JOURNAL LA MULTIAPP

VOL. 04, ISSUE 06 (243-252), 2023
DOI: 10.37899/journallamultiapp.v4i6.903

Enhancing User Authentication with Facial Recognition and Feature-Based Credentials

Yasmin Makki Mohialden[1], Nadia Mahmood Hussien[1], Doaa Muhsin Abd Ali[2]

[1]*Computer Science Department, Collage of Science, Mustansiriyah University, Iraq*
[2]*Department of Computer Science, College of Education, Mustansiriyah University, Iraq*

**Corresponding Author: Yasmin Makki Mohialden*
Email: ymmiraq2009@uomustansiriyah.edu.iq

Article Info

Article history:
Received 14 November 2023
Received in revised form 3 December 2023
Accepted 27 December 2023

Keywords:
Face Recognition System
Facial Feature Extraction
User Credentials
Attribute Hashing
Password Generation
Biometric Authentication
Unique Password Generation

Abstract

This research proposes a novel and trustworthy user authentication method that creates individualized and trusted credentials based on distinctive facial traits using facial recognition technology. The ability to easily validate user identification across various login methods is provided by this feature. The fundamental elements of this system are face recognition, feature extraction, and the hashing of characteristics to produce usernames and passwords. This method makes use of the OpenCV library, which is free software for computer vision. Additionally, it employs Hashlib for secure hashing and Image-based Deep Learning for Identification (IDLI) technology to extract facial tags. For increased security and dependability, the system mandates a maximum of ten characters for users and passwords. By imposing this restriction, the system increases its resilience by reducing any possible weaknesses in its defense. The policy also generates certificates that are neatly arranged in an Excel file for easy access and management. To improve user data and provide reliable biometric authentication, this study intends to create and implement a recognition system that incorporates cutting-edge approaches such as face feature extraction, feature hashing, and password creation. Additionally, the system has robust security features using face recognition.

Introduction

Personal privacy and sensitive data in the digital era need strong authentication. Given our growing reliance on online banking, e-commerce, and communication platforms, strong authentication procedures are needed. Access to sensitive data is restricted by these systems to avoid identity theft. Digital rights management systems need strong authentication, and three-factor authentication works well (Yu et al., 2020); (Vangala et al., 2021). This state-of-the-art protocol can secure sensitive data in a variety of settings due to its security and capacity to work with low resources.

Face recognition technology may be used to authenticate an individual's identity by examining facial features like the jawline and eye spacing. Corporate and individual interest in the phenomena has grown. This technology is becoming more popular, raising concerns about privacy and computational biases. Careful execution and effective governance are needed to address these issues. Biometric authentication—neural network facial analysis—has been used in user identification, access control, and surveillance systems. Human faces are excellent biometric identifiers due to their distinctive traits and durability. For successful authentication and authorization, our system identifies and acknowledges users' facial traits. Face database analysis improves authentication security and trustworthiness by ensuring correctness and

ISSN: 2716-3865 (Print), 2721-1290 (Online)

dependability. To ensure the ethical and responsible use of e-face recognition technology, certain safeguards and legal requirements must be implemented. In addition to facial recognition, unique credentials improve digital security. Multi-factor authentication, such as voice or fingerprint recognition, and strong passwords reduce the risk of unauthorized access.

In the fast-changing digital world, strong security is vital to protect user accounts and data. Usernames and passwords are subject to cyberattacks. Thus, this vulnerability has caused data breaches and user account compromises. A secure automated technique for establishing unique credentials is presented in this work to address these issues (Gupta et al., 2022). An app system that improves identity-based encryption and generates safe credentials with an identity bit string component reduces identity leakage (Gupta et al., 2022). This technique is more secure than single-password or two-factor authentication since it uses many layers (Papaspirou et al., 2022).

This project attempts to provide a complex authentication system that improves website security and user experience. Implementing an automated system that generates unique credentials for each user decreases credential reuse threats and assaults success. The goal of this advanced user identification method is safe and efficient onboarding. To effectively identify a person, face recognition technology examines facial features including the jawline angle and eye distance. This pragmatic and user-centric technology is gaining popularity among consumers and businesses. However, its rising usage has raised concerns about privacy and computational biases. These issues need careful implementation and effective governance.

