National College of Ireland

Two-layer security authentication system for a cloud application in order to decrease cyber attacks.

MSc Research Project
Cloud Computing

Nithish Narayana Dasa Aswartha
x21141762

School of Computing
National College of Ireland

Supervisor: Rashid Mijumbi

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Nithish Narayana Dasa Aswartha		
Student ID:	X21141762		
Programme:	Cloud Computing	**Year:**	2022
Module:	MSc Research Project		
Supervisor:	Rashid Mijumbi		
Submission Due Date:	15-12-2022		
Project Title:	Two-layer security authentication system for a cloud application in order to decrease cyber attacks.		
Word Count:	**5344**	**Page Count: 20**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Nithish Narayana Dasa Aswartha

Date: 15-12-2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Two-layer security authentication system for a cloud application in order to decrease cyber attacks

Nithish Narayana Dasa Aswartha
x21141762

Abstract

Thinking about Twenty-one-century life will involve data. It is modern gold, generated by people, systems, and organizations worldwide. Designs and patents, inventions, highly sensitive data, product and process concepts, and blueprints are all crucial to a company's success and must be protected. If product plans are leaked, a company's research and development may be wasted. It is bad for business when competitors can easily steal your years of work and use them to make similar, if not better, products at lower prices. In view of the physical and economic hazards of data breaches, even smaller IT companies prioritize client data protection. As a result of these vulnerabilities, hackers are able to launch a variety of attacks that wipe out data or prevent the system from functioning at all. Thus, this is the most important consideration in digital life. Therefore, doubling up on security measures lessens the likelihood of a system being compromised. In this research, I designed a two-layer security system in which each layer employs a unique security technique. In this model, two layers of security are used. Fingerprint login is used as the primary form of authentication in the first security layer. Facial recognition is utilized as a secondary authentication factor at the next level. Because of the increased difficulty for the attacker or hacker to gain access to the cloud web application, a two-level authentication method has been proposed. The key purpose for utilizing so many layers of authentication is so that if an attacker manages to break through one layer, the following layer will still keep the system secure. After successfully developing the authentication for the web application, I can see that only authorized users can log in to the web application, making your data safer and more secure.

1 Introduction

Security will be a key asset that needs to be taken care of in any organization. To guarantee user authentication, a variety of methods have been suggested and put to use. Being an open source, cloud computing is vulnerable to serious security breaches. Therefore, it is crucial to provide effective authentication methods so that users may access their resources. There are many encryption approaches, including symmetric and asymmetric encryption techniques, to close these gaps between users and cloud services. The two-level authentication method described in this paper includes some of the more common identifying factors, including Facial and Fingerprint recognition. A user username serves as an exclusive resource for

identifying him. Each username has a password that must be entered in order to authenticate the user's access to the system in the traditional method but in the proposal, we are using two-factor authentication of biometrics where all the data will be safest and more secure. The cloud system is susceptible to numerous security risks even though this level of security is mandated. Attacks can take many different forms, such as replay attacks, Man-in-the-middle attacks, and holding network traffic. For this research, we have taken two factors into consideration, such as Facial and Fingerprint recognition, and what attack can be done against which security measure. It has been assumed that these two layers of security give better authentication and ensures the reduction of security threats to the cloud system.
For example, Amazon Web Services (AWS) uses email address and password for user authentication. If a hacker is able to get beyond the authentication, they will be able to turn off all of the AWS services. Because of this, their clients will suffer greatly, and the company as a whole will suffer as well. I have developed robust authentication mechanisms for a web application that makes only authorized users can log into the web application using biometrics which is facial and fingerprint recognition. (K. Swedha and T. Dubey, 2018)

Biometrics have been the topic of many research publications, and their applications have been explored in a wide range of contexts, including smart attendance, airports, surveillance, locker access, and workplace entry. However, are not yet fully implemented for Cloud web applications. Additionally, In my research I have seen that researchers developed single authentication system for security purpose which is not safer in 20th century. So, I have developed two layer protection for our system in order to secure the data. Despite the fact that AWS now supports traditional methods of authentication, the username and password combination outlined above remains the primary means of identification. Nowadays, you can unlock your phone or a mobile app with just a glance or a fingerprint. However, biometrics aren't typically used for web apps traditionally, so I developed a Two-stage biometric security for web or cloud web applications this provides vast security for the users who is accessing the web application and also developed a mechanism to automatically logout for the users of their sessions after the time out. This adds an extra layer of protection for any users using the web application. In this web application development accuracy in matching users biometrics is better than others. (R. K. Kodali and R. V. Hemadri, 2021).

2 Research Question

To what extent will biometric authentication play a role in improving the safety of web applications or cloud web applications and why?

Cyberattacks are a potential cause of data loss. To prevent this, strong authentication of the cloud-based web application is required.
Two-factor authentication, such as face detection and fingertip verification, is proposed in this research as a means of bolstering cloud application security. These are trickier to break since the capability to record and reuse/reproduce facial and fingerprint patterns are not yet readily accessible to the general population. The solution will only allow authorized users to log in to cloud applications, increasing safety and security.

