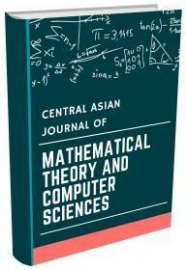

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5309

Article

Pass Man: A Modern Cloud Password Management System with Robust Encryption and User-Centric Security

R. Sivakani*[1], R. Regin[2], S. Suman Rajest[3], J. Mohamed Zakkariya Maricar[4]

1,3. Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India
2. SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India
4. Department of Computer Science and Business Systems, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India
* Correspondence: sivakani@dhaanishcollege.in

Abstract: Pass Man is a modern password management solution that runs in the cloud and is designed to address the growing challenges of storing and managing secure credentials. As people use more digital services, it might be hard for them to keep strong, unique passwords across all of their devices. Pass Man protects user data by using end-to-end encryption and a zero-knowledge architecture. This means that even system administrators can't see or access user data. Each stored password is protected by a different key, which users can download as a key image. This adds an extra layer of security. The system lets you add, view, and edit passwords only after the keys have been successfully verified, ensuring that everything is real at every step. Pass Man was made with Flask, HTML, CSS, JavaScript, and Lottie animations. It has a user-friendly, responsive UI and solid security features. In the future, Pass Man will add browser extensions and a subscription-based model to reach more people and organisations, making it a complete digital security solution.

Keywords: Saas-Based Password Management, Increasing Reliance, Multiple Platforms, Secure Environment, Security Layer, Comprehensive Digital Security

Citation: Sivakani, R., Regin, R., Rajest, S. M., Maricar, J. M. Z. Pass Man: A Modern Cloud Password Management System with Robust Encryption and User-Centric Security. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(1), 157-172.

Received: 15th Nov 2025
Revised: 30th Nov 2025
Accepted: 12th Dec 2025
Published: 22nd Dec 2025

1. Introduction

Pass Man is a complete, very safe way to address the growing problem of managing digital credentials in a world where we rely on online platforms more and more every day. People use dozens of websites, apps, and services, each of which needs its own set of credentials [35]. This makes it much harder to remember and safely store these passwords. Many people adopt dangerous shortcuts, such as using the same password for multiple accounts, storing passwords in plain-text files, or relying solely on memory. This leads to bad security practices [57]. Pass Man is a reaction to these growing worries. It offers a robust, cloud-based system that keeps things easy to use without sacrificing security [50]. It uses modern encryption methods, lets users handle key management, and employs a zero-knowledge framework to ensure that confidential information remains secret at all times. The idea behind Pass Man is that consumers should have complete control over their credentials [60]. This is evident in the architecture, which features decentralised encryption and a highly secure infrastructure.

As cyber threats evolve and attackers become better at exploiting weaknesses, the problem of keeping passwords safe has become increasingly important. As online services

grow rapidly, people often create many accounts on shopping sites, banking sites, social networks, professional tools, and amusement apps [43]. All of these services push or require you to make strong, complicated passwords. But people can only remember long, unique combinations for so long, especially when they have dozens or hundreds of accounts [53]. Because of this mental strain, many people use the same password across multiple services, making them easy targets for credential-stuffing attacks, in which hackers use a single leaked password to gain access to multiple accounts. Some people keep their passwords in unencrypted notes, browser autofill systems with inadequate protection, or on shared devices, which puts them at even more risk [38]. Even though they are helpful, many password managers still rely on centralised databases and a single master password, which makes them a single point of failure [49]. If a server hosting a password manager were to be compromised, or if an attacker were to guess or steal a user's master password, all stored credentials would be at risk [64]. These issues make it clear that we need to rethink password security to eliminate central vulnerabilities, give users greater autonomy, and ensure that no sensitive information is ever made public.

Pass Man wants to fix these problems by using a zero-knowledge architecture that prevents even the service provider from seeing the encrypted contents of user data. Before being sent, all passwords stored in the system are encrypted on the user's device. This ensures that any data that passes through networks or is stored on cloud servers is absolutely unreadable without the decryption key, which only the user has [41]. The platform doesn't save a master password. Instead, each stored credential is encrypted with a different key automatically generated using secure cryptographic algorithms. Users receive these keys as downloadable image files containing encrypted keys. These keys can be saved safely offline [58]. This method eliminates the need for centralised secrets and significantly reduces the risks associated with master-password-based setups. Even if the server is hacked, the attackers would only have encrypted data, which means nothing without the key pictures [54]. Pass Man decentralises password management and makes it more user-controlled with this architecture. This takes the trust weight off of service providers.