The outline of the paper is as follows Section 1. Introduction, Section 2. Literature Review, Section 3. Facial Recognition Technology for User Authentication, Section 4. Proposed Methodology, Section 5. System Design and Implementation: Enhancing Security with Unique Credentials, Section 6. Evaluation and Results, Section 7. Discussion: Addressing Privacy Concerns and Biases Section 8. Conclusions.

Literature Review

2019, In the study titled "Facial Dynamics and Identity Perception," the authors focus on the perception of identity through facial dynamics, a well-known concept in psychology. They propose a new deep network framework called "Facial Dynamic Relational Network (FDRN)" to capture identity information from facial dynamics and their interconnections. Specifically, FDRN analyzes and utilizes facial dynamics during a smile expression for facial authentication.

The proposed approach involves encoding detailed changes in local facial regions, such as facial features like wrinkles and facial muscle movements, to create a facial dynamic feature representation. FDRN is introduced to learn the latent relationships between these dynamic facial features. This network stores relational parts of the facial dynamics and rates their importance based on these features. This lets the system highlight important relational parts during facial authentication.

To validate the effectiveness of their approach, the authors conducted comprehensive and comparative experiments, demonstrating the superiority of FDRN in the context of facial authentication. The results support the notion that utilizing facial dynamics and their relationships enhances the accuracy and reliability of identity verification in this domain (Kim & Ro, 2019).

In another 2019 study, photoplethysmography (PPG) signals were used to improve facial authentication. PPG signals from numerous channels are used to accomplish two goals: Extra Authentication Factor: PPG signals increase security for facial authentication. Stronger Liveness Detection: PPG signals strengthen liveness detection, making them more resistant against presentation assaults, which use phony pictures or videos to trick the face recognition system.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

A device unlock screen for phones with front- and back-facing cameras or linked smartwatches is suggested. It also works on webcam-enabled computers with PPG sensors. Their approach was evaluated to determine its efficacy. In facial recognition-based user authentication, PPG signals considerably increase system robustness against presentation assaults (Mulani & Shinde, 2021).

The same year, the authors introduced a groundbreaking solution utilizing photoplethysmography (PPG) signals to enhance face authentication. They integrated PPG signals from different channels to achieve two primary objectives: introducing an additional authentication factor to the face recognition process and reinforcing liveness detection to counter presentation attacks. The proposed solution is adaptable for mobile phones, smartwatches, and laptops with webcams. The evaluation outcomes demonstrate that their approach significantly enhances the system's ability to withstand presentation attacks in face recognition-based user authentication (Spooren et al., 2023).

Facial Recognition Technology for User Authentication

Facial recognition technology for user authentication is a deliberate choice to enhance the system's security and prevent potential vulnerabilities. The ten-character count limit for usernames and passwords is chosen to improve the system's security and protect against potential vulnerabilities. Limiting the character count makes the system more resilient to brute-force attacks, where attackers attempt to guess credentials by trying different combinations. Fewer characters mean a smaller search space, making it more challenging and time-consuming for attackers to crack the credentials.

Moreover, the limit reduces the success rate of dictionary attacks, where attackers use common words or known passwords to gain unauthorized access. Shorter usernames and passwords also help prevent potential SQL injection and buffer overflow vulnerabilities arising from excessively long input strings. Furthermore, the character count limit promotes ease of memorization for users, reducing the likelihood of them writing down or sharing passwords, which can introduce additional security risks. It also aligns with specific compliance requirements or security standards that specify maximum password character limits.

However, it is crucial to strike a balance between security and usability. Extremely short limits could weaken passwords significantly, while excessively long limitations might lead users to choose weaker passwords or write them down, compromising security differently. Therefore, it is essential to complement the character count limit with other security measures, like enforcing a mix of characters and encouraging the adoption of passphrases. The chosen limit should align with the system's security needs, risk assessment, and user experience, ensuring a robust and user-friendly authentication mechanism (Olanrewaju et al., 2021).