3 Literature Review

In their work "The three-level Multi factor authentication technique for cloud technology," Charanjeet Singh and Dr. Tripat Deep Singh proposed a secure, easy-to-use, and economical authentication approach. The suggested study is based on the premise that several factors and levels make an authentication scheme difficult to break and resistant to diverse attacks. This study proposes 3L-MFA, three types of multiple factor authentication. Out-of-band authentication protects against man-in-the-middle attacks. First-level login and password encryption uses double encryption. Level two Out-of-Band authentication uses email and contact number for OTP verification. Stage three monitors user system interaction on the graphical screen utilizing probability combinations of integers and double encryption with SHA-1 and AES128-CBC to track button clicks, picture clicks, and menu item selections. This paper helped create the proposal.(Charanjeet Singh, 2019).

This paper defines about finger-print and facial recognition pros and cons by the authors Rupinder Saini and Narinder Rana's in their paper "Contrast of Different Biometric Methods" which examines biometric technologies by listing their pros and cons.
Face, Iris, Fingerprint, Finger Vein, Voice, and lip are briefly introduced. The comparison criteria include accuracy, template size, pricing, security, and lengthy dependability (Rupinder Saini, 2014).

The authors, Mohammad Shabaz and Gaganpreet Kaur, propose a better one-way hash-and-nonce-based safer two-factor authentication that leverages login credentials like user IDs and OTP authentication but resists brute-force password attacks. cracking, MITM attacks, account/session hijacking, etc (Gaganpreet kaur, 2022)

The paper titles "Analysis of Web Authentication methods using Amazon Web Services" from the authors K. Swedha and T. Dubey explains about Due to its simplicity, many applications implement single sign-on.This improves usability and reduces redundancy. Thus, HTTP Basic and OTP-based authentication of the single set of user information is essential. HTTP Basic authentication is almost twice as fast as OTP.(K. Swedha and T. Dubey, 2018)

The paper titles "Attendance Management System" from the authors R. K. Kodali and R. V. Hemadri explians about This study evaluates and analyzes intelligent attendance-marking solutions. This study proposes a facial recognition-based attendance system. Face recognition in a chaotic classroom is done with a tiny, accurate strongly supervised network. User-friendly web apps are created. Amazon EC2 instances perform all analytics.

Understand cloud security issues to write this paper. "Cloud security difficulties and challenges: A survey" by Kakali Chatterjee and Ashish Singh covers cloud technologies, security issues, risks, and solutions. In 2017, the study examined the cloud architecture framework, cloud security concepts, threats, and assaults, and cloud security challenges (Kakali Chatterjee).

“Cyber-Attacks in Cloud Computing: A Case Study” by Jitendra Singh titled as “The International Journal of Electronics and Information Engineering” explains cloud cyberattacks. This paper helped them understand cloud-specific cyberattacks and improve their defenses (Singh, 2014). This article explains cloud security in greater detail. ENISA and

NIST, among many others, were formed to address cloud security concerns. These organizations' advice on cloud data security is helpful(Singh, 2014).

"Biometrics in the Cloud: Limitations and Research Activities" gives writers a new viewpoint on biometrics-as-a-service (BaaS). This article gives biometric data for cloud services for humans. Considering this concept, we could leverage cloud for all software to make it worldwide (Aniello Castiglione, 2017). However, providing BaaS requires overcoming many barriers. For instance, building a computing architecture that safeguards users' confidentiality and can manage robust and efficient biometrics fusion computation to enable scenario detection and obtaining in the cloud and auto-scaling algorithms that currently safeguard privacy is a research difficulty. Internet-connected smart devices like Internet of Things gadgets in smart homes and cities and smart apps like Android and iOS devices are also driving BaaS growth. Due to the growing volume of data kept on and accessible from such devices and the sophistication of cyber and cyber physical attacks, standard authentication and identification solutions like usernames and passwords need to be replaced.

The authors of "A unique method to improve multi-level security system employing fingerprint authentication in the cloud" (N. Jayapandian, A. M. J. Md. Zubair Rahman, M. Koushikaa, and S. Radhikadevi) propose a way to address the various security issues that have arisen due to the service and the idea of trying to implement fingerprints in the forthcoming models, which shows that the proposed schemes are both highly effective and provably reliable (N. Jayapandian, 2016).

S. Ziyad and S. Rehman proposed a report on cloud computing authentication trends and topics. This article discusses cloud computing trends. It helps us predict the future and suggests research that integrates cloud auth (Anon., 2014).

"User Authentication in Cloud Computing" by Hyokyung Chang and Euiin Choi states that cloud computing has security issues related to application security, access control, virtualization technology security, and availability of service, and massive traffic handling. User authentication requires high security.The paper briefly discusses authentication process and systems for access control and their difficulties (Hyokyung Chang, 2011).

"Two Factor Authentication for Cloud Computing" suggests employing a two-factor authentication framework to enforce mobile out-of-band (OOB) and Public Key Infrastructure (PKI) auth for cloud services. The study later concludes that the framework's security analysis resists fraud and replay assaults, prohibiting fraudulent clients from being used cloud services (Shirly Lee, 2010). Authentication verifies the user's identity before giving access to the basic services, ensuring that only legitimate people can use the program. Two-factor authentication uses two authentication methods to ensure the proper user gets access to a protected system or server. Two-factor authentication makes program access harder for unauthorized users. This research achieves its purpose by adding mobile OOB authentication to a PKI validation process during cloud user account setup.