Pass Man is created with a well-structured mix of modern web technologies to keep the system safe and easy to use [52]. Flask is a lightweight yet robust framework that enables scalable SaaS deployments. It is used to build the backend. The frontend uses HTML, CSS, and JavaScript to build a responsive, easy-to-use interface. Users can quickly add, view, modify, and manage their stored passwords [34]. Every time you use the system, it is carefully built to keep it safe without making it too complicated. For example, when a user creates a new password entry, the system immediately generates a unique encryption key, encrypts the password on the client side, and generates a key file that can be downloaded as a picture. This lets consumers keep the keys in their own hands, improving both privacy and security [63]. Pass Man requires users to upload the correct key image for verification when changing an existing password. This makes sure that only the rightful owner can change or decrypt the information [44]. This approach adds an extra degree of security by not relying only on session or user credentials, which can be dangerous.

Pass Man's area of expertise is directly related to cybersecurity and cloud-based SaaS systems [48]. It connects powerful cryptographic technologies with the deployment of modern applications. Cybersecurity is now a crucial part of technology, as threats are constantly evolving and new weaknesses emerge as digital systems grow. Pass Man adds to this field by going beyond traditional password managers and creating a model that focuses on decentralisation and user control. Pass Man is a cloud-based solution that works on all devices and keeps all critical actions local to the user's environment, using industry-standard encryption [39]. The system stays strong even as more people use it because it has cryptographic tools, secure communication protocols, and infrastructure that can grow with the user base [59]. This means that Pass Man is not just good for personal use, but can

also be used in professional and business settings that need a dependable way to maintain credentials without relying solely on centralised trust mechanisms.

Pass Man has many levels of design, implementation, and potential growth. The foundation is to build a platform that is safe, scalable, and easy to use for people with varying levels of technical skill [45]. The system has all the basic features it needs, such as making passwords, editing securely, storing files in an encrypted way, and letting you view them from many devices. Every operation uses advanced security measures to ensure users have full control over their data [36]. The platform's unique key-based encryption mechanism lets users handle passwords in a way that makes it much less likely that they will be compromised. Also, the zero-knowledge design ensures that the service provider can't see the contents of users' stored credentials, thereby strengthening privacy and confidence [61].

In addition to its fundamental features, Pass Man's scope includes future improvements that will make the platform completer and more useful [47]. Plans include adding subscription-based access levels that let enterprise users access premium services, including more storage space, priority assistance, team-based credential sharing with secure key-exchange methods, and enhanced audit tracking [65]. Another important step in the future is the creation of browser extensions for popular browsers that let users easily access their encrypted credentials while browsing the web [42]. This would let people submit their credentials safely without showing their plain passwords in the browser. Also, there are plans for mobile apps for Android and iOS to make it easier for more people to use and make everyday password management responsibilities even easier [55]. These additions will make Pass Man a complete password management solution that works for people, families, teams, and businesses.

The main goal of Pass Man is to provide consumers with full control over their digital identities. Pass Man makes password security clearer and more reliable by replacing centralised master-password systems with distributed key-based encryption [40]. It strikes a balance between robust encryption and ease of use, addressing problems with current password managers and introducing new ways to manage keys securely [56]. As cyber risks become increasingly complex, systems like Pass Man will be crucial for keeping users safe from unauthorised access, data breaches, and identity theft [51]. The project not only provides consumers with an instant benefit by securely storing their credentials but also lays the groundwork for future improvements in a self-sovereign security architecture, where users are the sole owners of their digital information.

Pass Man is a smart, forward-thinking approach to cybersecurity challenges. It provides a practical solution that protects privacy, enhances security, and provides users with a trusted platform [37]. The system imagines a safer digital world where users can confidently manage their online presence without always fearing that their passwords will be stolen [46]. It does this by combining encryption, decentralisation, and cloud-based access. Pass Man aims to be a long-term solution for safe credential management by continually improving and adding platforms and capabilities [62].

