TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

THAPATHALI CAMPUS

A Minor Project Proposal

On

Printing Through Smartphone with Secured Data Transfer

Submitted By:

Aarjan Ghimire (THA075BCT001)

Anish Poudel (THA075BCT008)

Niranjan Adhikari (THA075BCT029)

Submitted To:

Department of Electronics and Computer Engineering

Thapathali Campus

Kathmandu, Nepal

3rd January, 2022

ACKNOWLEDGEMENT

We would like to express our deepest appreciation to Associate Professor Er. Shanta Maharjan. And also we would like to express our gratitude equally to all the Faculty Members and whole Electronics and Computer department, Thapathali Campus, who continually and conveniently conveyed a spirit of adventure in regard to research and an excitement in regard to guiding to study as well as preparing this proposal. Without their guidance and persistent help this project would not have been possible. We owe a debt of gratitude to everybody directly or indirectly involved for bringing this proposal into limelight.

Aarjan Ghimire (THA075BCT001)

Anish Poudel (THA075BCT008)

Niranjan Adhikari (THA075BCT029)

ABSTRACT

The current solutions provided for transferring files while printing has been insecure and tedious at best. In our observation we have found that the documents required for printing has to change and this Project has been identified as a viable solution to this problem. As the average Nepali is not as tech savvy, we have concluded that a tool with simple and responsive user interface would be the best way to interact with the user. There is also a paramount need for security while handing the sensitive documents. So, this tool utilizes the industry standard SHA-256 and AES-256 to keep those files secured. The tool will also be available in open-source repos so that handles the transparency with which the files would be handled. This in turn guarantees user the sense of security. As the service is intended to be free to use and it has the potential to capture the currently non existing market for secure data transfer while using untrusted computers to handle their information.

Keywords: AES-256, application, database, Security, SHA-256

Table of Contents

List of Figures

List of Table

List of Abbreviations

AES	Advance Encryption Standard
API	Application Programming Interface
PHP	Hypertext Pre-processor
QR	Quick Response
SHA	Secured Hash Algorithm
UI	User Interface
URL	Uniform Resource Locator
US	United States

1 INTRODUCTION

Project was conceived as a solution to the problem that we have faced many times. The old solutions (link sharing provided by android and drive) that we used did not fulfill our need for minimal interaction and logging in untrusted computers which could be riddled with malwares made us uncomfortable and created our desire for a better solution that could fit our and similar needs of general public. We were able to do some research on how we may approach this problem and concluded that our expertise may run short while tacking a real-world problem as we had no experience regarding the matter. So, we decided it would be a good opportunity to tackle this problem with the help of our supportive teachers and the time provided for our minor project seemed enough to tackle this problem.

As it will have security embedded into every system that has potential to be exploited will be secured against such attacks. Some configurations of encryption model may arise some problems but as they are essential, we have decided to go the industry standard. We have learnt many topics in our course and we intend to utilize those courses while creating our data base and the interactions with said database will be done in php and c++ respectively.

1.1 Background

There were many times when we were frustrated with the available solutions when we searched the web for potential answers to our problem none of which were the perfect fit for the problem that we were facing. We landed on the conclusion of creating one ourselves and the timing could not be more desirable. So, creating this tool and providing it for free for all would entail removing the barrier as well as removing frustrations for other users. Most of the time spent on visiting Nepali Government offices have usually been on the side of collecting information which has to be printed and the steps will be reduced by implementing the solution that we have decided to provide. Managers can also request to print the documents using the printers in offices rather than print the document at home and risk forgetting them on their home which has been repeated more times than they would like to acknowledge. As we have faced the same problems even while presenting and creating presentations for the college

projects. These problems have created a perfect background for the creating of Project which has shown potential to reduce the time taken and the complexity of the problem.

1.2 Motivation

The difficulty faced by the common people in the Nepali society with transferring their documents for converting them to hardcopy should not go unnoticed since small effort from us can solve this problem. We as a responsible citizen working on the related field, we should try to solve this issue. This is the major motivation for this project.