A study of cloud security concerns dependent on user, system, and technical model is undertaken by Ghaffari et al. The survey identified cyber security challenges and addressed them to various groups, procedures, and technology to provide practical, feasible, and inexpensive security measures. Researchers review major cloud computing research. The PPT model's classification of cloud security issues and solutions followed. The proposed technique is then applied to categorise these issues. (Fariba Ghaffari, 2019).

"Understanding Cloud Computing Vulnerabilities" by Bernd Grobauer, Tobias Walloschek, and Elmar Stocker. The authors propose a safety cloud reference architecture, identify four aspects of cloud-specific problems, and demonstrate each design component with cloud-related flaws (Bernd Grobauer, 2011).

A mirror study by Chandini Kumari on cloud computing security threats and challenges found that new technologies like IoT and smart places have raised the likelihood of a cloud technology platform data breach. This study examined data security privacy and security issues. Discussing technology-classified data protections. The report suggests establishing a secure model and overcoming fundamental security issues for future research (Chandini Kumari, 2019).

"Secure Information in Cloud Employing Facial Recognition and Fingerprint" by Nitin Chauhan, Laxmi Ahuja, and Sunil Kumar Khatri claims that third parties can change, corrupt, delete, and grant access to our data. Cloud data security is critical. Thus, this study will address cloud computing data security using fingerprint and facial recognition technology (Nitin Chauhan, 2018).

Narng and Gupta examine cloud computing security issues. Cloud computing is risky, according to many. Cloud computing is risky since the service provider may not monitor or store data. In the paper, cloud computing issues are examined. Data security, confidentiality, and data issues are covered. In addition to security considerations, the paper reviews cloud infrastructure issues and challenges. The researcher argues that professional security standards should be developed and certified by outside parties to meet client needs and acquire their trust. Ashima Narang (2018).

Aditi Patel examined cloud security issues, threats, and attacks. As more firms use cloud technology, hackers exploit its flaws to steal sensitive data. Cloud service providers' new technologies create new vulnerabilities, the research concludes (Aditi Patel, 2020).

Santoso studied cloud technology vulnerabilities and cybercriminals. How might cloud migration affect security? This study addresses. This study's security requirements assessment can help corporations and other organizations transition from internal storage to cloud and reap its many benefits. 2019 (Santoso).

This article also emphasizes cloud services' security, which gives the impression of boundless resources because extra resources may be quickly accessed. This signifies the user won't see or control this component. Cloud service is sometimes called "virtual data center." Virtual computers run cloud computing. Cloud companies share virtual machine data with all clients, therefore a resource usually has numerous virtual machines. The supplier uses several virtual computers to fulfill a user's resource requirement. This allows numerous users to share hardware.

A paper examined cloud security issues and solutions. Four papers propose blockchain methods to solve cloud storage problems. Alatawi et al. explain the cloud system's design and important issues, teach readers about blockchain technology, and investigate the best blockchain approaches for cloud computing security (Alatawi, et al., 2020).

K Kushala and Shaylaja surveyed multi-cloud security trends. Cloud computing raises security risks for both customers and service providers. This paper discusses cloud technology (CC) and multi-cloud computing (MCC) detections, security challenges, and solutions. The researcher investigated each security technique, cloud type, and security risk (M V Kushala, 2020).

4 Research Methodology

Fingerprint Recognition:

The process of confirming someone's identification by matching their fingerprints to samples that have already been recorded, usually using a computer program in which the subject places a fingertip against a sensor to scan a fingerprint. This module follows a minutiae-based algorithm and fingerprint scanning consists of two stages: fingerprint identification and comparison. The user's fingerprints are required during registration. The software will evaluate the finger scans, construct a digit design derived from the conclusions of the analysis, then save the blueprint. Input from a sensor causes the system to generate a blueprint of the user's finger, which is then compared to the blueprints already stored in the system's digit libraries. The system does a one-to-one comparison between the live finger template and a blueprint defined in the Module for 1:1 matching, and a one-to-n comparison between the live finger template and all fingertip blueprints for the found finger in finding. In both circumstances, the system will produce the same conclusion, whether succeeded or fail.

Facial Recognition:

An individual's identification can be verified or established through the use of facial recognition. People in images, films, or in real-time can all be identified with the use of facial recognition technologies. It follows the Local Binary patterns algorithm to detect the faces.

Following these guidelines, we create a facial recognition module in the prototype:

Step 1: Collection of data

The first step in developing a machine learning system is accessing a publicly available dataset. It is necessary to have both the images and the accompanying captions. These descriptors have to come from a small pool of possibilities. Moreover, there needs to be roughly the same amount of samples across all categories of photography. Classifiers will be biased towards over-fitting into the most generally represented categories if there are twice as many similar images as there are unique images and five times as many different images as there are similar ones.
Class imbalance is a frequent problem in machine learning, and there are many approaches to addressing it.

Step 2: Divide the data

After that, we divide the data set in half.
(1) A set of lessons given in preparation for a specific task
(2) A battery of evaluations

The classifier "learns" the appearance of each category by making assumptions about the data input and then improving itself until the assumptions are wrong, using a training data set. After training a classifier, it may be tested on the test dataset to see how well it performed.
It's crucial to have separate and non-overlapping training and testing datasets. Since the classifier has already seen and "trained" from the testing examples if they are part of the training data, this is an unfair advantage. Therefore, the testing set is kept separate from the testing set and is used for the sole purpose of evaluating the performance of the network.

