

Portland State University

PDXScholar

University Honors Theses

University Honors College

5-26-2017

Methods for Safeguarding Client Data

Jelon L. Anderson

Portland State University

Follow this and additional works at: <https://pdxscholar.library.pdx.edu/honorstheses>

Let us know how access to this document benefits you.

Recommended Citation

Anderson, Jelon L., "Methods for Safeguarding Client Data" (2017). *University Honors Theses*. Paper 412.
<https://doi.org/10.15760/honors.405>

This Thesis is brought to you for free and open access. It has been accepted for inclusion in University Honors Theses by an authorized administrator of PDXScholar. Please contact us if we can make this document more accessible: pdxscholar@pdx.edu.

Methods for Safeguarding Client Data

by
Jelon Anderson

*An undergraduate honors thesis submitted in partial fulfillment of
the requirements for the degree of Bachelor of Science*

*in
University Honors
and
Computer Engineering*

Thesis Adviser
Garrison Greenwood

Portland State University
May 26, 2017

Methods for Safeguarding Client Data

Jelon Anderson, Dr. Garrison Greenwood

April 2017

Abstract

An evaluation of the modern security methods in which best protect client's data for an engineering capstone project.

Introduction

Today, the number of novel applications such as sensors, cyber-physical systems, smart mobile devices, cloud systems, data analytics, social networks, Internet of Things (IoT), and smart and connected healthcare are drastically increasing. The amount of data generated, collected, stored, and processed is referred as Big Data [1]. Modern analytics project technology will consume our society to the point where there is an electronic device connected to the internet within three feet of every person 24 hours a day. The number of devices connected to the internet will continued to sky-rock each year. By 2020, more than 20.8 billion IoT devices will be installed worldwide [2]. With this rapid technology growth, a proportional increase in the number of cyber-crimes, hacks, data breach and company lawsuits becomes inevitable.

In this paper, we target the issue of the security breach by surveying recent headlines with the primary focus on lawsuits and the number of users affected by the security breaches. The goal is to identify common security practices used to protect against cyber criminals. Based on the identified methods, an evaluation will be assessed to pinpoint the most applicable security protocol for the small business, RapidMade.

Motivation and Background

More than ever, data breaches are happening on a regular basis. In fact, within the past five years, several well-known businesses made headlines around data security. These multi-billion companies include Amazon, Target, Anthem, Yahoo, Facebook, Hewlett Packard, Verizon, Ebay

and more. Even smaller business like Wright Hotels, PATCO Construction, Providence, and Volunteer Voyage suffered cyber-attacks.

The motivation behind this topic and this research paper derives from my Capstone project. Within the scope of the capstone, the outcome of the project is to deliver a customer portal protocol where clients can register, login, or place orders as guests. To fulfill both engineering and honors' thesis requirement, my advisor, Dr. Garrison Greenwood, and I found data security and safeguard client information to be the most applicable approach in meeting both requirements.

Technology Emergence

The evolution of technology has transformed our economy and revolutionized human behavior in the digital age. In fact, there is a 25,000 percent increase in the number of internet users from 1993 to 2017 [3].



Figure 1: Figure shows the comparison between the world population with the number of active internet users, active social media users, mobile subscription user, and mobile social users.

Within the same period of time, our world's population only rose 33 percent. As of today, the current world population reaches over 7.4 billion people. More than 3.7 billion people are active internet users with and it is growing at a rate of 10 new users per second. Of that 3.7 billion people, more than 1.87 billion of them are monthly active users on FaceBook, 1 billion users each on WhatsApp and Facebook Messenger, 600 million on Instagram, 300 million on Snapchat, 66 million are Amazon Prime members, and more than 21.5 million are members of the most popular dating domain match.com [4].

Problem

Technology has refashioned how businesses operate today compare to 20 years ago. Before the emergence of the internet, businesses operated under the brick and mortar structure where consumers physically commuted to the store, picked out their product, and then commuted to their destination. Around 1991, when the internet opened for commercial use, businesses started creating websites, applications and other platforms to sell goods and services. These platforms invented the click and order structure that brought leisure and conveniences to the consumers. In order to take advantage of this, customers have to be registered in the business's database.

Creating an account involves customers providing confidential and personal information which includes first and last name, date of birth, email address, physical address, phone number, credit card information etc. Consequently, people are giving up their personal identity and carrying the risk of having their information exposed or stolen.