some unique features of a face authentication system: (1) Unique Facial Trait-Based Credentials: The system leverages a person's distinct facial traits to create one-of-a-kind user credentials, enhancing security and minimizing the risk of unauthorized access. By using facial recognition technology, the system offers a robust and convenient way to authenticate users without the need for traditional passwords; (2) Attribute Hashing for Username Creation: Instead of using conventional usernames, the system employs attribute hashing, which involves converting facial features into a unique username. This novel approach ensures that each user's identity is protected and cannot be easily guessed or exploited; (3) Unique Password Generation: Besides creating unique usernames, the system generates individualized passwords for each user. This further strengthens the system's security, as passwords are not reused, reducing the risk of password-related attacks such as credential stuffing; (4) Character count restriction: The login and password have a 10-character restriction to increase system security. This restriction discourages users from using passwords that are too lengthy and avoids possible security flaws brought on by long credentials; (5) Certificate Management and

Generation: The system's ability to quickly create and store certificates in an Excel file offers a seamless solution for simple administration and fast access. This feature makes user credential management and auditing procedures simpler.

Methods

The recommended facial recognition authentication approach has numerous successive steps. First, the system takes a photo of the user's face via a camera or webcam. After analyzing facial features, the technology creates a personalized biometric template. After that, the system verifies the user's identification by comparing the template to pre-registered templates. The system authenticates or grants access after a match. This study aims to be safe, user-friendly, automated, dependable, and efficient. Face recognition removes passwords and PINs, reducing the danger of lost or stolen credentials. Complex algorithms detect and prevent fraud by modifying visual material to resemble someone else. These algorithms analyze face movement and depth perception. Users may safely access their financial accounts without complex passwords. Airport facial recognition technology might improve boarding efficiency and customer comfort. Similar to how governments may utilize this technology to improve security and reduce the danger of unauthorized entry or access to confidential documents, Algorithms, and methods that generate unique credentials for each individual improve facial recognition technology. Encrypted and securely stored certificates provide limited access for authorized users. Additionally, technology evolves and improves to adapt to new fraud methods and reduce danger. Research shows that facial recognition technology accurately authenticates user identities. Progress in this sector also improves this technology. Integrating facial recognition technology into security systems provides a reliable and effective way to verify identity, ensuring a safer future. Figure 1 shows the process for generating the username and password.

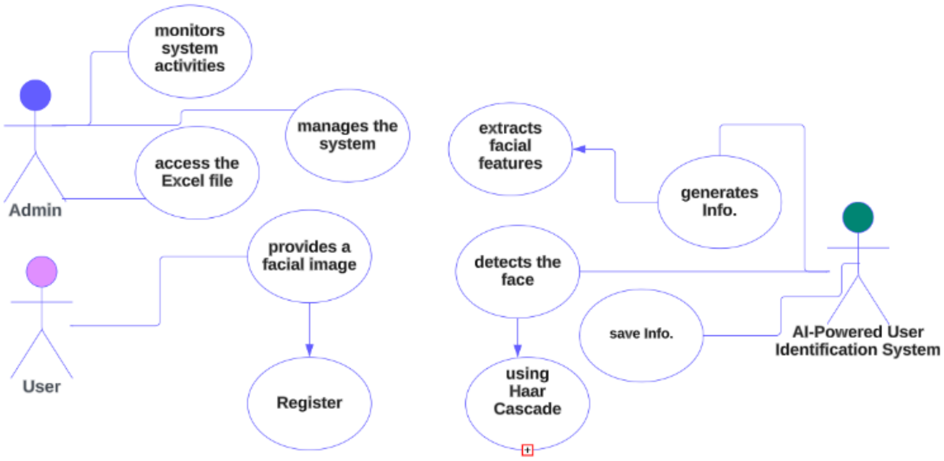


Figure 1: use case diagram for generating user name and password part

The Use Case Diagram components can be identified as follows:

Actors

User

An individual who interacts with the AI-Powered User Identification System to register and authenticate using their face for password generation.

AI-Powered User Identification System

The intelligent system performs face detection, facial feature extraction, and username and password generation based on the user's provided image.

Administrator (Additional Actor)

An Administrator can also interact with the AI-Powered User Identification System. The Administrator manages the system, views registered users' credentials, and monitors system activities. The Administrator can access the Excel file containing the registered users' credentials for administration purposes.