Step 3: Network training

Training is under underway utilizing the instructional set of images to educate the network. Our goal is to learn how to properly recognize each part of our labeled data. The software adapts and enhances itself when it makes mistakes. Typically, a gradient descent technique is used for this purpose.

Step 4: Evaluation

Now we can put the network is trained to the test. The testing set photographs must all be presented to the network so it can figure out what each image's label is. The model's predictions are then contrasted with the testing set's ground-truth labels. Image categories are reflected by the ground-truth labels. Classifier performance can then be measured through the use of collective statistics such as accuracy, recall, and f-measure, which are derived from the number of correct predictions made by the classifier.
In order to determine if a real person is logging into the system, this suggested framework employs a web camera to repeatedly check if the user's biometrics match those stored in the system at regular intervals.
A user's identity is confirmed during the login process through a verification step. While static techniques provide more secure user authentication than passwords alone, once a user has logged in, they cannot be tracked. The opposing point of view is that fingerprints are stored continuously throughout the encounter as part of a constant identifying system.
The user's keystrokes are tracked continuously during the loop, allowing for accurate analysis. If a user's fingerprints don't match their profile after the initial verification, they won't be able to log in.

The proposed research can help reduce the security flaws that afflict modern computer systems. Developers and users encounter a number of threats while attempting to authenticate users, including password cracking, shoulder surfing, guessing, spyware, brute force, and social engineering.
If an attacker can observe a user's typing pattern when they log in, they will have simple access to their password. There is no risk of shoulder surfing compromising the authentication process. Since the proposed study's fingerprint reader records authorized users' fingerprints every two minutes, even if an attacker performs shoulder surfing and steals the credentials, the intruder will not have complete access to the system. Using the saved identity, the scanner can confirm the user's identity.
Data-gathering software is known as "spyware." An adversary can compromise a user by planting spyware in their profile. However, this problem can be solved by the proposed research since, if no valid user logs in within 2 minutes, the computer locks itself.
Social engineering refers to the practice of manipulating users to get sensitive information. Social engineering is the only way for an attacker to gain the user's credentials, but the

system's continual verification of the user's fingerprints makes social engineering attacks impossible.
A brute-force attack is when an attacker tries every conceivable combination of characters in the password.
He uses techniques that perform this action to simplify matters. However, there is hope that the proposed study can help lessen the risk. The burglar can break the password, but the biometrics and fingerprint reader are secure. This ensures the system's security.

4.1 Architectural Design

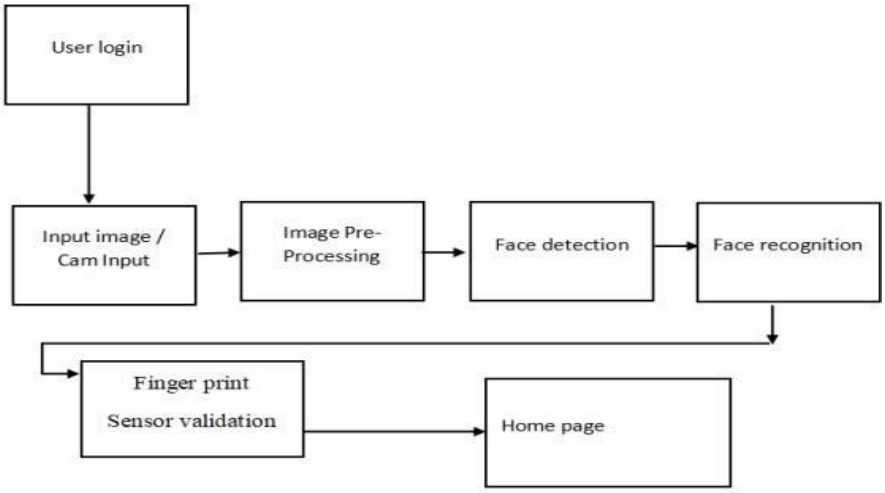

Figure 1: Architectural Design.

Application Working procedure:

The initial Procedure is to Sign Up. The user must provide a genuine name and other information during registration. Second, the system will request bio-metrics after the user has entered their information. Third, the bio-metrics are collected when the system verifies the entered information is correct. Both fingerprints and facial prints can be used for biometric authentication. In which the webcam is used for Facial recognition and the fingerprint sensor is used for Fingerprint recognition.
The collected information about an individual is now being kept in a database. As a result of this, biometrics can serve as a reliable authentication mechanism. The user can access the online application with a valid email id and fingerprints and faceprints after completing registration. After the information is given. In order to gain access to the application's data, the system first verifies the user's credentials against the database to ensure a proper match. A warning will appear if any of the information provided is incorrect.

4.2 Why Biometrics for security

Biometrics plays a vital role in security because they are always with us and they are hard to replicate, steal or hack. As biometrics uses physical characteristics from a user as a form of credential for verifying the identity of an individual and for security authentication.

Biometrics has a growing role in day today's security. The term biometrics actually means bio(life), and metrics (measurement). The physical traits of the individual such as fingerprint, facial recognition, the color of the hair, the color of the iris, signature, etc. Makes an individual stand out of the crowd. The biometrics latest technology takes the user's physiological behavior as input, verifies, and identifies the unique user.

