INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 995-1001

EYES AND PRINTS: A NEXT-GEN APPROACH TO CLOUD-BACKED SECURITY AND LAW ENFORCEMENT

Pranav Jejurkar[1], Aayush More[2], Durgesh Joshi[3], Prof. R.M. Shaikh[4]

[1,2,3]Computer Engineering Student, LoGMIEER, Nashik, India.

[4]H.O.D. , Asst. Professor, Computer Engineering Department, Lo GMIEER, Nashik, India.

DOI: https://www.doi.org/10.58257/IJPREMS33346

ABSTRACT

The proliferation of Internet of Things (IoT) devices has revolutionized the domain of security systems, offering innovative solutions for access control and surveillance. In this research paper, we present the development and deployment of a cloud-backed smart door lock system utilizing IoT devices, specifically the Raspberry Pi platform, integrated with Google Cloud Platform (GCP). The system incorporates biometric authentication, surveillance capabilities, and cloud-based storage to provide a comprehensive solution for access control and monitoring. Key components of the system include a Raspberry Pi Zero, R307 fingerprint scanner, Raspberry Pi Camera Module Rev 1.3, and a VGA to HDMI converter for interfacing with a monitor. Through Python programming language, the system facilitates fingerprint enrollment, verification, and image capture functionalities, ensuring seamless user interaction. Fingerprint data and captured images are securely stored in Google Cloud Storage, leveraging GCP's advanced security features and scalability.

This paper offers a detailed exploration of the hardware components, software architecture, and integration with cloud services, providing insights into the design principles, implementation challenges, and performance considerations of the smart door lock system. By elucidating the functionalities, features, and potential applications of the system, this research contributes to the advancement of IoT-based security technologies and inspires further innovation in the field.

Keywords: IoT-based Smart Door Locks, Biometric Authentication, Cloud-Based Security, Law Enforcement, Fingerprint Sensor, Raspberry Pi Zero.

1. INTRODUCTION

The rapid evolution of technology has led to significant advancements in security and access control systems, with the emergence of Internet of Things (IoT) devices offering innovative solutions for both residential and commercial applications.

Among these, the integration of IoT devices with cloud computing technologies has revolutionized the landscape of security systems, enabling the development of smarter, more efficient, and more connected solutions. This research paper aims to explore the development and implementation of a cloud-backed smart door lock system leveraging IoT devices, specifically the Raspberry Pi platform, in conjunction with Google Cloud Platform (GCP). By integrating biometric authentication, surveillance capabilities, and cloud-based storage, the system offers a comprehensive solution for access control and monitoring. The primary objective of this paper is to present a detailed overview of the design, development, and deployment of the smart door lock system.

This includes a comprehensive analysis of the hardware components used, the software architecture employed, and the integration with cloud services. Additionally, the paper will discuss the functionalities, features, and potential applications of the system, as well as its implications for security and privacy. Through this research, we aim to contribute to the body of knowledge surrounding IoT-based security systems, highlighting the potential of cloud-backed solutions in enhancing security, accessibility, and scalability. By providing insights into the design principles, implementation challenges, and performance considerations of the smart door lock system, this paper seeks to inspire further innovation and research in the field of IoT security technologies.

1.1. Motivation

The increasing need for robust security solutions in both residential and commercial environments has spurred interest in developing innovative access control systems. By leveraging the capabilities of IoT devices and affordable hardware platforms like Raspberry Pi, this research aims to address the demand for reliable and cost-effective security solutions. The integration of biometric authentication and surveillance functionalities in the proposed smart door lock system offers a compelling solution to enhance security and provide peace of mind to users. This research paper seeks to explore the feasibility and effectiveness of such systems while inspiring further advancements in the field of IoT-based security technologies.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 995-1001

2. LITERATURE SURVEY

2.1 Smart security system for door access based on unique authentication - K.Umamaheswari , P.Mahitha

Smart voice password and biometric based security system for door locking in smart homes:

A smart door locking system based on biometric and voice password unique identification, has been developed to enhance the security level of door access. This will provide access to only authorized persons. If an unauthorized person tries to intrude, the verification fails, and the buzzer will be activated with a beep sound and the owner will receive an alert message. The data of the people who tried to access the door will be stored.