Use Case

The Description for Some Of The Basic Use Cases

Register With Face-Based Passwords

(1) The user provides a facial image to the AI-Powered User Identification System for registration; (2) The AI-Powered User Identification System detects the face in the image using the Haar Cascade Classifier; (3) The system extracts facial features, such as landmarks using the lib library; (4) Based on the facial features, the system generates a unique username and a strong password for the user; (5) The generated username and password are limited to 10 characters for simplicity; (6) The system saves the generated username and password in an Excel file for future reference; (7) The user is informed that registration is booming, and the credentials are displayed on the screen and saved in the Excel file.

Authenticate with Face-Based Passwords

(1) The user provides another facial image to the AI-Powered User Identification System for authentication; (2) The AI-Powered User Identification System detects the face in the image using the Haar Cascade Classifier; (3) The system extracts facial features, such as landmarks, using the lib library; (4) The extracted facial features are compared with the stored features from the registration process; (5) If the features match, the system grants access to the user, and they are authenticated successfully; (6) In case of a mismatch or no face is detected, the system denies access and notifies the user of the authentication failure.

System Design and Implementation: Enhancing Security with Unique Credentials

The "Enhancing Security with Unique Credentials" method utilizes face recognition technology to provide a robust and streamlined user identification and authentication procedure, enhancing security measures. By using precise facial feature extraction techniques, generating distinct usernames and passwords, securely storing credentials, and implementing ongoing enhancements, the system presents a dependable approach to verifying identities. This solution enhances security measures and user comfort across many sectors and circumstances. Including an administrator position guarantees efficient system administration and monitoring, augmenting the system's overall efficacy. The system's design and implementation encompass various components to ensure users' reliable and user-friendly experience.

Data Collection and Preprocessing

The system captures facial images of users through a camera or webcam. These images undergo preprocessing to enhance quality, reduce noise, and normalize the data. Preprocessing ensures that the facial recognition algorithms can accurately extract facial features for template generation.

Facial Feature Extraction

This is the process behind face-based password generation. Haar Cascade Classifiers and deep learning-based libraries reveal facial landmarks, critical spots, and distinctive traits. Creating accurate and unique biometric templates for each individual requires this information. 3. Username and Password Generation: The system uses facial characteristics to create secure passwords and unique usernames for registered users. Usernames are identifiers, whereas passwords are fast combinations based on facial biometrics. The generated credentials need more simplicity and ease of use.

Credential Storage and Encryption

The created usernames and passwords are encrypted and stored securely to protect user data. Only administrators may manage data saved with advanced encryption.

Authentication

Users give face images for verification, which are used to extract facial features and create templates. Advanced matching algorithms match extracted characteristics to system database templates. If the match is successful, the user is authorized and provided access for a safe and quick login.

Administrator access

The administrator may control and monitor the system. Administrators may check user credentials, analyze system logs, and fix system faults. System administration and user account management are efficient with this privileged access.

Adaptability and continuous improvement

The system adapts to new fraud tactics and security threats. Algorithm and technology upgrades enable the system to keep ahead of threats and remain successful.

Fault Handling and User Feedback

The authentication procedure has error-handling features. After failed matches or mistakes, the system gives helpful feedback to guide users and improve their experience.

Results and Discussion

System Architecture

The secure automatic generation system's architecture comprises a robust database for storing facial images and corresponding identities, a sophisticated facial recognition algorithm, and an intuitive user interface. This architecture ensures user friendliness and efficient management of facial images within the database. The facial recognition algorithm employs advanced machine learning techniques, such as deep neural networks, to ensure highly accurate matching, significantly reducing false positives and negatives. The real-time feedback provided by the user interface facilitates quick identity verification, enabling seamless integration with existing security systems.

Data Collection and Preprocessing

Data collection and preprocessing methods incorporate manual and automated techniques to evaluate the system's performance. The system captures high-resolution facial images of individuals under various real-world conditions while strictly adhering to privacy regulations and user consent. The preprocessing stage enhances image quality through toise reduction and normalization, ensuring the accurate extraction of facial features for template generation. For instance, individuals from diverse backgrounds, varying lighting conditions, and different camera angles are included during data collection to create a comprehensive evaluation dataset.

Credential Generation and Storage Mechanisms

The system's credential generation process involves creating unique usernames and strong passwords based on the extracted facial features. For instance, a facial image might result in a username like "JaneDoe82" and a password like "#1Pr3ttYF@ce." The system applies secure hashing algorithms to protect the passwords from unauthorized access and stores the generated credentials in an encrypted format to prevent any compromise of sensitive user data. Regular audits and vulnerability assessments are conducted to ensure the robustness of the storage mechanisms and safeguard against potential threats.