4.3 Flowchart

The above diagram represents the flow of the application step by step. At first, the user will visit the web application through the specific URL to access the data.
If it is an old user, he/she doesn't have to sign up. If he/she is a new user and is visiting the web application for the first time, he/she will have to sign up for the biometrics that is for the user's fingerprint and facial recognition. Once both biometrics are completed successfully,the user can log in and access the web application. The old user he/she can directly sign in with biometrics and access the web application.

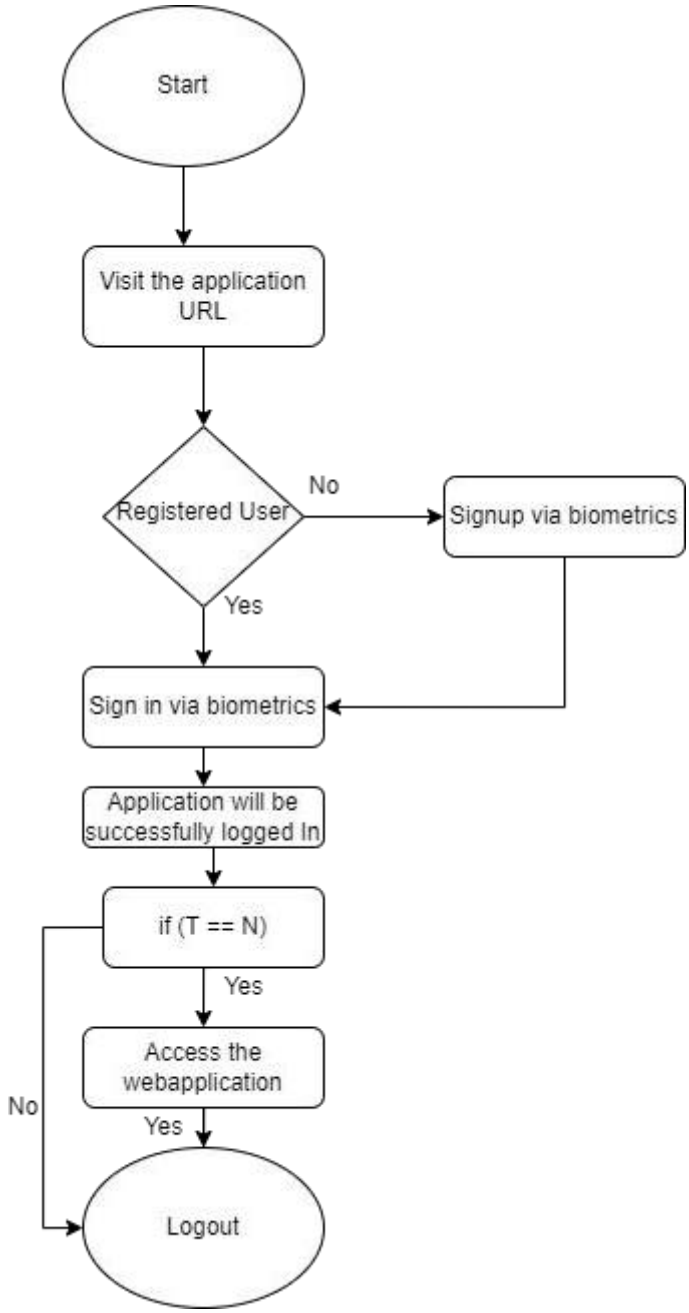

Figure 2: Flowchart

4.3 Sequence Diagram

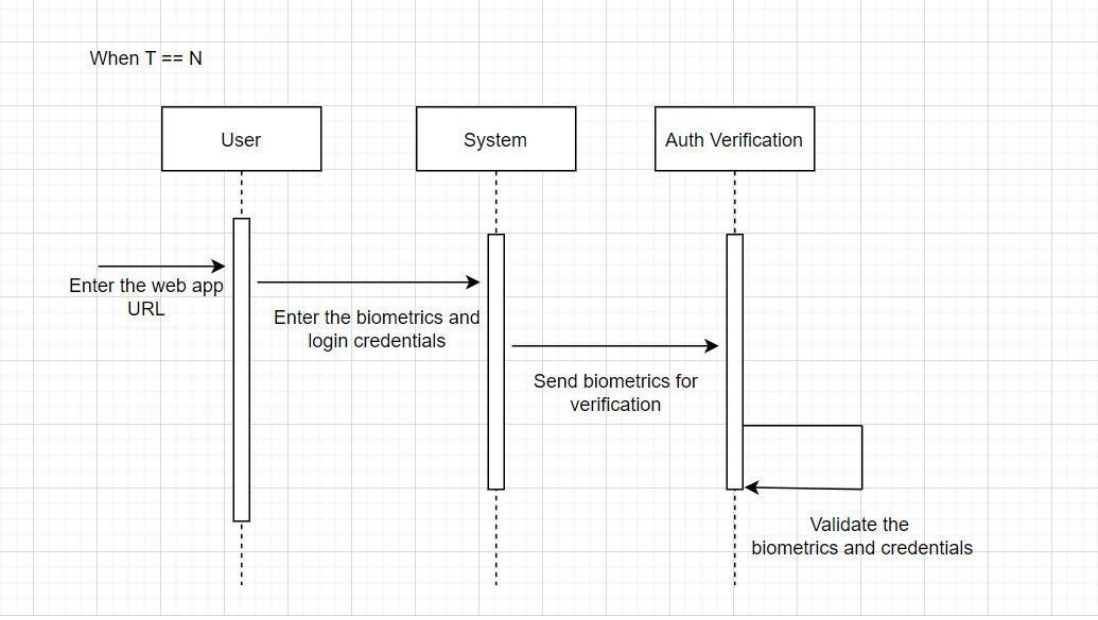

Figure 3: Sequence Diagram.