2.2 A systematic review on Fingerprint based Biometric Authentication System - Hemalatha S

Real-time Fingerprint Recognition System:

In the process of analyzing fingerprint-based authentication systems, multiple works have been considered. The ultimate goal is to understand the needs of fingerprint-based recognition systems and study the merits, demerits and shortfalls of existing systems. It is understood that biometric templates like fingerprints are highly robust and reliable for the purpose of authentication when compared with passwords, PINs, or highly stuffed keys. It is also noted that there exists a significant difference between the fingerprint-samples of a single person captured at different occasions. Thus, the comparison task is a probabilistic one which is really a vice versa of strict matching of passwords or keys.

2.4 A Real-Time Face Detection Method Based on Blink Detection - Hui Qi, Chenxu Wu, Ying Shi, Xiaobo Qi, Kaige Duan, And Xiaobin Wang

Real-Time Video Face Recognition:

This paper proposes a real-time face detection method based on blink detection called LBAS_Resnet50 to solve the problems of illumination and expression changes in the process of real-time face recognition. The model takes ResNet50 as the basic network structure and sends the texture features extracted by the LBP algorithm into the basic network to improve the tolerance to illumination in the recognition process. Then by adding BiLSTM to obtain context information, it is convenient to extract time series features, to improve the accuracy of real-time recognition. At the same time, the channel attention mechanism is added to extract key feature information and assign important weights, and SPP pooling is used to improve the robustness of the model. Finally, the real face is judged by eye blink detection. The experimental results indicate that the method proposed in this paper has a good effect on the accuracy of anti-spoofing real-time face recognition. Due to the different structures of paper, electronic device screens and real faces, the facial images acquired by cameras differ in brightness and illumination information. In the next research, we will consider efficiently separating brightness and reflected light features from RGB images to further improve model performance. In addition, we will consider applying sparse representation to deep learning based on face recognition.

2.5 Surveillance System for Real-Time High-Precision Recognition of Criminal Faces from Wild Videos - Hyun-Bin Kim, Nakhoon Choi, Hye-Jeong Kwon, And Heeyoul Kim

Crime Prevention Using Computer Vision:

The proposed system analyzes video footage captured by surveillance cameras in real-time. By using a method that iteratively detects and identifies faces in each frame, the footage can be analyzed immediately without storing it. By proposing a face recognition method that uses down-sampling to identify face positions and utilizes them in the original quality image, the performance of face detection and identification can be improved on the same hardware to enable real-time detection.

It contributes to improving the precision of object tracking by storing the location of the detected face in the video and the identification information predicted by the system. The face tracking ID unit also compensates for the problems of the prediction unit when performing face recognition in video data. The face tracking ID unit minimizes the prediction flipping problem caused by the congested embedding problem due to the large size of the embedding DB through the identification score accumulation method. The threshold value used in the identification score accumulation method was detected through experiments to find the optimal threshold. In addition, a data set was created for evaluation and measurement in the overall experiment. Since the proposed system uses the input and output formats of common face detection and identification systems, it ensures freedom of tuning, which allows practical users to easily apply different models suitable for specific domains.

This is evidenced by the improvement in accuracy and F-1 score during migration in the experiments according to the identification method. In addition, two parameters can be utilized to derive the final score for the tracked object, allowing a high precision or recall being selected. In our experiments, we obtained an accuracy of 0.900 and an F-1 score of 0.943 for ($\alpha = 4.5$, $\beta = 15$).