Entering the 21st century, technology advancement has allowed data security to be more robust. However, cyber-criminals still find ways to break through the security walls and access servers to steal valuable information. Recently, Amazon, the largest e-commerce in the world was attacked. Back in July of 2016, Amazon, suffered a security breach where a hacker by the Twitter name of El Taylor (@0x2Taylor) accessed Amazon's servers and released 80,000 Kindle login credentials to the public [5]. The attacker claimed he breached a server and had access to user's email, password, city, state, phone number, zip code, user-agent, LastLoginIP, Proxy IP, and street address. When Amazon found out about the incident, they responded immediately and disabled all the accounts. According to the Vice President of Operations at the cybersecurity firm, Synack Tony Gambacorta quotes, "Given all this data I would have no reason to believe this isn't valid. I can definitely see phone numbers, street addresses, email addresses, the last time a user logged in (7:33 p.m. on June 5th of this year, meaning this isn't old data), how many times that user tried to log in, how many times he successfully logged in and his login source IP address." [6]. Later on, Amazon claimed the hack was illegitimate and the leaked information did not come from Amazon's server. Amazon's conclusion to the incident raises a question on the validity of Amazon's statement when considering the market share of the company.

Online dating has become the very popular nowadays. Some of the modern dating platform includes, Match, Tinder, Coffee meets Bagel, Meetme, Bumble, and more. Dating platforms often dig deeper into intimate information compared to other platforms. For example,

users are required to answer detailed questions such as height, age, ethnicity, occupation, hobbies and so forth. In addition, the dating search engines also require users to specify age and ethnicity preference. Unfortunately, a Canadian dating company broke news headline in 2015. According to Steven Devin, the editor of Network Security, a team of hackers called “The Impact Team” exposed 40 million user accounts on a Canadian dating site Ashley Madison run by Avid Life Media (ALM) based in Toronto, Canada [7]. The incident was reported on the morning of July 12, 2015 when employees found changes in their home website with an unusual song playing in the background. The attackers stated their motive behind the breach after they released a few thousand user records. When the issue was ignored after the initial leak, a massive amount of 20 GBs of data were published. According to Time news, two Canadian law firms filed a \$578 million class-action lawsuit against the company as of result of the breach.

Consequently, people may choose to shop at traditional brick and mortar stores. Based on observation and statistical data, the last two months are the busiest time of the year for shoppers. As the holiday season rolls around, businesses have huge discounts to funnel shoppers to their stores to purchase gifts, decorations, and supplies to celebrate. In fact, one of the largest security breach happened during the 2013 holiday season. The victim of this massive breach, affecting 42 million people, was the Minneapolis based company, Target Corporation. According to the Washington Post, an estimated 42 million people who shopped in stores between Nov. 27 and Dec. 15 had their credit and debit card account information stolen. Later, Target revised the number of affected customers to 70 million. As of result, Target has agreed to pay 10 million dollars to settle a class-action lawsuit [8] and the total estimated expenses related to the data breach reached as high as \$252 million. [9]

In summary, these are a few major incidents reported within the last five years. Information technology, IT, and data security continues to be a relevant topic in current and future technology. In fact, the identify theft resource center reported the number of U.S. data breaches hit an all-time high of 1093 in 2016 – an increase of 40 percent over the previous year. [10]

Current Security Methods

This thesis is an applied research and targets a technical question seen in the corporate world rather than from an academic perspective. It is unrealistic for companies and businesses to

release proprietary information for academic research. With this limitation, the paper focuses on three fundamental security methods that are widely applied by businesses: authentication, encryption, access control.

Authentication

Authentication is perhaps the most popular and accepted level of security. Authentication is defined as the process of matching the provided credentials with user information stored on file. This information is organized inside a database that resides either on a local operating system or on cloud servers. In fact, cloud databases has become the standard for massive data storage. Current high-tech corporations like Google and Apple utilize the cloud to expand their businesses through applications like Gmail, Google Calendar, Google Hangout, Google Wallet, iCloud, iCloud Calendar, and Apple music as well as many service features including storage backup, synchronization of mail, contacts, and calendars between devices. The authentication process is crucial because it guarantees the information gathered associates with the right participant registered on the platform, that only authorized people are granted access to the data and tools, that only legitimate and protected devices are used and information can only be sent through authorized and approved channels [11]. By implementing these security policies, it adds significant pressure on companies to implement secured practices in order to safeguard client information. On the other hand, clients must hold themselves responsible in protecting their own identity by not sharing this information to the unwanted people.