1.3 Problem Definition

Transferring files to a random computer has always needs either a pre-existing connection, a physical connection or a file sharing service which requires tedious identification which has always required extra steps which could be mitigated if there was a solution just tailored towards this problem. Pre-existing connection seems impossible while printing in a random computer. File sharing service requires to be setup and documents shared this way have either almost unlimited lifespan on the web or they require extra steps to secure the file shared. Physical connection is not viable in those conditions where the user forgets the connectors or the connectors do not have port to be connected. So in regards to the above problems we have decided on certain objectives specified below.

1.4 Project Objective

The main aim of this project is to obtain hassle free and easy to use application for printing over internet. It is designed to meet following objectives:

- To achieve secure document transfer.
- To eliminate unnecessary steps for user to printing from their smartphone.

1.5 Project Scope and Application

Even though most of the documents are stored physically, we need them in printed form. And to print document, we have to send data to the printer. And for most user, they don’t have printer. So, for printing purpose we need to send data to the printer on

another network, thus we use internet. And mostly it is not easy for general user. Thus, this project is intended to use in this scenario.

Some use scenario are as follows:

1. Any printing shops or office space where document comes from customers.
2. Different Military and Governmental Organization due to high data protection.
3. Personal use as it has better user accessibility due to QR code, which is viable as no. of smartphone user is thrice as no. of PC user.
4. With slight modification of code, the variant of project may provide better and easy document sharing.

2 LITRATURE REVIEW

There has been some work on the field to transfer documents like Google provides google drive and some document sharing focused platforms such as MEGA. They while providing secure form of data transfer are tedious to setup on random machines using your own account as accounts of Gmail have been used to verify identities around the web. Some services which require less setup time is found at uploaded.net [1] which have shown better setup times and don't require you to fulfill identification but are less transparent and such services have shown to store your documents without encryption and there has been at times news of such websites stealing your documents and selling them to identity thief or charging them unfairly. And these services while there has also shown some complexity while using for just printing. So, a tailored solution has a potential to solve the problems with the existing solutions.

There have been many solutions to the document transferring process which would be not possible if not for the services such as Google Drive [2], MEGA [3] etc. These services do have solutions for transferring adequate data but to utilize those services you need to have basic computer knowledge which is extremely lacking in the majority of Nepali users.

Google has created custom encryption algorithms for better security and has created big data algorithms to handle large number of potential users. Without services like Gmail, Google Drive, Upload.net transferring data would have been a far more technical problem to the user than they can conceive solution for.

Existing services have shown large setup and repetitive steps for transferring documents and those services which have easy UI and smaller setup times have shown time and time again to be less secured and they have had large data breaches which has been a lasting problem. For security the US government has created SHA-256[4] algorithm for hashing information one way. For both encryption and decryption US government has also created AES-256[5] which has shown time and time again to be nearly impossible to hack.