The above diagram depicts the sequence in which the process is carried out. Once the user navigates to the specific URL to access the data on the web application, the user has to provide the required information which is the user's biometrics, his fingerprint, and his face prints are captured and these biometrics are sent to the verification purpose with the biometrics of the user which is already restored during the signup process done at the beginning.
Once the authentication process is completed and the biometrics are verified, individuals will then be allowed to access the information on the web application. If the biometrics of the individual does not match, an error message will be displayed and access to the content on the web application will be denied.

5 Implementation

A fingerprint sensor and system web camera are used for biometric authentication in the prototype's hardware implementation.

5.1 Hardware Implementation

TTL (Time To Live) GT-521F32 fingerprint scanner was selected as the biometric sensor because of its small form factor and high processing speed.
The user's fingerprint is obtained using a four-step procedure involving scanning, extraction, pattern creation, and comparison. The most widely used fingerprint reader is an optical reader. Sensors made up of complementary metal oxide semiconductors convert reflected light into electrical signals. Electric currents flow differently along the finger as a result of the fingerprint's ridges and valleys. The ridges and valleys on each of its fingers provide an insulating barrier that slows down the reader's electric current.
After all of this information is recorded, a fingerprint scan is used to confirm the genuine user. In order to build a complete and accurate fingerprint picture of the person, the scanner frequently demands multiple scans from the same finger.

And the picture is attached for reference.

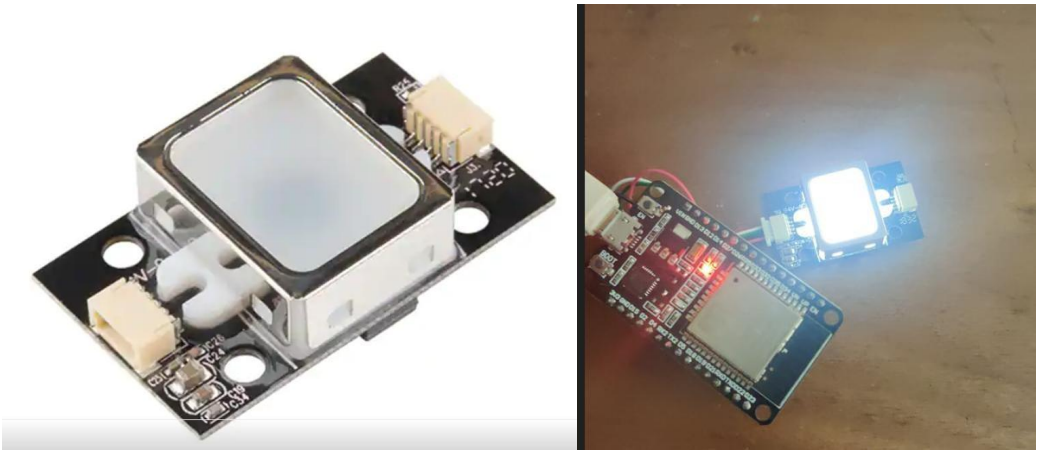

Figure 4: Fingerprint Sensor and Micro controller.

Web camera:

The Web camera module is used to capture a high-resolution photograph of the user's face for this research. Low-light face photography also makes use of a number of different libraries. The module has a five-megapixel web camera with a fixed focus that can record video at 1080p30, 720p60, and VGA90 resolutions, in addition to still images. It's a built-in part of the laptop itself.

Figure 5: Web Camera

5.2 Software Implementation

Arduino, Blynk, Visual Studio and below attached.

```
certifi==2022.9.24
charset-normalizer==2.1.1
click==8.1.3
colorama==0.4.6
Flask==2.2.2
idna==3.4
importlib-metadata==5.1.0
imutils==0.5.4
itsdangerous==2.1.2
Jinja2==3.1.2
MarkupSafe==2.1.1
numpy==1.21.6
opencv-contrib-python==4.5.1.48
opencv-python==4.5.1.48
Pillow==9.3.0
requests==2.28.1
typing-extensions==4.4.0
urllib3==1.26.13
Werkzeug==2.2.2
zipp==3.11.0
```

Figure 6: Software Dependencies.

6. Evaluation

The fingerprint and facial recognition multi-factor authentication prototype are successfully Implemented. A few experimental results are stated below.

6.1 Experiment 1: Face recognition

Whenever the user wants to log in to the application via webcam, the system recognizes the registered user successfully without fail.

