Analysis of the Results

System Overview



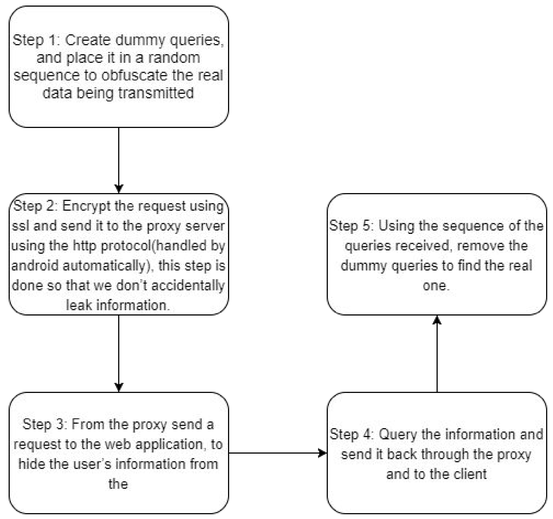
Privacy Test



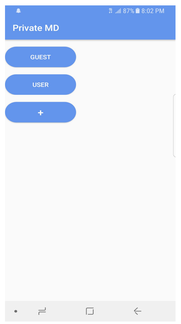
It is evident that the android application automatically encrypts the data being sent.

Primary Handshake showing that the client is connecting to Amazon

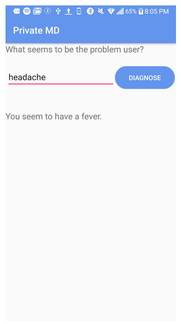
Proposed Algorithm



App User Interface



Main screen of the application



Diagnosis Screen

DISCUSSIONS

Usability and user privacy are two fundamental requirements for medical applications. Our frame-work 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.

Improvements and potential downfalls of implemented system
- Sending queries to only one 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

CONCLUSIONS

- Our frame-work allows users to map symptoms to diseases using the online service that was developed.
- A modified version of a PIR system, PriView, was defined and without revealing any of their symptoms to the service provider, a user is able to get a medical diagnosis
- Wireshark showed the information being sent to the proxy is encrypted and pen testing showed there are many existing proxy servers which need to be replicated for a man in the middle attack
- We were able to generate random queries which prevents the proxy from knowing the true query and using the proxy prevents the internet service from determining the user's identity

FUTURE WORK

Future Work:
- Implement more security techniques and analyze their security
- Measure energy consumption
- Measure bandwidth usage
- Measure latency
- Increase the accuracy of the diagnosis using wordnet and SNOMED-CT
- Locate a doctor specific to the user

REFERENCES

[1]Surabhi Gaur,Melody Moh,Mahesh Balakrishnan, "Hiding behind the clouds: Efficient, privacy-preserving queries via cloud proxies - IEEE Xplore Document", Ieeexplore.ieee.org, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/6825035/. [Accessed: 13- Jun- 2017].

[2]People.dbmi.columbia.edu. (2017). Disease. [online] Available at: http://people.dbmi.columbia.edu/~friedma/Projects/DiseaseSymptomKB/index.html [Accessed 1 Aug. 2017].

[3]E. Kushilevitz and R. Ostrovsky, "Replication is not needed: single database, computationally-private information retrieval", Dl.acm.org, 2017. [Online]. Available: http://dl.acm.org/citation.cfm?id=796363. [Accessed: 13- Jun- 2017].

[4]Flaticon. (2017). Apple logo free vector icons designed by Freepik. [online] Available at: https://www.flaticon.com/free-icon/apple-logo_37150 [Accessed 2 Aug. 2017].

[5]Android, smart phone icon. (2017). [image] Available at: https://www.iconfinder.com/icons/211118/android_smart_phone_icon [Accessed 31 Jul. 2017].

[6] Python Logo. (2017). [image] Available at: https://www.python.org/community/logos/ [Accessed 31 Jul. 2017].

[7] Django Logo. (2017). [image] Available at: https://www.djangoproject.com/community/logos/ [Accessed 31 Jul. 2017].

[8] Amazon AWS Logo. (2017). [image] Available at: http://www.zdnet.com/article/aws-makes-database-migration-service-available-to-all-customers/ [Accessed 31 Jul. 2017].

[9] Android Studio Icon. (2017). [image] Available at: https://commons.wikimedia.org/wiki/File:Android_Studio_icon.svg [Accessed 31 Jul. 2017].

[10]Heroku Icon. (2017). [image] Available at: https://icons8.com/icon/31085/heroku [Accessed 31 Jul. 2017].

[11]WireShark Icon. (2017). [image] Available at: https://wireshark.en.uptodown.com/windows [Accessed 31 Jul. 2017].

ACKNOWLEDGEMENT

The project is funded by National Science Foundation
Grant No. CNS-1559652 and New York Institute of Technology.