3 METHODOLOGY

3.1 System block Diagram

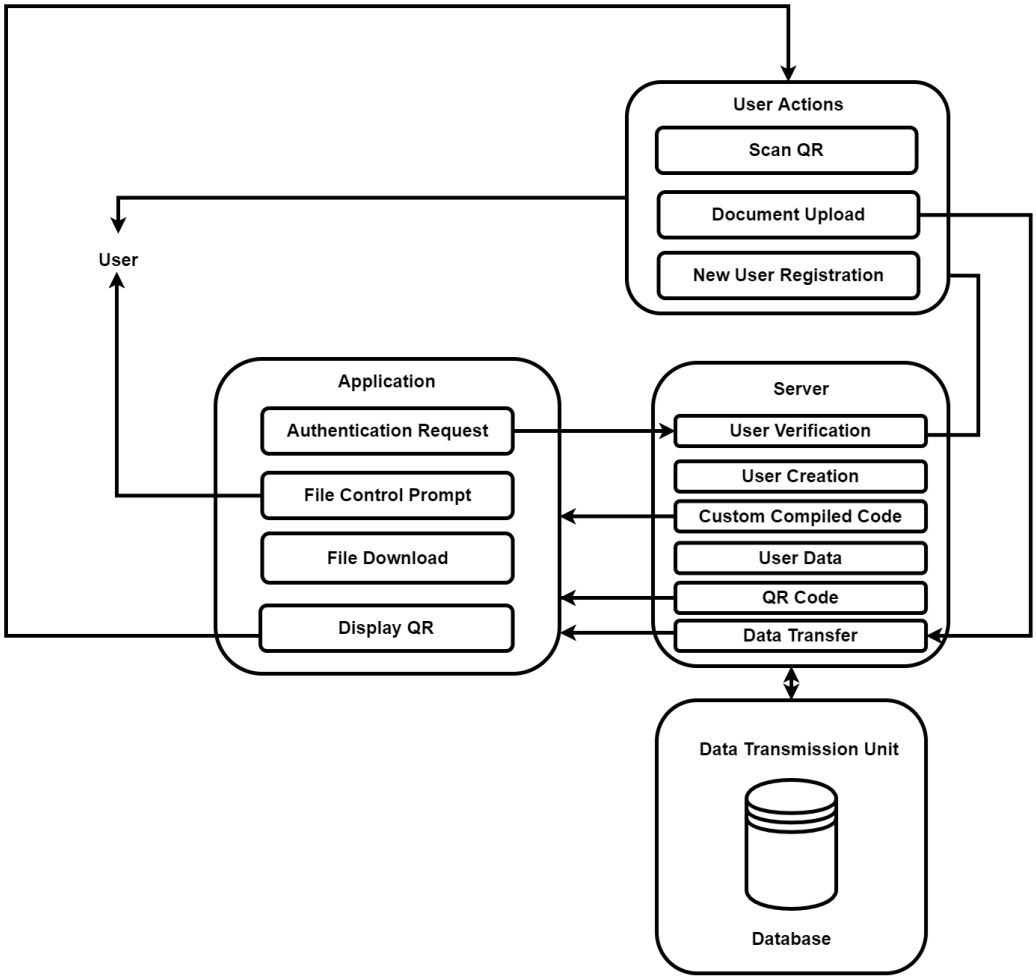

Fig 3.1 System Block Diagram

The entire system is mainly divided into 3 major components namely User, Server Computer. The first component (User) has the document which is required to be printed and the user scans the QR code which identifies the computer in which the file is indented to be sent. Database acquires the document and tracks it for the application. Then stores the data and sets the variable for data ready status. The application when it queries for data and its identification is authenticated and a secure key is passed. The application downloads the data and uses the key to decrypt the document which is promptly deleted after.

3.2 Working Principle

3.2.1 QR Display and Scan

A random identifier is generated when an application first starts by the server. It is then requested from the computer which hosts the application. The QR is then displayed which is then scanned by a phone. Which takes the phone to a custom URL with contains identifiers for the application. And the phone is prompted to upload the document which they intend to transmit to the application website.

3.2.2 Data Transmission

The data is first uploaded from the device and its name is stored in the database. The document is then sent to the server using post method. As it is more secure than get method. Its name is then encrypted and stored at the server in the directory custom created for this unique application. The application periodically requests if there are any document that are pending transmission for it. Then when the server acknowledges there to be document for that application a simple handshake is done to verify the authentication and then the document is transmitted with the accompanying key. The key is used to decrypt the document and then a prompt is shown to requesting the user's permission for printing the file and the printing prompt is then shown.