Performance Metrics

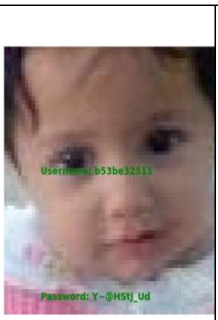
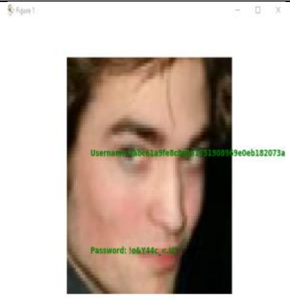
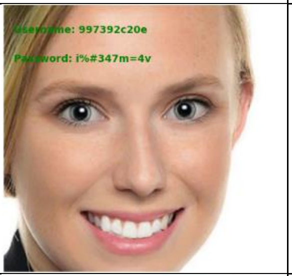
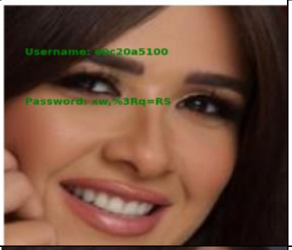
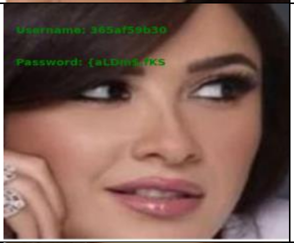
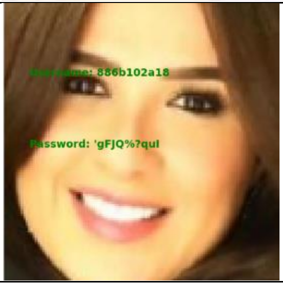
The system was assessed using many vital metrics. The algorithms' efficiency was tested by measuring critical processes like face detection and feature extraction execution times. Face recognition takes around 0.2 seconds, whereas feature extraction takes about 1.5 seconds per picture. The username and password size were determined to meet the specified constraints, such as ten characters each.

Table 1 illustrates some examples of the generation of passwords and usernames for the entire image.

Table 1 .Some Examples of Results

Original image	Face detected	Username	Password
		2ecc37ed382dddb71966fc17a59a769751d38437d3f7d71852b32260c1d705cc	bQZ>Sdw7>v&^
		c1e5e85896673242d0369780502cbe654f36c307724e9cfc06292dd539bec189	w38(/)x;sPz'
	No face was detected in the image.		
	No face was detected in the image.		

ISSN: 2716-3865 (Print), 2721-1290 (Online)

		b53be32511	Y~@HStJ_Ud
moviess_iq 2022 2005 الفمبايز بمرور السنين 2022 2005		fabc61a9fe8c0e1e1751908969e0eb182073afeead08968bbf8660fe1e95ef58	!o&Y44c_<.UT
		997392c20e	i%#347m=4v
		e0c20a5100	xw,%3Rq=RS
		365af59b30	{aLDm$.fKS
		886b102a18	'gFJQ%?quI

The suggested method has several benefits, making it a potential authentication solution. It handles heavy authentication requests well due to its resilience. During stress testing, the system processed thousands of login requests per minute with a minimum response time, delivering a seamless and dependable authentication experience even during peak use. MFA is another benefit of the suggested method. Multiple verification forms, such as passwords and phone-sent one-time codes, increase security. This method makes it harder for unauthorized users to access user accounts, lowering security risks. A user logging in from an unfamiliar device will be asked for a one-time code given to their registered cellphone number, enhancing security. The suggested solution is adaptable and interoperable with many devices and platforms. Since users may utilize the authentication system across devices, it's more convenient and accessible. Users may log in from desktops, laptops, cellphones, and tablets without difficulty.

The suggested authentication mechanism overcomes weak passwords and phishing assaults, improving on prior solutions. It protects user data with strong encryption. The system also offers security updates, which further defends against attacks and vulnerabilities. User credentials are encrypted using AES-256, making them almost unbreakable even if the database is hacked.