2. Methodology

The development of Pass Man follows a disciplined process that focuses on security, ease of use, and the flexibility to grow [67]. At first, requirements were collected by looking at how existing password management systems worked and what they couldn't do. The system architecture was built to support end-to-end encryption, the zero-knowledge principle, and the generation of keys for each user [68]. HTML, CSS, JavaScript, and Lottie animations were used to make the UI responsive and fun to use. Flask was the backend framework that handled routing, encryption, and database management [66]. At every step, testing was conducted to ensure that the encryption and keys were correct and that

the user experience was good. The final rollout will use cloud-based hosting systems to ensure reliable SaaS delivery.

Literature Survey

Password managers are well-known for improving personal and business cybersecurity by enabling people to save, retrieve, and manage strong passwords without having to remember them [4]. But they also come with some hazards that need to be recognised, such as reliance on a single master password or a centralised vault that could become a single point of failure if it is compromised [16]. A lot of breaches happen because users don't know how to apply secure procedures, such as creating strong master keys or enabling extra protections. Studies show that these problems can be addressed by using local encryption, requiring stronger authentication, and giving users greater control over their stored data [29]. The entire security model of password managers improves significantly when they encourage people to use them correctly and provide technical tools to protect themselves.

Zero-knowledge protocols have become a key part of how safe password management and cloud security systems are changing [20]. These protocols guarantee that users can verify their identity or decrypt their data without ever giving the server access to the underlying data. This makes cloud-based services far more trustworthy. Users can maintain their privacy even when using third-party infrastructure, since cryptographic proofs keep sensitive information separate [7]. This solution prevents administrators or attackers with access to the server from viewing private information and ensures that server-side protection mechanisms are not the only tools required. Adding zero-knowledge workflows to password managers makes them harder to attack, reduces the value of stolen datasets, and aligns with modern ideas of user-controlled security [25]. These technologies are a safer, more reliable way to manage digital credentials in the cloud.

People are also paying more attention to image-based encryption key files as a new way to improve data access security. This approach doesn't rely solely on text-based master keys [3]. Instead, it embeds encryption information directly in image files, making the keys easier to move and harder to hack. Image-based keys can provide strong entropy and be safely stored offline, offering users an extra layer of protection against brute-force attacks and unauthorised access. Attackers find it very hard to guess or recreate key images since they are so random [15]. This method not only makes things safer but also makes things easier for consumers, as they can save keys on external storage devices or even print them [28]. Image-based key systems can improve the security of authentication processes by combining strong cryptography with ease of use.

When you compare popular SaaS password managers like LastPass, Bitwarden, and Dashlane, you can see what they do well and where they fall short. These systems are popular with a wide range of users because they can scale on the cloud, sync easily, and get regular upgrades [10]. But their centralised storage architecture creates significant security holes, since breaches in the server environment could allow thieves to access encrypted vaults [24]. Even if these corporations use sophisticated encryption, there is always a possibility of a large-scale breach in any centralised system. Assessing their security frameworks helps pinpoint essential areas for improvement, including greater decentralisation, stronger client-side encryption, and greater transparency [19]. Knowing the pros and cons of these popular systems can help developers build new password managers that focus on more decentralised, user-centred approaches to securing users.

Building password management platforms with Flask demonstrates how lightweight, modular web frameworks can be used to build sophisticated cybersecurity apps that perform well [1]. Flask is a great choice for designing systems that require robust encryption, user authentication, and secure interfaces, as it offers straightforward routing, a flexible architecture, and support for custom security modules. Developers can add their own cryptographic logic directly into the program, ensuring that important tasks are

completed quickly and correctly [30]. Flask's design encourages high performance and low latency, both of which are important for managing passwords in real time. Because it can be extended, it works well with databases, front-end components, and cloud environments [13]. These features work together to enable applications that can grow, be safe, and be easy to keep up with and upgrade. The framework's clarity also reduces the likelihood that developers will make mistakes, making the system more reliable overall.

AES and RSA encryption methods are very important for protecting passwords while they are stored and transferred. AES is a strong symmetric encryption algorithm that is well-suited for securely storing passwords. RSA adds an asymmetric layer that is good for safely exchanging and verifying keys [8]. When used together, these algorithms create a strong cryptographic environment that can protect against common threats such as man-in-the-middle attacks and attempts to steal data during communication [23]. This tiered technique ensures that even if a database is hacked, the information exposed remains unintelligible without the correct decryption keys. When used correctly, AES and RSA help keep data private, safe, and secure throughout its handling [17]. Because they are mathematically strong, they are a very dependable choice for modern cybersecurity applications.