As the topic of data security continues to grow through research, newer authentication methods have emerged. One of the popular practices of authentication is the *two-factor authentication*, also known as 2FA.

The idea of 2FA is to provide an extra layer of security that requires additional authentication besides password and username or email.

This second authentication often is something that only the client has in

their possession such as a device or piece of information that they know or have immediate access to, like a text via email, smartphone, or questionnaires answers. In a recent study, research conducted in King

Saud University on the

vulnerability of extracting private and confidential data from computer systems with removable massive storage devices. Within the research, they proposed an algorithm through verifying identification keys and directory paths that gets generated by a wired connection with the Information generated by the smartphone. Performing comparison of parameters before granting access. Their process is illustrated in figure 2. The outcome of their research protocol uses the user's name and password and the user's smartphone as the 2FA [12]. Furthermore, it uses a discrete logarithmic problem and forward hashing to protect the integrity of the exchanged message before providing user access to the storage devices. Today, 2FA with smartphone and questionnaire answers are widely popular in social media and banking. The most common form of verification is a digit code sent via text message or email. To add in extra security, the code expires after a fixed period. As research continues to develop in authentication, newer verification methods like spatial, time, current location, and biometric characteristics are being implemented.

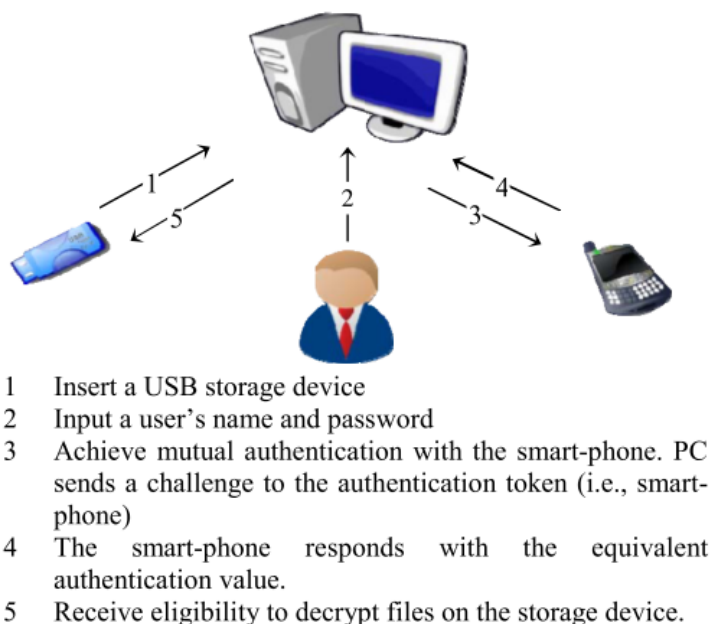


Figure 2 The Main Framework of Securing Mass Storage Devices with 2FA.

Encryption/Hashing

Encryption is considered the most effective technique in achieving data security. According to Cath Everett, an editor and journalist from “The Manager” expresses encryption technology as the central to the functioning of today’s global economy in the digital world. Every financial transaction over the internet, every website it opens, every email sent cannot be established without encryption technology. This technology plays a vital role because it ensures the integrity and confidentiality of data, safeguards privacy and enables organizations and consumers to conduct business in a networked economy [13]. Encryption happens with everything we do on the internet, Bluetooth data transmit, email send, text messages and more. As humans, we live in the world of encryption.

Data encryption is the concept of protecting data when users transport sensitive data to the cloud or other platforms. Chang Xue-zhou of Shijiazhuang Institute of Railway Technology defines encryption as the process of data transmission needs to effectively protected and controlled to prevent data loss and leakage. [14] The generic idea of the data encryption process shows in figure 3. The data is first encrypted with a public key generated by the recipient. Then it uses the key with encryption to convert the original data turns into ciphertext, also known as encrypted text. This special text is unreadable and impossible to interpret. On the receiving end, the system generates a private key with the decryption algorithm to retrieve back the original data. Doing so, encryption ensures to prevent data leakage and even if interceptor steals the data, it cannot be restored to its original content without the private key.