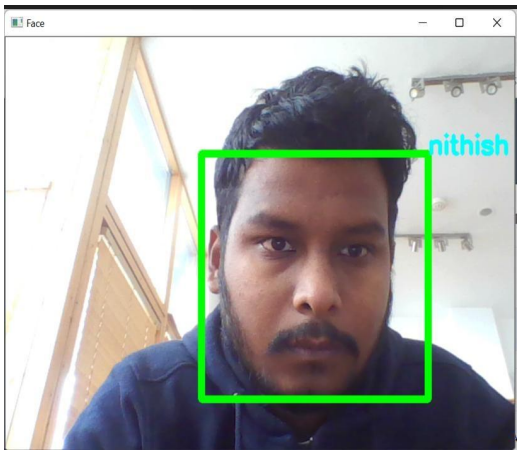

Figure 7: Face Recognition Experiment 1.

6.2 Experiment 2

The system can also recognize the registered user whenever the person is a little far from the system also.

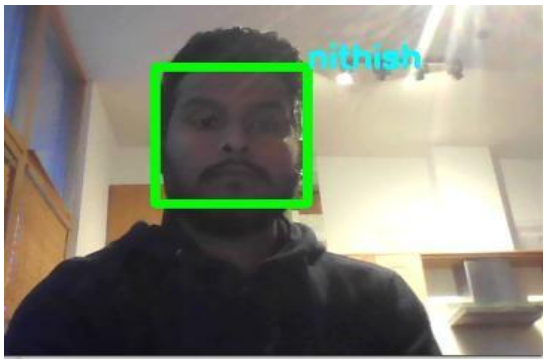

Figure 8: Face Recognition Experiment 2

6.3 Experiment 3

This prototype is incredibly powerful, however, it only recognizes when someone is facing the webcam. The system stops you from logging in when you place a selfie picture using a mobile device in front of a webcam. This prototype can detect liveness. When a genuine registered user is in front of the webcam, that is when it detects you.

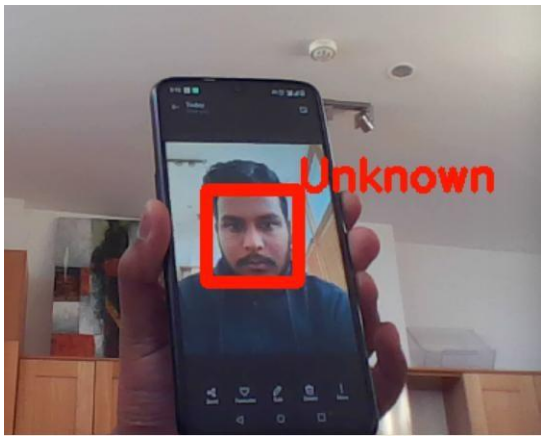

Figure 9: Face Recognition Experiment 3

6.4 Experiment 4

Coming back to fingerprint detection, whenever a finger is placed on the fingerprint sensor it will detect the registered finger within seconds and the accuracy is very good. When the system finds the match found it will display in the logs as 1.

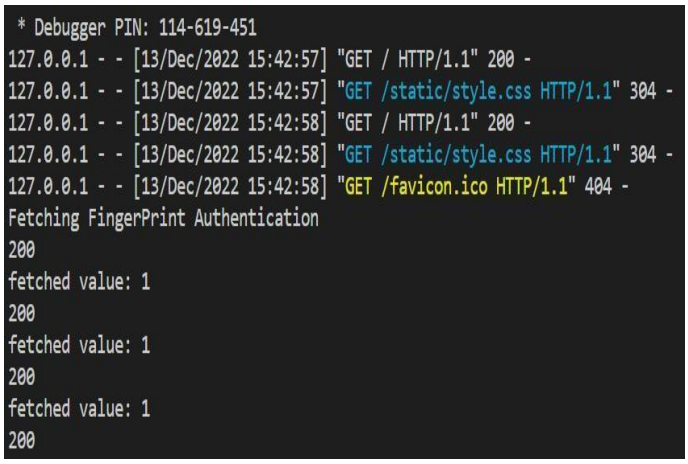

Figure 10: Fingerprint Recognition Experiment 4

6.5 Experiment 5

Whenever the wrong finger is placed on the reader it displays an error message as Unknown detected.

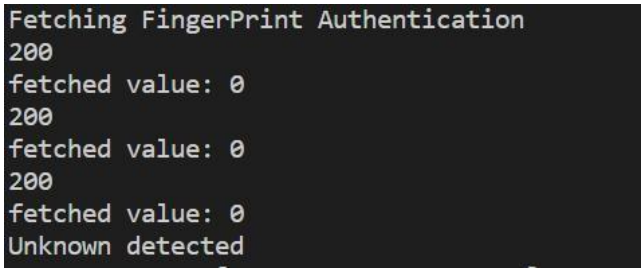

Figure 11: Fingerprint Recognition Experiment 5

6.6 Experiment 6

Loss and accuracy metrics for facial recognition on test and training data. As the Epoch value, i.e. the number of iterated photos, increases, the validation and training loss values decrease noticeably. R reduction in loss Despite this discrepancy, both the Training overall accuracy and the verification accuracy value have both increased and remained steady at 100%. This graph shows that the model has been trained to identify an authenticated user's true face.