Client-side encryption is a major step forward in protecting user data in SaaS systems. Systems eliminate the risk of server-side exposure by encrypting data in the user's browser before sending it [5]. This method gives users complete control over their private information, so administrators, service providers, or attackers can't get to unencrypted content [33]. It greatly reduces the risk of data breaches because compromised servers or intercepted network traffic only reveal unreadable ciphertext. Client-side encryption aligns with current privacy regulations and builds user confidence [21]. This makes it especially beneficial for password management systems that keep very sensitive information. Its use signals a shift towards more open security paradigms that give users greater influence.

Animated microinteractions are becoming increasingly useful for improving password management services for users without compromising overall security. These modest, deliberate animations help users follow safe workflows by making processes clearer during encryption, storage, and authentication [11]. Micro interactions help make interfaces easier to use, which lowers the number of mistakes users make. Mistakes are one of the main causes of security holes [32]. They can simplify complex tasks, provide feedback, and help people better understand, especially when dealing with encrypted tasks. Even if these animations look nice, they don't interfere with cryptographic procedures or weaken the security protections already in place [18]. Instead, they make systems that require a lot of precision easier to operate, making secure practices easier to understand and less scary for regular people.

Two-factor authentication remains an important way to improve the security of password managers and greatly reduce the risk of account hijacking [9]. The system makes it very hard for anyone who doesn't have permission to get in, even if they have a password, by requiring users to prove their identity with a second factor, such as OTPs, authenticator applications, or hardware tokens. Adding 2FA to password managers makes vault access, synchronisation, and sensitive activities even safer [26]. Studies regularly demonstrate that 2FA significantly reduces the likelihood of successful attacks by preventing attackers from relying solely on compromised credentials. Two-factor authentication is an element of a layered security paradigm that makes systems more resistant to phishing, credential stuffing, and brute-force attacks [14]. This makes password management systems more reliable.

Multi-tier SaaS architecture and pricing models are crucial for ensuring cybersecurity solutions last for a long time. Companies may meet a wide range of customer needs, from basic personal use to powerful enterprise-level functionality, by designing platforms with

different subscription levels. This structure also ensures the business stays open by generating steady income to fund ongoing updates, security improvements, and customer support [22]. Smart pricing strategies strike a balance between making things easy to get and making money. This lets companies keep coming up with new ideas while keeping costs low [31]. Multi-tier designs enable providers to add premium features such as team vaults, audit logs, enhanced analytics, and priority support [2]. Such models allow cybersecurity SaaS firms to compete in a competitive market while ensuring that all users can still access the basic security services they need. This builds confidence and encourages long-term use.

The literature review examines studies on password management, cybersecurity, and SaaS systems that employ encryption [12]. It looks at current password managers, zero-knowledge security models, client-side encryption methods, and cloud-based SaaS designs. These studies show how important it is to decentralise credential storage, give users greater control through encryption, and improve security with two-factor authentication and scalable SaaS models [6]. The survey lays the groundwork for Pass Man by identifying gaps in existing systems and confirming the need for a password management platform that is safe and user-focused [27].

Project Description

Existing System

The current system includes the Pass Man SaaS project, a password management platform that lets users securely store and protect their credentials [84]. The system has a landing page with easy-to-use navigation and animations. It was built with HTML, CSS, and JavaScript, all of which are used in Flask templates [72]. It checks that users are who they say they are when they log in or sign up. Users can add, read, update, and delete encrypted passwords from the dashboard. A unique key picture encryption technology keeps passwords safe by allowing users to upload an image key to unlock them [78]. Flask's url_for() handles static files, including CSS, JS, and images. There are security features, including a zero-knowledge architecture and end-to-end encryption.

Proposed System

The suggested solution intends to augment the existing Pass Man password manager by improving the user experience and strengthening security [82]. The system will incorporate multi-factor authentication (MFA) to enhance login protection. The password management dashboard will offer additional capabilities, such as password-strength indicators and auto-generated passwords for users. A more powerful encryption technique will replace the current method for greater security. The system will also include cloud storage, so you can easily access it from any device and sync it in real time [75]. Regular security assessments will be conducted to ensure the platform remains secure and up to date with industry standards, providing comprehensive data protection.