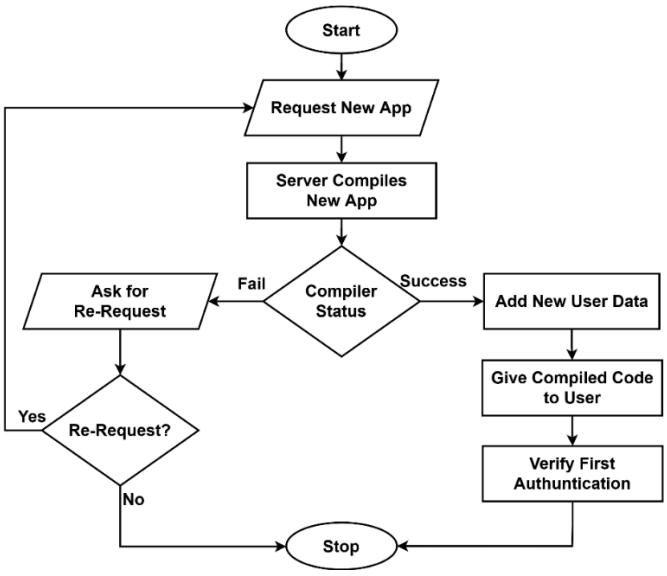

Fig 3.2 Initial Registration Flowchart

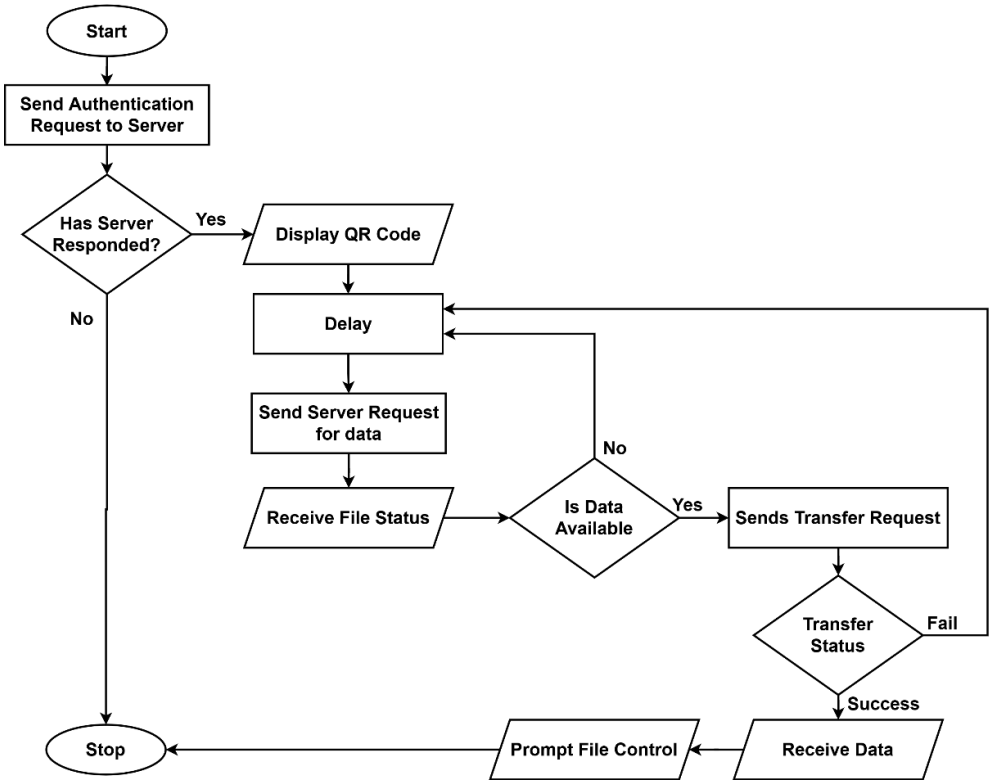

Fig 3.3 Basic Application Flowchart

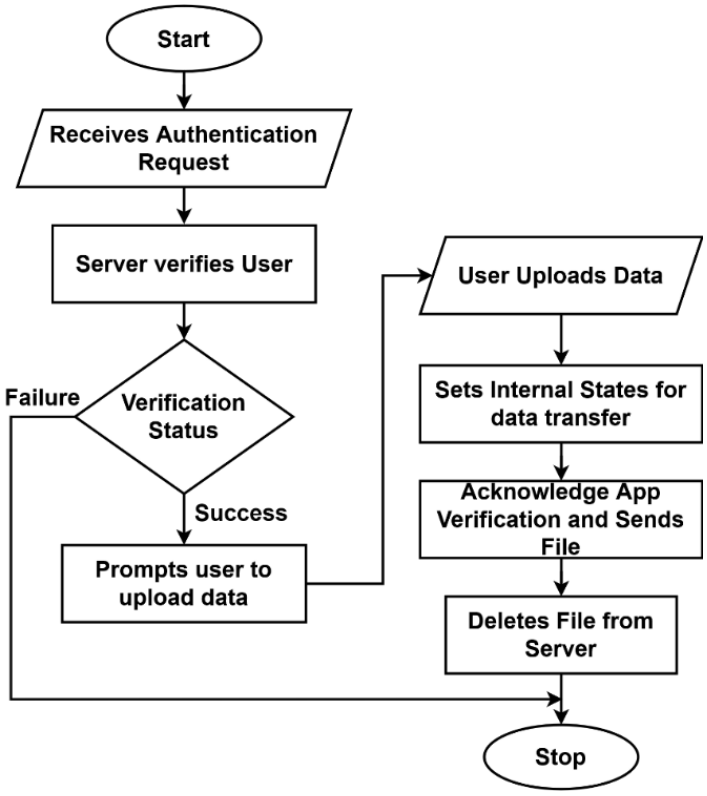

Fig 3.4 Server Flowchart

3.3 Description of Implementation tools

3.3.1 Hardware Requirement

Project does have some initial requirements as the application requires internet connection as computer and phone which have to communicate through a non-intrusive method. It is also apparent that you need a printer to print those documents. The computer that has to run the application has certain Hardware specification to match:

3.3.2 Software Requirement

The Application also requires a database for storing the data, verifying the data as well as authentication for an extra layer of security. And as is apparent you also need the application installed on your computer which requires a unique identifier as the server needs to keep the track of where the documents were intended to be sent. The mobile application also needs to have a browser with file access permission as the uploading step could not be completed without those files. The printer driver also needs to be present on the computer which fulfills the last step of the transferring process while printing.

3.3.2.1 C++

The application is mainly written in C++ so modifying the application requires a moderate level of C++ and Windows API knowledge.

3.3.2.2 PHP

PHP has been chosen as the language for the server side needs. PHP (recursive acronym for PHP: Hypertext Preprocessor) is widely- used open-source scripting language that is especially suited for web development and can be embedded into HTML. It is used primarily in our context for interaction with the database which in turn provides us with authentication features, file tracking and user tracking.

3.3.2.3 Python

Python has been chosen to complete some direct database manipulation through the Application and it has been concluded to be used in rarely used features which are limited by the network which will help us negate the slower running speed of the program.

4 EXPECTED OUTPUT