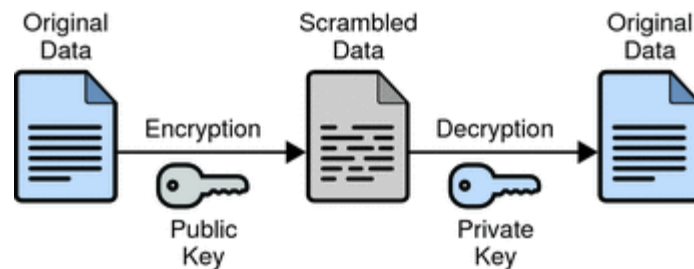


Figure 3 Encryption process flow

Similar to encryption, hashing is another fundamental technique used to provide password security. Hashing is converts something readable into a fixed length of mishmash characters. From a high-level security standpoint, the hashing is widely used on username (or email address) and password. The moment a user submits their information, it searches through the cloud server database for a matching username or email. If no match is found, an error will displayed. However, if a match is found, the login process proceeds to the next phase of

password encryption. The password goes through a hash function that scrambles the user's known password to jumbled mess of random characters. Then a comparison between the generated character string with the incomprehensible string hashed to the user inside the database. Again, access is only granted only if a matching result is found. Hashing techniques can also be applied to emails, phone numbers, dates of birth, credit cards, full name, and much more. The figure below illustrates how hashing fundamentally works with storing a password. It is widely used in the authentication process.



This is the same password

id	name	email	password
1	John Smith	john@somewhere.com	john856

id	name	email	password
1	John Smith	john@somewhere.com	ad65d5054042fda44ba3fdc97cee80c6

After encrypted "john856"

Figure 4 Password before and after hashing.

Access Control

Another common practice used to increase data security is Access Control, AC. According to Vincent and Rick of Cybertrust, AC policy is a set of rules that restrict which objects or people cannot access a source of data [15]. An example of AC is authorized badges to specific rooms in a building. From the confidentiality, integrity, privacy and security point of view, AC happens behind the scenes, and it is monitored by authorized IT professionals and coding experts who sets the AC requirements. The owner tailors the access rights of different users and provides means of specifying required credentials or bind attributes upon access. Doing this ensures the highest level of security and safety of data by restricting unauthorized access to sensitive data.

AC is commonly used with encryption. In a 2016 edition of the magazine *IEEE Access*, Abid discussed that encryption based techniques can be further divided into attribute based encryption (ABE), identity based encryption (IBE), and storage path encryption (SPE) [1]. ABE entails complex restriction attributes set by the data owner, and decryption may only occur upon satisfying all the defined access attributes. IBE focuses on the usage of human identifiers like an

email address or IP address as public keys to preserve the anonymity of transaction. SPE is separating a chunk of data into many sequential parts and storing them in different storage media owned by different cloud providers. The encryption happens on the storage path to the data as oppose of the actual data. The figure below illustrates the features and limitations to each of the encryption scheme with the utilization of AC.

Encryption scheme	Features	Limitations
Identity based encryption	<ul style="list-style-type: none"> Access control is based on the identity of a user Complete access over all resources 	<ul style="list-style-type: none"> Time consuming in large environment Granular access control is hard to implement Changing ciphertext receiver is not possible Data to be processed must be downloaded and decrypted
Attribute based encryption	<ul style="list-style-type: none"> Access control is based on user's attribute More secure and flexible as granular access control is possible 	<ul style="list-style-type: none"> Computational overhead in handling different user categories Updating ciphertext receiver is not possible Data to be processed must be downloaded and decrypted
Proxy re-encryption	<ul style="list-style-type: none"> Can be deployed in IBE or ABE scheme settings Updating Ciphertext receiver is possible 	<ul style="list-style-type: none"> Computational overhead Data to be processed must be downloaded and decrypted

Capstone Description

As mentioned previously, the motivation behind this topic comes from my Capstone project for the local business RapidMade. RapidMade specializes in revolutionary 3D printing technologies and allows clients to maximize the function of objects through delivering product in metals, plastics and full-color ceramics. The current platform has no automation and requires clients to enter order information upon each order. Furthermore, clients cannot track their previous orders or re-order anything without the hassle of filling out a new order form. With that being said, RapidMade proposed this capstone project to create an automated web portal that solves these inconveniences.