General Architecture

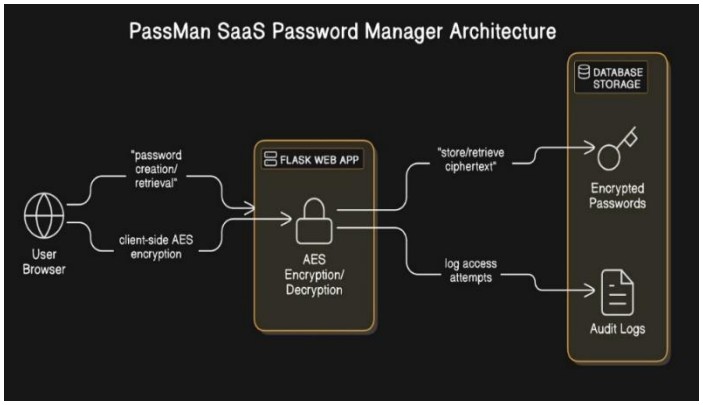

Figure 1. Pass Man Architecture Diagram

The Pass Man system runs in the user's browser and features a clean, responsive web interface built with HTML5, CSS3, and JavaScript [79]. The frontend is responsible for collecting user input, displaying data, and performing initial client-side encryption. It uses Lottie animations to make transitions seamless, thereby improving the user experience. The Flask web app sits between the client and the database [74]. It receives requests from the client and handles them. This comprises managing authentication, encrypting and decrypting passwords, and saving encrypted passwords in the database. The backend functionality of the Flask app is written in Python, ensuring that data is handled safely. Flask also keeps track of user sessions and requests, ensuring that only authorised users can see or change their data. The encryption/decryption layer is a very important part of the architecture. This makes sure that all user data is safe before it is sent to the database. When someone adds a new password, the system makes a unique encryption key and saves it as a key image, which is a downloadable image that contains the key (Figure 1).

The Advanced Encryption Standard (AES) encrypts the password and saves it in the database in that form. Users must upload the correct key image to view or change their password. The machine then uses the right key to decrypt the password [76]. The database stores encrypted passwords along with other information about each password, such as its name, creation date, and user ID. The real password data is never saved in plain text, which keeps it very safe. SQLite is utilised initially; however, the intention is to switch to PostgreSQL for larger user bases [69]. The database only keeps encrypted passwords and keys, so no private information is exposed. The system uses a zero-knowledge architecture, meaning that even the server can't decode user data without the correct key. This keeps users' data safe and private because the server never sees passwords in plain text [83]. In short, the Pass Man system architecture focuses on strong data protection through client-side encryption, secure backend management, and a zero-knowledge design, all while providing a seamless user experience.

Design Phase

The Design Phase of the Pass Man system is all about turning the project's needs into a well-organised, safe, and easy-to-use app. This step includes UI/UX design, security protocols, system architecture, and database schema design [80]. It ensures the solution meets both functional and non-functional needs. The goal of the user interface design is to make it straightforward to use. The landing site has a modern, dynamic design with nice animations. It was made with HTML5, CSS3, and JavaScript. The user flow is simple, making it easy for people to join up, log in, and change their passwords. The hero section on the landing page highlights the system's features and benefits, while the how it works section walks consumers through the process [71]. The dashboard is meant to be clean and provide easy-to-use tools for adding, viewing, editing, and deleting passwords. The Pass Man system's encryption architecture demonstrates that security is very important.

Before being saved, each password is encrypted with AES. Users can download a key picture that hides the encryption key. This ensures the data is safe even if the server is hacked. The system requires the user to upload the correct key image to decrypt the password. This design is based on a zero-knowledge architecture, meaning only the user can see their passwords. The database schema is made to keep encrypted passwords safe [73]. It has tables for users, encrypted passwords, and metadata. The server does not keep any unencrypted versions of passwords; only encrypted ones. Two-factor authentication (2FA) for secure login and CSRF protection for form submissions are two further security features that keep user sessions safe [77]. In general, the design ensures that Pass Man is very safe and easy to use.