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 995-1001

2.6 A Novel Front Door Security (FDS) Algorithm Using GoogleNet-BiLSTM Hybridization - Luiz Paulo Oliveira Paula, Md. Whaiduzzaman, Nuruzzaman Faruqui, Imran Mahmud, (Senior Member, IEEE), Eric Charles Hawkinson, And Sandeep Trivedi ,(Senior Member, IEEE)

Front Door Security Algorithm using Human Activity Recognition:

The research paper presents an innovative automatic Front Door Security (FDS) algorithm using Human Activity Recognition (HAR) to detect security threats at the front door from a real-time video feed with 73.18% accuracy. The FDS algorithm uses an innovative combination of GoogleNet- BiLSTM hybrid network to classify activities, such as attempts to break the door by kicking, punching, or hitting, as well as gun violence. The paper discusses the design of the hybrid network, the selection and processing of the video data set, and the training of the LSTM network. It also presents the experimental results and performance evaluation of the proposed algorithm, demonstrating its potential for ensuring better safety with 71.49% precision, 68.2% recall, and an F1- score of 0.65. The paper also discusses the application of AI technology in strengthening front-door security and highlights the significance of applying AI in physical security. Additionally, the limitations and future scope of the proposed system are discussed, with the authors emphasizing the need for further research to improve the system's service quality and robustness. Overall, the paper showcases the potential of the FDS algorithm in providing an automatic and intelligent security system for front doors at an affordable cost.

2.7 When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark - Zhizhong Huang, Graduate Student Member, IEEE, Junping Zhang, Senior Member, IEEE, and Hongming Shan, Senior Member, IEEE

Introduction to MTLFace:

The research paper proposes a unified, multi-task learning framework called MTLFace for age-invariant face recognition (AIFR) and face age synthesis (FAS). The framework includes attention-based feature decomposition to separate identity- and age-related features, and a novel identity conditional module for achieving identity-level FAS with improved age smoothness. The proposed MTLFace is evaluated on benchmark cross-age datasets and demonstrates superior performance compared to state-of-the-art methods for both AIFR and FAS. Additionally, the paper introduces a new large cross-age face dataset for tracing long-missing children and a new benchmark dataset called ECAF. The experimental results on these datasets show that MTLFace outperforms existing state-of-the-art methods for AIFR and FAS and achieves competitive performance for general face recognition. The framework also includes a selective fine-tuning strategy to further boost AIFR by automatically selecting high-quality synthesized faces from FAS for fine-tuning. Overall, the proposed MTLFace shows strong generalization ability and effectiveness in addressing the challenges of age-invariant face recognition and face age synthesis.

MTL Face Framework and Features:

The research paper introduces MTLFace, a multi-task framework for age-invariant face recognition (AIFR) and face age synthesis (FAS). It addresses the lack of visual results for AIFR and compromised recognition due to artifacts in FAS. MTLFace utilizes attention-based feature decomposition and an identity conditional module for identity-level FAS. Additionally, it presents a large cross-age face dataset and a benchmark for tracing long-missing children. Experimental results demonstrate MTLFace outperforms state-of-the-art methods for AIFR and FAS. MTLFace achieves continuous face age synthesis using a StyleGAN-based architecture and maintains stable training by employing perceptual image patch similarity (LPIPS) loss. While MTLFace improves discrimination of the face recognition model for face rejuvenation, it faces challenges in face aging due to ghost artifacts. The paper acknowledges limitations and discusses solutions for improving background preservation in face age synthesis. Overall, MTLFace shows significant advancements in AIFR and FAS tasks.

2.7 Finger Vein Recognition Based on Anatomical Features of Vein Patterns - Arya Krishnan and Tony Thomas

Finger Vein Recognition Based on Anatomical Features and FEBA Representation:

The research paper presents a new approach to finger vein recognition based on distinct anatomical vein patterns. It introduces a feature representation method using a 6 × 6 feature matrix derived from identifying six vein patterns (F1F2EB1B2A) through anatomical analysis. The proposed method offers template security and invariance to scaling, translation, and rotation changes. Experimental results showcase superior recognition performance, with an EER around 0.02% and an average recognition accuracy of 98%, compared to existing approaches. The proposed method outperforms existing methods, as shown in a comprehensive evaluation using HKPU, SDUMLA, and in-house datasets. The new approach demonstrates robustness to rotation, scaling, and translation, presenting promising results

for finger vein recognition. The paper suggests future research directions to improve the feature representation by incorporating more pattern-based features and adding more sub-patterns to the fundamental F2EB2A pattern.