In our solution, my team and I considered safely storing confidential client information inside a cloud database. Some of the profile information includes first and last name, company name, phone number, state, email address, billing address, shipping address and shipping account number. In addition to storing and safeguarding clients' sensitive information, updating user profile information, allowing changing of passwords, auto filling client information in new order forms for returning users, guest checking out, and viewing past orders are also part of the deliverables.

Analzyation

Authentication

As discussed in the previous section, authentication is one of the project deliverables because the company wants a customer portal that stores personal information and the only way to accomplish this is inside a database. Therefore, it is necessary to apply the authentication technique to validate user's identity before providing access to the portal. Furthermore, authentication restricts unauthorized access to the database, so it provides a secured method to safeguard customer data. In order to safely protect client information, authentication is a top priority in the project.

Encryption/Hashing

Similar to the authentication method, encryption and hashing are important techniques for data security. By converting the user-known character string into an arbitrary ASCII string with the hash function or encryption algorithm, it prevents the user who monitors the database and attackers from knowing the credentials set by the clients. Both techniques are useful for manipulating any proprietary data that clients don't want outsiders to see, and it is widely applied on password and credit card information.

Furthermore, since both techniques aim to scramble readable information into unreadable random characters, even if personal information is stolen and disclosed, it remains incomprehensible unless decryption with private key or reverse hashing occurs before the leakage. Nevertheless, scrambling data is an important practice when considering data security.

Access Control

AC is a selective restriction of who can access the content inside a database. Every database has an owner and the owner permits privileged access for different users. If no user gets added to the database, it restricts all access to the database. In the case of *GoDaddy*, after a user gets added to the database the owner selects a list of privileges for that particular user. Under the manage user privileges page in the Control panel (Cpanel), there are 18 different privileges for a user to a database. They are Alter, Create, Create Temporary Tables, Delete, Event, Index, Lock tables, Select, Trigger, Alter Routine, Create Routine, Create View, Drop, Execute, Insert, References, Show View, and Update. Depending on the status of the user in a company, the owner has the

luxury to grant different privileges. In summary, AC helps monitor and manage the activities of a database by selective restriction of access.

Current Implementation

Given the deliverables and restrictions from RapidMade, the open source database my team chose was MySQL. The open source general purpose scripting language we used was Personal Home Page (PHP), which is designed for web development. The major benefit of using PHP is that it can be embedded inside Hyper Text Markup Language (HTML) and works perfectly with Cascade Style Sheet (CSS), which controls the layouts of the webpage. The open source management tool we chose to handle the administration of Structured Query Language (SQL) database is phpMyAdmin. PhpMyAdmin allows the web browser script to read user inputs to create, modify, or delete items within the database, as well as managing user permissions. The reason behind using open source tools is to keep the budget at a minimum and there are lots of resources to study and learn from to implement our design.

Combining PHP, HTML, and CSS, my team and I designed the script with RapidMade's theme in mind. Figure 5 shows a screenshot of the home page; it shows the options for users to login, register as a new customer, or place an order as a guest.

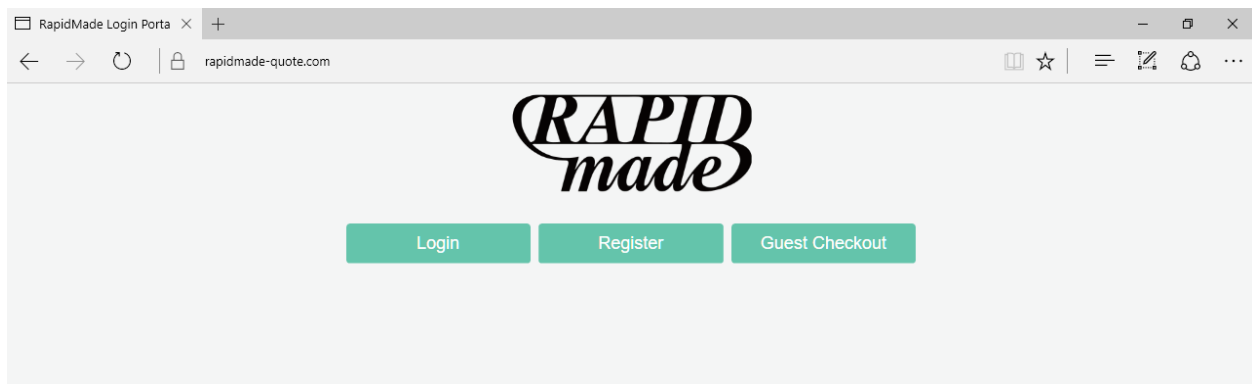
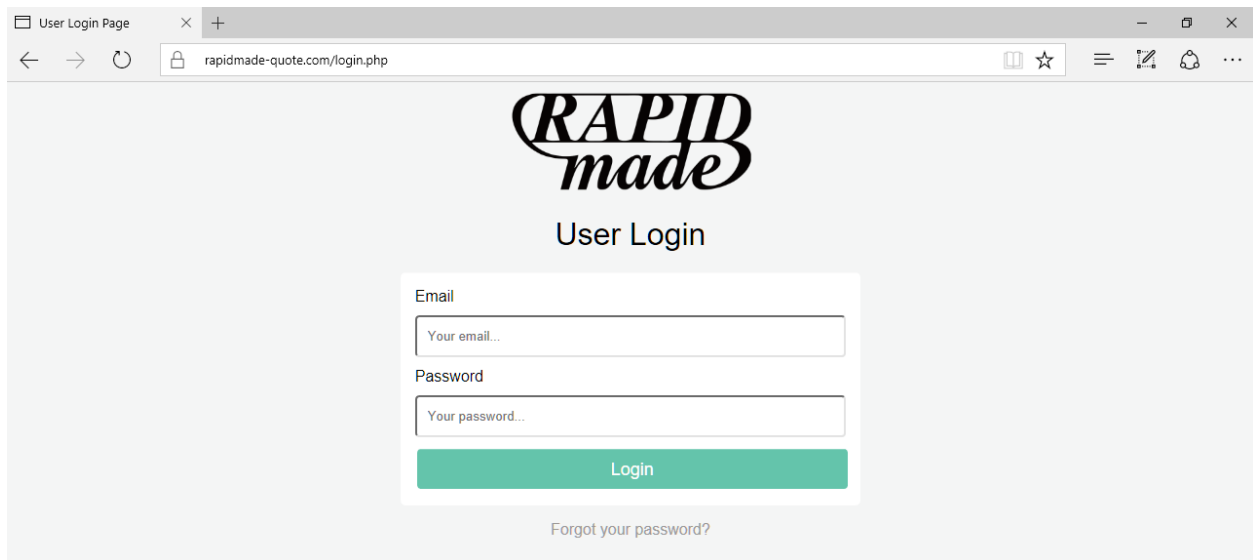


Figure 5 Current homepage with different user options.

When a user clicks on the login button, the website redirects him or her to the login script. A screenshot is shown in figure 6. Within the login script, the webpage prompts the user to sign in with their registered email and password. Similarly, the register page shown in figure 7 uses the same format to insert a new customer into RapidMade's database. However, additional

fields like first and last name, company name, phone number, billing address and shipping account number (if have one were) are added to meet the deliverable needs.



The screenshot shows a web browser window with the title 'User Login Page' and the address bar displaying 'rapidmade-quote.com/login.php'. The page content includes the 'RAPID made' logo, the heading 'User Login', and a login form. The form has two input fields: 'Email' with placeholder text 'Your email...' and 'Password' with placeholder text 'Your password...'. Below these fields is a green 'Login' button. At the bottom of the form area is a link that says 'Forgot your password?'.

Figure 6 Login page for returning users.

InPrivate Registration x + - □ x

← → ↻ | rapidmade-quote.com/register.php

RAPID
made

New User Registration

Email

li4@pdx.edu

Password

.....

Confirm password

.....

Company Name

PSU

First Name

Jelon

Last Name

Anderson

Phone Number

1234567890

Register

Already have an account? [Log in](#) | [Forgot your password?](#) | [Home](#)

Copyright © 2012-2017 RapidMade, Inc. All Rights Reserved.

2828 SW Kelly Ave, Suite B, Portland, OR 97201 | Tel: [503-943-2781](tel:503-943-2781) | Fax: 503-808-7894 | info@rapidmade.com

Figure 7 Register page for new users.

An additional feature my team implemented was after the registration form is submitted and before granting access. We designed an email verification step where we send an email to the registered email for validation. This confirms the identity of the user and legitimize the email address. Refer to figure 8.