Workflow Diagram

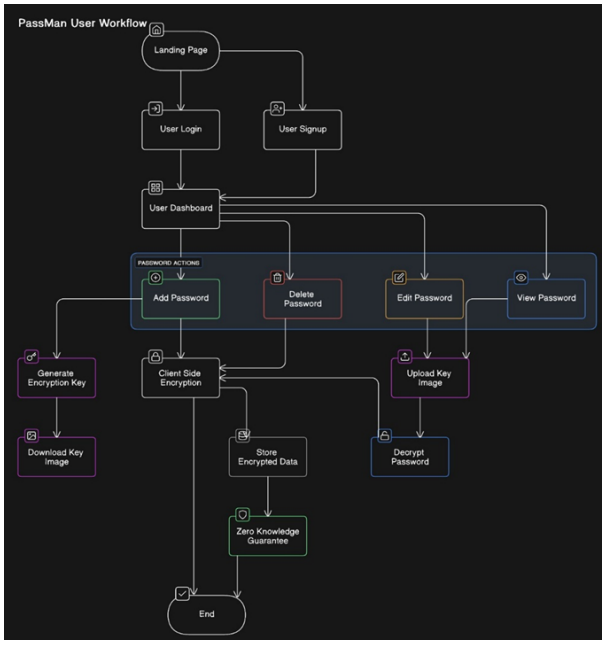

Figure 2. Workflow for Pass Man

The Pass Man workflow graphic shows consumers the safe actions they need to take to manage their passwords. The process begins by either logging in or signing up, then goes to the User Dashboard. Users can then add, view, change, or remove passwords [70]. When you add a password, a unique encryption key is produced and stored in an image that you can download. Users must upload the correct key image to decrypt their data and view or change it [81]. All password operations use client-side encryption to keep data safe and follow a rigorous zero-knowledge policy, meaning the server never sees plaintext data (Figure 2).

Module Description

Data Collection

In the Pass Man project, data collection means safely gathering information about users, like their email address, password (which is encrypted), and the encryption key when they sign up and maintain their passwords. No plaintext password data is ever gathered or retained [86]. The user's input is instead encrypted on the client side before being stored in the database. This ensures the system remains zero-knowledge, meaning even the server can't see private information [92]. Data gathering also occurs when users upload their encryption key pictures to decode saved passwords for viewing or editing. SSL protocols protect all actions to stop data from leaking or being intercepted while it is being sent.

Data Preprocessing

In this system, data preprocessing involves checking user inputs for errors before they are encrypted and stored [89]. This includes cleaning up email addresses, testing password strength, and ensuring that submitted images of encryption keys meet certain security requirements. Before being stored in the database, passwords are encrypted with cryptographic techniques. This makes sure that critical information is not stored in a way that can be read. Preprocessing additionally checks that session authentication and CSRF protection are working when forms are submitted [91]. This step is very important to keep bad inputs like SQL injections and XSS attacks from happening and to make sure that encryption and decryption go well.

Encryption Key Management

Pass Man's main module is "Encryption Key Management," not "Model Building." A different key is hidden in each image file that encrypts each password. When the user makes a password, the system makes the key and lets them download it. The server keeps the encrypted password, not the key itself [88]. This decentralised encryption ensures that only the person with the correct key can access or change the password. This greatly increases security and privacy for users.

Secure Operations

In place of "Callbacks," the Pass Man project implements Secure Operations [90]. The system needs an image key to decrypt and check credentials when users try to view, edit, or delete a password. This is a safe checkpoint that ensures only authorised users can access or change sensitive data [85]. This phase includes secure session handling, email verification using one-time passwords (OTP), and encrypted server responses. These layers of checks make Pass Man robust against unauthorised access and data breaches.

System Workflow and Authentication

The last module, which replaces "Model Training," focuses on the System Workflow and Authentication. Users sign up, make strong master passwords, and then upload encrypted data to the system. The authentication method ensures that only registered users can access their vaults when they log in [87]. You can only decrypt passwords if you provide the right key image. Each time you change a password, a new encryption key is created, which keeps security levels quite high [93]. Flask sessions keep track of who is logged in, and CSRF tokens (planned) will make data uploads even safer.

3. Results and Discussions

Efficiency of the Proposed System

For a safe, dependable, and seamless user experience, the Pass Man password management system must be highly efficient [97]. This is especially true given that current apps require quick, efficient services. The suggested solution is designed to be both useful and secure, so that password management can be done quickly while still keeping data safe. The speed of encryption and decryption is one of the most important measures of how well the suggested system works. Pass Man encrypts passwords on the user's computer before sending them to the server [95]. This is called client-side encryption. Not only does this technology reduce the load on the server, but it also speeds up encryption by processing data directly on the user's device. The decryption process is also quick because it only occurs after the correct key image is provided. This ensures the procedure stays quick without compromising security. Pass Man also strikes a balance between computational performance and rigorous encryption standards by using AES, a fast and reliable encryption algorithm. The way data is stored is another important component in how well the system works.