At the end of the project, we will be able to print the document over the internet. The end user will be able to use the project without technical knowledge and get rid of tedious work. The most of the steps will have been eliminated from the user and will be handled by the application. The security that was almost non-existent will be introduced as a form of extra layer of protection.

The user should feel comfortable and the process of printing the document will require much less input from the user which will entail saved time.

5 PROJECT SCHEDULE

To make the project in time, we need to make as best of our judgement for scheduling our project. As the steps we need are defined, we planned out the estimated time so that interlinked and routine processes are one after another along with overlapping time.

Table 5.1 Gantt Chart

Task Name	Dec 1-15	Dec 16-31	Jan 1-15	Jan 16-31	Feb 1-14	Feb 15-27
Planning						
Research						
Requirement Analysis						
System Configuration						
Coding						
Testing						
Validation						
Documentation						

6 PROJECT BUDGET

As per planned for this project, student access might be given to us by Azure platform which might be sufficient. But it case access is denied, we might have to purchase hosting and disk Space.

Table 6.1 Budget Estimation

S.N.	**Product**	**Cost (in NRs.)**
1	Hosting (FTP and Website)	1200.00
2	Disk Space	560.00
	Total	1760.00

References

[1] Cyando AG. *Store & share your files* [online]. Available: uploaded.net

[2] Google. (2012). *Cloud Storage for Work and Home* [online]. Available: https://www.google.com/drive

[3] MEGA Ltd. (2012, November 29). New Zealand, Available: https://mega.io

[4] National Institute of Standards and Technology (NIST). (2001). "Announcing Approval of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard" *The Daily Journal of United States Government* [online], vol. 180. issue 1. Available: https://www.federalregister.gov/documents/2002/08/26/02-21599/announcing-approval-of-federal-information-processing-standard-fips-180-2-secure-hash-standard-a

[5] V. Rijmen, J. Daemen, (2001 November) "Announcing the ADVANCED ENCRYPTION STANDARD (AES)". *Federal Information Processing Standards Publication* [online]. Vol. 197. Issue 1. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf