The Mobile Cloud Server

**Introduction:**

Cloud computing and backup services have revolutionized modern computing. Files can now be uploaded to a website and then immediately accessed from the other side of the globe. Just a few decades ago and within the lifetime of most people taking CS370 this technology has completely taken the technology industry by storm. With services such as Icloud and Verizon Backup the loss of a cell phone has become a minor inconvenience with data recovery compared to a total loss of the data 15 years ago. But as data breaches occur security becomes a major concern for many consumers.

Our group has set out to solve a problem that plagues so much of our databases and servers; hackers being able to remotely breach a server or database. Using the Raspberry Pi we intend on building a fully functional mobile cloud server that can be put online and offline as needed. While offline the files on the Raspberry Pi are inaccessible to the rest of the world and secure.

While online this server can be accessed remotely from anywhere in the world to upload and download files as needed. This allows for secure backup for any files. Using the power of the Apache libraries we will configure the Raspberry Pi to become a Mobile Cloud server. When operating the server will have password protection and encryption using https.  Though this is on a small scale, this way of files storage has uses on a large scale. If data only had to exist when it is needed by the user and not when it is not, the added level of security could prove extremely difficult for hackers to breach.

**Problem Characterization:**

All cloud computing services suffer from the same critical flaws. Your data is only as secure as your password. Also how ethical the engineers at said company are. If you backup birth certificates, social security card, and bank information for example, your data might as well be public if your account is breached. An example of this is the 2017 breach of the credit bureau Equifax. 150 million people had their data compromised by hackers. This data included sensitive information such as social security numbers. Federal authorities estimate 99% of people affected in this breach had their social security numbers compromised. That constitutes 145.5 million people or about half the population of the United States.

The scapegoat for this was one former IT worker for Equifax. Though this statement by their former CEO has raised eyebrows, the incompetence of one employee allowing this to happen is very disturbing. Equifax’s “official” answer is this employee did not manually patch the application that was compromised. Events such as this have given thought to starting to decentralize data of this scale to allow for a higher degree of security.

The problem with all databases is all the computers in them are connected to every other internet capable device in the world all the time. These databases are only secure until one hacker figures out how to breach their firewall. Given these databases can be breached from anywhere in the world this gives hackers many opportunities to attempt to breach these databases. Attempts to breach these databases happen continuously and the hackers must only be successful once to compromise hundreds of millions of user’s data.

Another problem with the centralization of databases is the continuous threat of cyber warfare. Companies for example that the pentagon contracts with all have large databases. Countries such as North Korea which frequently engages with the United States in cyber warfare. They only have to be successful once to gain valuable military secrets. But the most infamous public cyber warfare would be the 2014 hack of Sony by the North Korean hacking group Guardians of Peace.

In 2014 Sony released the film *The Interview* which was a comedy about a plot to assassinate North Korean leader Kim Jong-Un. Although North Korea demanded Sony pull the film, they went ahead and released it on December 6th, 2014. The group retaliated by breaching the Sony employee databases and released employee information. Because of this data breach personal information of many Sony employees is still circulating on the internet today.  Still weeks after this attack all phone and internet communications went down in North Korea for several days from a cyber-attack. No government has taken responsibility for the responsive attack on North Korea but it is generally believed the United States launched a Denial of Service Attack in response for the Sony hack.

With all these breaches and attacks the question comes, “What if the data in question only needed to exist when it is needed?”.  What this means if only have the server online when the files need to be accessed and offline and inaccessible to all when they are not needed. Our group aims to find a feasible solution to the security issues that plague modern databases. Using the power of modern solid state memory files can be made inaccessible to the rest of the world and 100% secure.

**Solution:**

After discussing these problems as a group and conducting our own research, we felt that the best solution to problem characterizations would be to create a private cloud server. After even more research and discussion we found just what we were looking for in NextCloud. According to their website, “Nextcloud offers industry-leading on-premises file sync and online collaboration technology. Our expertise is in combining the convenience and ease of use of consumer-grade solutions like Dropbox and Google Drive with the security, privacy and control business needs.Our self-hosted solutions ensure you know where data is, who has access, and that even meta-data does not leak.” Just looking at this you can clearly see NextCloud tackles all the problems that we were concerned about. Our confidence in NextCloud was only further strengthened when looking at their credibility. After googling reviews and looking at their partners and seeing nothing but great reviews and outstanding partners, we realized the only thing left for us to do was find a way to meet the requirements with our raspberry pi.