2.8 Multimodal Finger Recognition Based on Asymmetric Networks with Fused Similarity - Yiwei Huang, Hui Ma, And Mingyang Wang

A Multimodal Approach Using Attention Mechanisms and Fusion Networks:

The research paper proposes an end-to-end multimodal finger recognition model that integrates attention mechanisms into a similarity-aware encoder to address the limitations of existing biometric fusion methods in dealing with correlations and redundancy of multimodal features. The paper introduces a finger asymmetric backbone network (FAB-Net) for extracting intra-modal features and a novel attention-based encoder fusion network (AEF-Net) with channel attention to improve performance in multimodal biometric systems. The effectiveness of the proposed method is validated through recognition experiments on three multimodal finger databases, demonstrating its ability to generate more discriminative common representations and achieve advanced recognition accuracy. The paper provides insights into the importance of considering the correlation and redundancy of multimodal information and demonstrates the potential of the proposed approach for improving multimodal biometric recognition.

2.9 Invisible Adversarial Attacks on Deep Learning-Based Face Recognition Models - Chih-Yang Lin, (Senior Member, IEEE), Feng-Jie Chen, Hui-Fuang Ng, (Member, IEEE), and Wei-Yang Lin (Member, IEEE)

Mask generation method based on facial landmark detection and super-pixel segmentation:

The paper proposes a method for generating imperceptible adversarial face images based on facial landmark detection and super-pixel segmentation. The paper highlights the vulnerabilities of existing face recognition systems to adversarial attacks. The proposed method involves extracting facial landmarks, segmenting super-pixels, and inserting adversarial noise within the masked areas. Experimental results demonstrate the success of the proposed method in fooling face recognition systems in real-world scenarios. The study utilizes performance metrics such as Attack Success Rate (ASR) and Structural Similarity Index Measure (SSIM) to evaluate the effectiveness of the proposed method. The results show that the proposed method can generate imperceptible adversarial samples with high SSIM values and maintain attack success in real-world scenarios, such as when captured by a camera or subjected to different lighting conditions and camera viewing angles. The proposed method is shown to be effective against various face recognition models and robust against different adversarial defense mechanisms.

3. EXISTING SYSTEM

The existing system for access control and surveillance typically relies on traditional mechanisms such as mechanical locks, keypads, or card-based entry systems. While these systems serve the fundamental purpose of securing premises, they often lack advanced features and integration capabilities seen in modern IoT-based solutions.

3.1 Mechanical Locks:

- Mechanical locks are the most basic form of access control, relying on physical keys to grant entry.
- While simple and widely used, mechanical locks offer limited security features and are susceptible to lock picking and unauthorized duplication of keys.
- They lack the ability to provide detailed access logs or real-time monitoring of entry points.

3.2 Keypad Entry Systems:

- Keypad entry systems allow users to enter a numerical code to gain access to a secured area.
- These systems offer a higher level of security compared to mechanical locks as they require a unique code for entry.
- However, they are still vulnerable to code guessing and unauthorized access if the code is compromised.

3.3 Card-Based Entry Systems:

- Card-based entry systems utilize RFID or smart cards to grant access to authorized users.
- Users present their card to a reader, which verifies the card's credentials and grants entry if authorized.
- While more secure than mechanical locks and keypad systems, card-based entry systems require the issuance and management of physical cards, which can be cumbersome and costly.

3.4 Surveillance Systems:

- Surveillance systems typically consist of CCTV cameras placed strategically to monitor entry points and other areas of interest.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 995-1001

- These systems provide a passive means of monitoring and recording activities but do not offer active access control features.
- Footage from surveillance cameras can be reviewed after an event has occurred but does not prevent unauthorized access in real-time.

While these existing systems serve their intended purposes, they often lack integration with modern technologies and advanced features such as biometric authentication and real-time monitoring. The proposed smart door lock system aims to bridge this gap by leveraging IoT devices and biometric authentication to create a more secure and efficient access control solution.

4. PROPOSED SYSTEM

The proposed system aims to develop a cloud-backed smart door lock solution that leverages Internet of Things (IoT) devices, specifically utilizing the Raspberry Pi platform integrated with Google Cloud Platform (GCP). The system will offer advanced access control and surveillance functionalities, enhancing security and providing real-time monitoring capabilities.

Key features of the proposed system include:

A. Biometric Authentication: The system will incorporate fingerprint recognition technology using the R307 fingerprint scanner, allowing authorized users to gain access to the premises securely.

B. Surveillance Capabilities: A Raspberry Pi Camera Module Rev 1.3 will be utilized for real-time image capture, enabling users to monitor activity at the door remotely.

C. Cloud-Based Storage: Fingerprint data and captured images will be securely stored in Google Cloud Storage, ensuring data integrity, availability, and scalability. GCP's advanced security features, such as encryption and access controls, will be employed to protect the stored data.

D. User Interface: The system will feature a user-friendly interface implemented using Python programming language, allowing users to enroll fingerprints, verify identities, and view surveillance footage.

E. Integration with Cloud Services: The proposed system will leverage various GCP services, such as Cloud Functions, Cloud Pub/Sub, and Cloud Vision API, for advanced data processing, analysis, and automation.

Overall, the proposed system offers a comprehensive solution for access control and surveillance, combining the power of IoT devices with cloud computing technologies to enhance security, accessibility, and scalability. Through this research, we aim to demonstrate the feasibility and effectiveness of such systems while inspiring further advancements in the field of IoT-based security solutions.

5. SYSTEM ARCHITECTURE

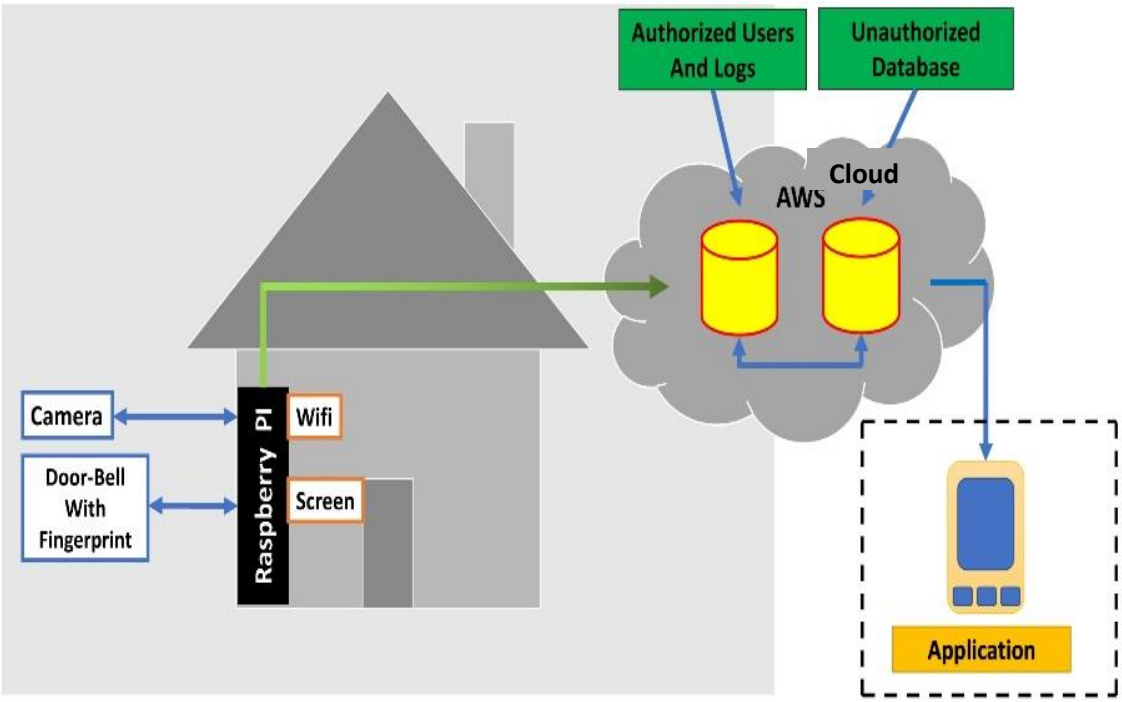

Figure 1: System Architecture.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 995-1001