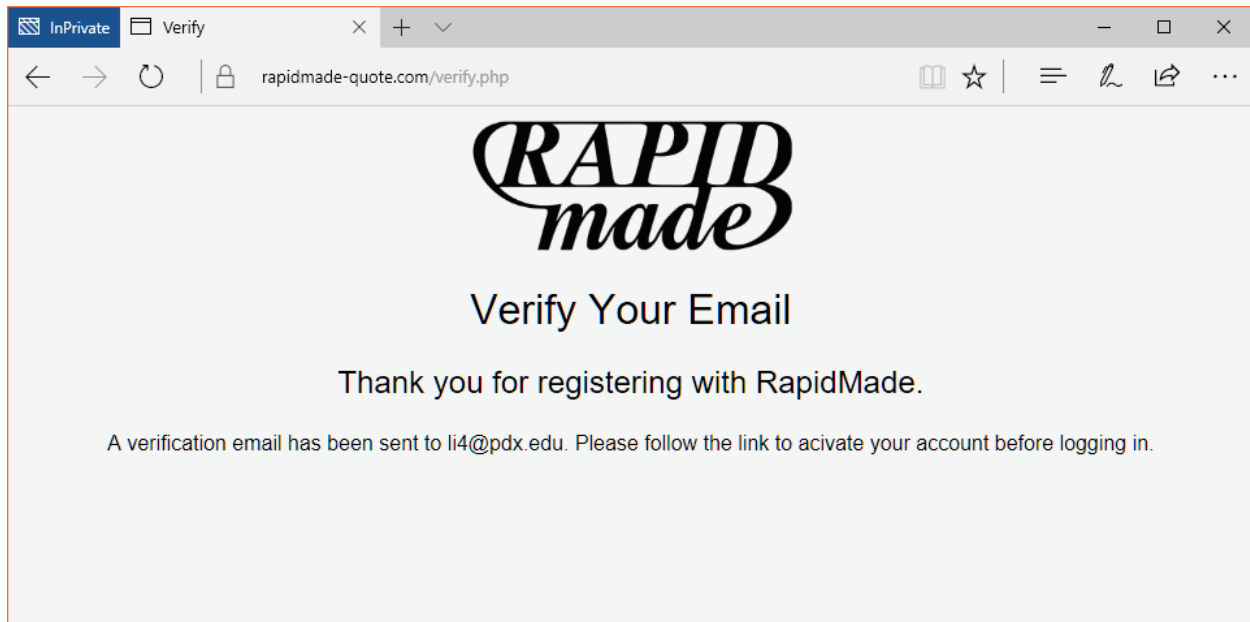


Figure 8 Email verification process after registration.

Using the hash function embedded inside PHP, we managed to convert the password string into an arbitrary ASCII string and stored that along with the associated user's email in the database. The exact method will not be disclosed due to a proprietary agreement, and it violates company confidentiality.

In addition to authentication with hashing, AC was also implemented in our work. RapidMade purchased a *GoDaddy* domain and my team set up the MySQL inside GoDaddy's Cpanel. One of the requirements for a database is adding privilege access to manage the database entries. This information is registered inside the PHP code and a connection is established when a user lands on the website. If the script contains invalid user information or if connected to the wrong database, network connection error occurs. In addition, admin access is also implemented in the design. Administrators of the company are redirected to a specially designed dashboard webpage with an admin privileges tab. This option allows administrators to permit or revoke admin privileges.

Another level of security that was purchased with the domain is Secure Sockets Layer, or SSL. This is a standard security technology for establishing an encrypted link between a web server and a browser. This protocol ensures that all the data being passed between the web server and the browsers remains private and integral. The purchase of the *GoDaddy* domain comes with a digital SSL certificate. The way to validate this security protocol is by examining a lock icon with the keyword *Secure* to the far left of the address bar.

Additional Security Suggestions

Given our current implementation of authentication, encryption and AC to increase further security, the following will be my recommendations:

- *Log audit.* Auditing enables IT professionals and code experts to determine if the security of the data directory has been compromised. An audit log helps monitor the behavior of the database by tracking timestamp, user login information, source and destination addresses, and files that were opened and more.
- *Audit failed login attempts.* Implementing this method ensures account safety by disabling accounts after a maximum number of failed login attempts. This prevents access until the account is re-enabled again.
- *Multi-Factor Authentication.* As discussed previously, 2FA method ensure maximal data protection by authenticating again via text message or email right after the initial authentication, or have the user answer security questions after the initial login.
- *Unique passwords with special characters.* By adding special characters as a requirement for passwords it increases the total number of passwords available.
- *Complex encryption algorithms/hash function.* The more complicated the encryption algorithm, the complex the decryption becomes. Hence, it results in better security.