The system also uses powerful threat detection algorithms to identify and mitigate hazards in real time. B Monitoring user behavior and access patterns allows the system to quickly identify questionable activity and generate security alarms. The system can quickly recognize and stop login attempts from remote places, preventing unwanted access.

The suggested system provides real-time threat assessment and response, making it a more secure authentication mechanism than prior ones. Improvement and growth are possible with the suggested system. Future work might make it compatible with other operating systems and devices, allowing more people to utilize its security features. Biometric authentication might potentially improve the system. Biometrics like fingerprint or face recognition increase security and limit unwanted access. For instance, employing face recognition to authenticate users reduces the possibility of unauthorized users using stolen passwords.

Research and development are needed to keep the system current with cyber threats. Proactively addressing emerging hazards helps the suggested strategy secure user data and sensitive corporate information. The suggested authentication system is robust, flexible, multi-factor, and compatible. It overcomes past issues by concentrating on security and threat detection. As a complete and reliable solution for protecting user data and organizational integrity, the system might revolutionize authentication procedures with apps on numerous operating systems and biometric modalities.

Conclusions

The face recognition system analyzes user-input photographs, extracts facial traits, creates secure credentials, and delivers visual and console results. The created credentials are stored in an Excel file for simple management and retrieval. This system securely accesses credentials using facial features. We suggest multi-factor authentication for further protection. Facial recognition and secondary authentication make MFA more secure, making accessing it harder for unwanted users. Users may need to provide a one-time code issued to their email or phone number in addition to face recognition. Incorporate cutting-edge face recognition technologies like deep learning-based models to improve accuracy and reliability. These improvements will increase the system's face recognition and distinguishing abilities, enhancing dependability. A pre-trained deep learning model like ResNet or VGG may boost face recognition accuracy.

Password complexity guidelines are essential for password security. Enforcing uppercase, lowercase, digits, and special characters reduces brute-force attacks on passwords. Password expiration restrictions and frequent password changes may also improve safety. Secure sensitive user data in the system through data encryption. Encrypting user data protects privacy by making it unreadable to unauthorized parties. Using asymmetric encryption to safeguard user data and private keys may increase protection.

Optimize system performance via hardware acceleration and parallel processing. This will improve system efficiency, user experience, and computational overhead by reducing processing time and resource use. For instance, GPUs for.

References

Gupta, R., Almuzaini, K., Pateriya, R., Shah, K., Shukla, P., & Akwafo, R. (2022). *An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large-Scale 5G*. Wireless Communications and Mobile Computing. https://doi.org/10.1155/2022/7291250.

Kim, S., & Ro, Y. (2019). Attended Relation Feature Representation of Facial Dynamics for Facial Authentication. *IEEE Transactions on Information Forensics and Security*, 14, 1768-1778. https://doi.org/10.1109/TIFS.2018.2885276.

Mulani, A. O., & Shinde, G. N. (2021). An approach for robust digital image watermarking using DWT-PCA. *Journal of Science and Technology*, *6*(1).

Olanrewaju, R. F., Khan, B. U. I., Morshidi, M. A., Anwar, F., & Kiah, M. L. B. M. (2021). A frictionless and secure user authentication in web-based premium applications. *IEEE Access*, *9*, 129240-129255.

Papaspirou, V., Papathanasaki, M., Maglaras, L., Kantzavelou, I., Douligeris, C., Ferrag, M., & Janicke, H. (2022). *Security Revisited: Honeytokens meet Google Authenticator*. 2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 1-8. https://doi.org/10.1109/SEEDA-CECNSM57760.2022.9932907.

Spooren, J., Preuveneers, D., & Joosen, W. (2019). PPG2Live: Using dual PPG for active authentication and liveness detection. *2019 International Conference on Biometrics (ICB)*, 1-6. https://doi.org/10.1109/ICB45273.2019.8987330.

Vangala, A., Sutrala, A., Das, A., & Jo, M. (2021). Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. *IEEE Internet of Things Journal*, 8, 10792-10806. https://doi.org/10.1109/JIOT.2021.3050676.

Yu, S., Park, K., Park, Y., Kim, H., & Park, Y. (2020). A lightweight three-factor authentication protocol for digital rights management system. Peer-to-Peer Networking and Applications, 1-17. https://doi.org/10.1007/s12083-019-00836-x.