**Methodology:**

During the early stages of configuring the network settings and other procedures for some reason we could not connect to the CSU Eid wifi. Fortunately we managed to figure it out but soon realized that it allowed access to our personal passwords so we decided to use the CSU guest wifi despite it obviously very slower. The reason for that is being our emphasis on security and feeling we are compromising that if we don't stick with the guest wifi. Another issue we were having during the early stages was what later found out to be that we were using the wrong password. Thankfully this problem was solved relatively quickly thanks to someone pointing this issue out on the class message board and the solution also being posted there. After configuring the network settings and other general first-time setup procedures for our Raspberry Pi, we then had to install and setup Apache and PHP so that Nextcloud could run on this platform.  After installing and setting up Apache and PHP, we installed and extracted the latest version of Nextcloud. From there, we set up a directory - local to our Raspberry Pi - to store the data that is sent to our server. After this, we assigned ownership and permissions to access this new Nextcloud data folder directly from the Raspberry Pi. We assigned ownership and permissions to read and write to administrators. Now, we were able to access the Nextcloud server through HTTP by going to \*our Raspberry Pi’s IP Address\*/nextcloud. We made an account with a username and a password so that we could securely access our data. Finally, we are now able to upload and download files to our server (though, for now, the maximum file size for uploading is 1GB, which we can easily change in one of the configuration files). Those files we chose to upload were just some basic python tutorial codes to show that even teachers could also use this and it works just as well. We could also migrate the destination folder, but our 32GB SD card that also houses the operating system should be sufficient for this project.  Our server is set up, and, when the Raspberry Pi is connected to a network, we can access our files and data.

After a several hours of frustrating work we were finally able to configure a static IP address after looking onto the Raspberry Pi website. This now allowed the Raspberry Pi to be accessible from anywhere in the world when connected.

**Libraries:**

Using the external cloud service “Nextcloud”, along with PHP7.0 and Apache2 libraries, we were able to host a cloud server with our Raspberry Pi acting as the host on a network.  Nextcloud is a consumer-based cloud service that allows for secure data transactions and permission-based data accessing. The Apache2 library is a recent release of the Apache HTTP server - an open-source and free cross-platform web server software - which allows us to access our cloud through HTTP by connecting to our Raspberry Pi’s IP Address. Finally, PHP7.0 is used as a server-side scripting language that is used by Nextcloud in conjunction with Apache2 to ensure that we can access data through the Raspberry Pi.

**Conclusion:**

Companies - especially in the social media realm - love our data.  Many of them track our data and sell our patterns and interests to advertising companies to personalize and target products to us.  Personal and secure cloud servers are a perfect way of counteracting the constant spying and sniffing going on with other, more public file sharing services.  With technology allowing for data to become more and more easily available, companies and individuals alike are actively looking for secure, private data-storage solutions.  This project proves that a solution does not require ridiculously priced hosts or a profound knowledge on self-hosting a server. With the Raspberry Pi, along with the Nextcloud service - running with Apache and PHP - safe and secure data storage is incredibly easy.

**Bibliography:**

1.    “Equifax Breaks down Just How Bad Last Year's Data Breach Was.” *NBCNews.com*, NBCUniversal News Group, www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496.

2.    “Sony Pictures Hack.” *Wikipedia*, Wikimedia Foundation, 27 Oct. 2018, en.wikipedia.org/wiki/Sony\_Pictures\_hack.

3.    “The Former Equifax CEO Took an Apology Tour on the Hill.” *NBCNews.com*, NBCUniversal News Group, www.nbcnews.com/business/consumer/former-equifax-ceo-blames-one-it-guy-massive-hack-n807956?icid=related.

4.    “How to Setup a Raspberry Pi Nextcloud Server.” *Pi My Life Up*, 16 Aug. 2018, pimylifeup.com/raspberry-pi-nextcloud-server/.