Conclusion

In summary, data security is a prevalent topic in today's economy. As businesses migrate from brick and mortar to click and order, protection of personal information remains the highest priority. By increasing the level of security protection, it decreases the risk of publicizing confidential information which can save millions of dollars from lawsuits. On a smaller scale, RapidMade is a start-up firm wanting to bring convenience and better customer experience. My team utilized a SQL database with the phpMyAdmin management tool and scripting language PHP, HTML, and CSS to create a customer portal. Bring features like registering as a customer, logging in, checking out as guest, updating the user profile, updating the password, viewing past orders, submitting a reorder, and filling out a new order. Within our design, we also applied common security practices like authentication, encryption, and AC to safely protect client data. With the time frame we were given, my team deliver a working prototype after 6 months.

Considering the time constraint, additional security methods were suggested for the next step. All in all, my team and I had a positive experience and developed a solid webpage design and database knowledge that will be helpful in our future endeavors.

Reference

- [1] ABID MEHMOOD, IYNKARAN NATGUNANATHAN, YONG XIANG, , GUANG HUA, A. S. G. (2016). Protection of Big Data Privacy Protection of Big Data Privacy. *Access, Ieee*, 4(January), 1821–1834. <http://doi.org/10.1109/ACCESS.2016.2558446>
- [2] Bertino, E. (2016). Data Security and Privacy: Concepts, Approaches, and Research Directions. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 400–407. <http://doi.org/10.1109/COMPSAC.2016.89>
- [3] Internet Users. (n.d.). Retrieved May 20, 2017 from <http://www.internetlivestats.com/internet-users/>
- [4] Chaffey, D. (2017, April 27). Digital Marketing Megatrends 2017. Retrieved May 20, 2017, from <http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>
- [5] Uzunovic, A. (2016, July 11). Amazon Suffers Security Breach; 80,000 Login Credentials Leaked (Updated). Retrieved May 20, 2017, from <https://www.hackread.com/amazon-suffers-security-breach/>
- [6] Ehrenkranz, M. (2016, July 12). This Hacker Just Declared War on Amazon - But Now Your Personal Info Is at Risk. Retrieved May 20, 2017, from <https://mic.com/articles/148207/a-hacker-claims-to-have-leaked-80-000-amazon-users-passwords-and-personal-information#.mB4xIYL97>
- [7] Mansfield-Devine, S. (2015). The Ashley Madison affair. *Network Security*, 2015(9), 8–16. [http://doi.org/10.1016/S1353-4858\(15\)30080-5](http://doi.org/10.1016/S1353-4858(15)30080-5)
- [8] Yang, J. L., & Jayakumar, A. (2014, January 10). Target says up to 70 million more customers were hit by December data breach. Retrieved May 20, 2017, from https://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html?utm_term=.6470e983f5ba
- [9] Tabuchi, H. (2015, March 19). \$10 Million Settlement in Target Data Breach Gets Preliminary Approval. Retrieved May 20, 2017, from <https://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html>
- [10] Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout . (2017, January 19). Retrieved May 20, 2017, from <http://www.idtheftcenter.org/2016databreaches.html>
- [11] Puppala, M., He, T., Yu, X., Chen, S., Ogunti, R., & Wong, S. T. C. (2016). Data Security and Privacy Management in Healthcare Applications and Clinical Data Warehouse Environment, 5–8.
- [12] Eldefrawy, M. H., Khan, M. K., & Elkamchouchi, H. (2014). The use of two authentication factors to enhance the security of mass storage devices. *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New*

Generations, 196–200. <http://doi.org/10.1109/ITNG.2014.13>

[13] Everett, C. (2016). Should encryption software be banned? *Network Security*, 2016(8), 14–17. [http://doi.org/10.1016/S1353-4858\(16\)30078-2](http://doi.org/10.1016/S1353-4858(16)30078-2)

[14] Xue-Zhou, C. (2015). Network Data Encryption Strategy for Cloud Computing. *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, 693–697. <http://doi.org/10.1109/ICMTMA.2015.172>

[15] Hu, V. C., & Kuhn, R. (2016). Access Control Policy Verification, (C). <http://doi.org/10.1109/MC.2016.368>