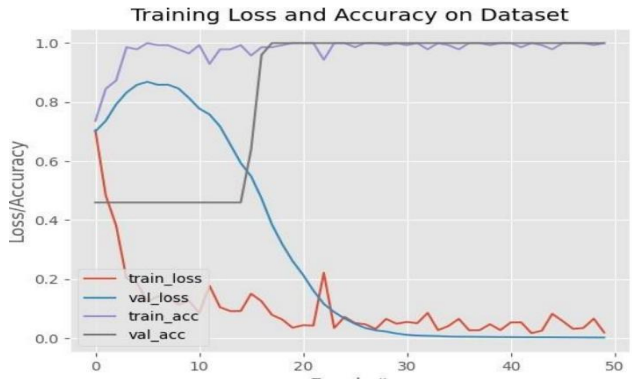

Figure 12: Graph

7 Discussion

The suggested study improves multi-factor authentication and performs constant user verification during the session. The old security systems relied on email and passwords, which are not a particularly secure method of authentication.
The research is hindered by the inability to integrate this paradigm into future devices without negatively impacting the user interface.
This framework can be adapted for use in a wide variety of additional scenarios, including data centres, security rooms, and cloud service logins (e.g., AWS, AZURE, etc.). Further development of the proposed study might involve the incorporation of a plethora of other biometric traits and the development of a system in which the user's every interaction with the system is logged and used to verify that the real user is in fact using the system. In the long run, additional work in this area can lead to more robust and secure systems.

8 Conclusion and Future Work

We may conclude that user verification is highly practicable due to its low implementation cost, high security, and protection. Biometric technology is a very sophisticated technological method with enormous potential. The usage of bio-metrics in modern software is expanding both steadily and rapidly. It also has a larger number of high-accuracy matches, which will be useful. The role in determining biometric legitimacy.
It holds a lot of potentials. According to the results of this research, biometric solutions offer significantly higher levels of security when it comes to protecting sensitive information. Full implementation of this prototype for cloud logins using current AWS services is possible in the future. Additional layers of security can be added to this system in the form of more stringent methods of identification, such as an iris scanner that would scan the user's iris (which is unique to each individual) to verify their identity and prevent impersonation. The recommended method was effectively implemented, and it will be an excellent fit for highly secure businesses.

References

K. Swedha and T. Dubey, "Analysis of Web Authentication Methods Using Amazon Web Services," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-6, doi: 10.1109/ICCCNT.2018.8494054.

R. K. Kodali and R. V. Hemadri, "Attendance Management System," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402659.

Aditi Patel, N. S. D. R. A. N., 2020. A detailed review of Cloud Security: Issues, Threats & Attacks. International Conference on Electronics, Communication and Aerospace Technology (ICECA).

Alatawi, S. et al., 2020. A Survey on Cloud Security Issues and Solution. International Conference on Computing and Information Technology (ICCIT-1441).

Aniello Castiglione, K.-K. R. C. M. N. F. N., 2017. Biometrics in the Cloud: Challenges and Research Opportunities. IEEE Cloud Computing, 4(4).

Anon., 2014. Critical Review of Authentication Mechanisms in Cloud. International Journal of Computer Science Issues (IJCSI), 11(3).

Ashima Narang, D. G., 2018. A Review on Different Security Issues and Challenges in Cloud Computing. International Conference on Computing, Power and Communication Technologies (GUCON).

Bernd Grobauer, T. W. E. S., 2011. Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy , 9(2).

Chandini Kumari, G. S. G. S. R. S. B., 2019. Security Issues and Challenges in Cloud Computing: A Mirror Review. International Conference on Computational Intelligence and Knowledge Economy (ICCIKE).

Charanjeet Singh, D. T. D. S., 2019. A 3-Level Multifactor Authentication Scheme for Cloud Computing. International Journal of Computer Engineering and Technology.

Farhan Bashir Shaikh, S. H., 2011. Security Threats in Cloud Computing. International Conference for Internet Technology and Secured Transactions.

Fariba Ghaffari, H. G. A. A., 2019. Cloud Security Issues Based on People, Process and Technology Model: A Survey. 2019 5th International Conference on Web Research (ICWR).

Gaganpreet kaur, M. S., 2022. A Secure Two-Factor Authentication Framework in Cloud Computing. Security and Communication Networks, p. 9.

Hyokyung Chang, E. C., 2011. User Authentication in Cloud Computing. s.l., International Conference on Ubiquitous Computing and Multimedia Applications.

Kakali Chatterjee, A. S., 2017. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications.

N. Jayapandian, A. M. J. M. Z. R. M. K. S. R., 2016. A novel approach to enhance multi level security system using encryption with fingerprint in cloud. World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Issue 10.1109/STARTUP.2016.7583903.

Nitin Chauhan, L. A. S. K. K., 2018. Secure Data in Cloud Computing Using Face Detection and Fingerprint. International Conference on Inventive Research in Computing Applications (ICIRCA).

Rupinder Saini, N. R., 2014. COMPARISON OF VARIOUS BIOMETRIC METHODS. International Journal of Advances in Science and Technology, 2(1).

Santoso, L. W., 2019. Cloud Technology: Opportunities for Cybercriminals and Security Challenges. International Conference on Ubi-Media Computing (Ubi-Media).

Shirly Lee, I. O. H. L. a. H. L., 2010. Two Factor Authentication for Cloud Computing. International Journal of Kimics, 8(4).

Singh, J., 2014. Cyber-Attacks in Cloud Computing: A Case Study. International Journal of Electronics and Information Engineering, Volume 1.