6. RESULTS AND OUTCOMES

6.1 R307 fingerprint scanner Output

6.1.1 Fingerprint Sensor Image Characteristics:

Grayscale: Fingerprint sensor images are typically grayscale, meaning they only contain shades of gray, from black (darkest) to white (lightest). This allows for better contrast between the ridges and valleys of the fingerprint pattern.

Resolution: The resolution of the image will depend on the specific fingerprint sensor being used. However, it's generally not as high as a typical photograph. The focus is on capturing the details of the fingerprint pattern rather than fine details like skin texture.

File Format: BMP (.bmp) is a common file format for storing bitmap images. It's a simple format that can be easily processed by many software programs. However, it can also be a large file format, especially for high-resolution images.

Fingerprint Image Usage in Your Project:

Enrollment: During the enrollment process, the fingerprint sensor captures a user's fingerprint and stores the image data (possibly the .bmp file you described) in a secure location, potentially on the Raspberry Pi itself or uploaded to the cloud storage you mentioned.

Verification: When a user attempts to unlock the door using their fingerprint, the sensor captures a new fingerprint image and compares it to the stored enrollment data. The system grants access if the patterns match sufficiently.

Security Considerations:

Data Storage: It's crucial to store the fingerprint image data securely. This might involve encryption or storing them in a tamper-proof location on the Raspberry Pi or within the cloud storage service.

Privacy: Fingerprint data is considered biometric information and subject to privacy regulations. Make sure to follow best practices for user consent and data handling according to the regulations in your area.

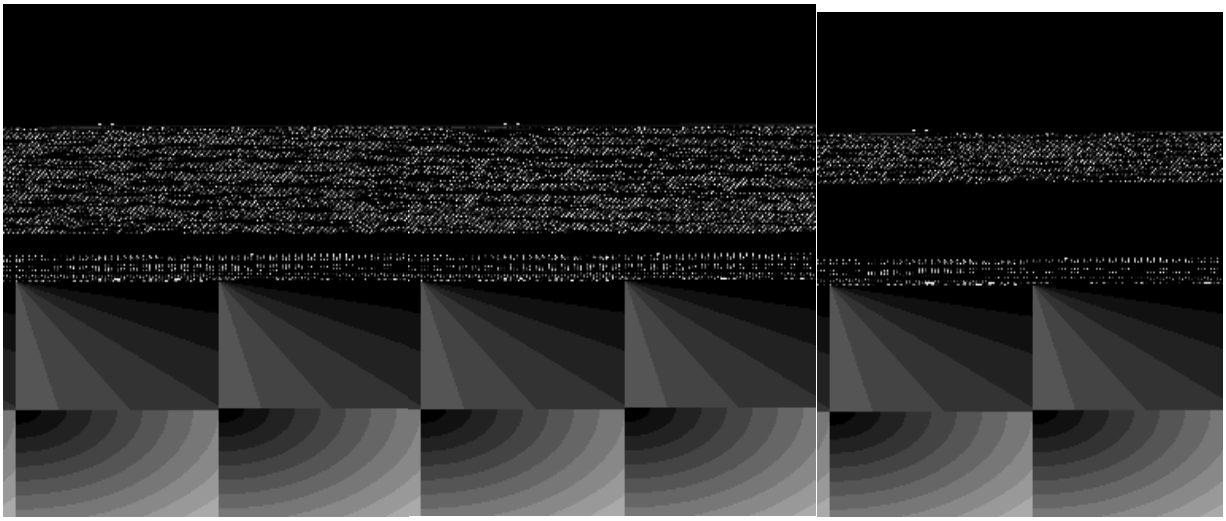

Figure 3: Fingerprints in raster graphics image file format

Raspberry Pi Camera Module Rev 1.3

Figure 3: Raspberry Pi Camera Module Rev 1.3 Captured Output

Sensor: 5-megapixel (MP) CMOS sensor

Resolution:

Photos: Up to 2592 x 1944 pixels

Videos:

1080p (1920 x 1080) @ 30fps

720p (1280 x 720) @ 60fps

640 x 480p @ (resolution and frame rate variations possible)

Interface: CSI (Camera Serial Interface) for direct connection to Raspberry Pi

Lens: Fixed focus lens

Form factor: Compact design, measuring around 25mm x 20mm x 9mm.

7. CONCLUSION

In conclusion, the development and deployment of a cloud-backed smart door lock system utilizing IoT devices, specifically the Raspberry Pi platform integrated with Google Cloud Platform (GCP), represents a significant advancement in the field of access control and surveillance technologies. Through the integration of biometric authentication, surveillance capabilities, and cloud-based storage, the system offers a comprehensive solution for enhancing security, accessibility, and scalability. The research presented in this paper has provided a detailed overview of the design, development, and deployment of the smart door lock system, including hardware components, software architecture, and integration with cloud services. By leveraging the capabilities of IoT devices and cloud computing technologies, the system enables real-time monitoring, secure access control, and seamless data storage and retrieval. Moreover, the proposed system has demonstrated the potential for innovative solutions in the domain of security systems, offering valuable insights into the design principles, implementation challenges, and performance considerations of IoT-based security technologies. The integration with Google Cloud Platform has enabled advanced data processing, analysis, and automation, further enhancing the functionality and efficiency of the system.

Overall, the research presented in this paper contributes to the advancement of IoT-based security technologies and inspires further innovation in the field. By showcasing the capabilities and benefits of cloud-backed smart door lock systems, this research paves the way for future developments in the realm of access control, surveillance, and security.

8. REFERENCES

[1] K. Umamaheswari and P. Mahitha, "Smart security system for door access based on unique authentication," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 1474- 1477, doi: 10.1109/I-SMAC52330.2021.9640855.

[2] S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-4, doi: 10.1109/ic- ETITE47903.2020.342.

[3] H. Qi, C. Wu, Y. Shi, X. Qi, K. Duan and X. Wang, "A Real-Time Face Detection Method Based on Blink Detection," in IEEE Access, vol. 11, pp. 28180-28189, 2023, doi: 10.1109/ACCESS.2023.3257986.

[4] H. -B. Kim, N. Choi, H. -J. Kwon and H. Kim, "Surveillance System for Real-Time High-Precision Recognition of Criminal Faces From Wild Videos," in IEEE Access, vol. 11, pp. 56066-56082, 2023, doi: 10.1109/ACCESS.2023.3282451.

[5] L. P. O. Paula, N. Faruqui, I. Mahmud, M. Whaiduzzaman, E. C. Hawkinson and S. Trivedi, "A Novel Front Door Security (FDS) Algorithm Using GoogleNet-BiLSTM Hybridization," in IEEE Access, vol. 11, pp. 19122-19134, 2023, doi: 10.1109/ACCESS.2023.3248509.

[6] Z. Huang, J. Zhang and H. Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 6, pp. 7917-7932, 1 June 2023, doi: 10.1109/TPAMI.2022.3217882.

[7] A. Krishnan and T. Thomas, "Finger Vein Recognition Based on Anatomical Features of Vein Patterns," in IEEE Access, vol. 11, pp. 39373-39384, 2023, doi: 10.1109/ACCESS.2023.3253203.

[8] Y. Huang, H. Ma and M. Wang, "Multimodal Finger Recognition Based on Asymmetric Networks With Fused Similarity," in IEEE Access, vol. 11, pp. 17497-17509, 2023, doi: 10.1109/ACCESS.2023.3242984.

[9] C. -Y. Lin, F. -J. Chen, H. -F. Ng and W. -Y. Lin, "Invisible Adversarial Attacks on Deep Learning- Based Face Recognition Models," in IEEE Access, vol. 11, pp. 51567-51577, 2023, doi: 10.1109/ACCESS.2023.3279488