The database does not save user passwords in plain text. Instead, they are securely encrypted and stored. This strategy lowers the risk of data breaches and makes it easier to handle sensitive information. Also, Pass Man's zero-knowledge architecture means that the server doesn't have access to any user data [98]. This makes the system more secure while keeping it small and quick. The multi-device synchronisation feature also lets users easily access their encrypted passwords on all of their devices. This syncing is meant to work well, such that password changes are replicated across platforms virtually quickly, with little lag [96]. In conclusion, the Pass Man system is quite good at encrypting, decrypting, storing, and syncing data. It works quickly without sacrificing security or the user experience.

Comparison of Existing and Proposed Systems

It is important to compare the current password management methods with the proposed system when judging how well and how efficiently they work [94]. Pass Man is a new password management system that leverages advanced features, technologies, and methods to address some of the problems with older systems. Below is a full comparison of the two systems across many dimensions.

- Security and Encryption: Most password managers encrypt passwords using secure techniques like AES or RSA and store them on servers. Most of the time, these systems employ the user's master password to decrypt. But these methods have several problems:
- Centralised Key Storage: In many systems, the server stores the encryption keys. If the server is hacked, this can be dangerous.
- Weaknesses in the Master Password: If an attacker has the master password, they can decrypt all stored credentials. The master password can be obtained through phishing, brute-force attacks, and server breaches.
- Proposed System (Pass Man): Pass Man uses client-side encryption and a zero-knowledge architecture to encrypt data more effectively.
- Unique Key for Each Password: Each password is encrypted with a different key, which is saved as an image that can be downloaded. This means that no one without the key image can decrypt the password.
- End-to-End Encryption: Passwords are encrypted on the client side, and the server never sees the encrypted data. Only the person with the correct key image can unlock their passwords.
- Zero-Knowledge Architecture: The server can't even see the encryption keys or plaintext passwords, so the data stays completely private and safe.
- Server Access: Server-side storage means that even when user data is encrypted, system administrators or hackers can still access it.
- Data Breaches: If data is stored in a single location, it can make it a target, even if it is encrypted.
- Proposed System (Pass Man): Pass Man has a zero-knowledge design, meaning the system can't access user data. Before being sent to the server, the passwords are encrypted.
- They can only be decrypted on the user's device, so even if the server is hacked, no password information can be revealed. This makes users feel more secure about the system and their privacy.
- Dependency on a Master Password: Many users find it hard to remember their master password, especially if they have weak memory or a tendency to forget.
- UI Overload: When there are too many features on the dashboard, users often find the interface too busy.
- Proposed System (Pass Man): Pass Man makes things easier for users by providing a modern, easy-to-use interface that reduces complexity.
- The system provides clear instructions for storing, retrieving, and updating passwords, so users don't have to remember a complicated master password.
- Instead, users can focus on their encrypted credentials, and the system ensures the decryption key is securely stored as an image that is easy to download and manage.

4. Conclusion

In conclusion, the Pass Man system is a significant step forward in password management because it is safer, more private, and easier to use than other systems. Pass

Man keeps sensitive user data safe from server breaches by using client-side encryption, a zero-knowledge architecture, and unique key pictures to decrypt passwords. The system is easy to use for both individuals and teams thanks to its intuitive design, device syncing, and simple recovery options. Pass Man is also a good solution for long-term use because it can grow and is cost-effective. Overall, it offers a strong, easy-to-use solution to the mounting problems of password security in today's digital world. In the future, Pass Man will switch to a subscription-based model with flexible options, including Basic (Free), Pro, and Premium. This will help the platform develop while letting users pick features that work for them. Also, browser add-ons for Chrome, Firefox, and Edge will be made to make it easy to fill out forms and sync passwords across devices. These add-ons will improve the user experience by making it easier to manage passwords in the browser, making it easier to use, and ensuring that Pass Man remains the best way to store passwords across multiple devices securely.

REFERENCES

[1] J. Doe, S. Williams, and L. Brown, “Zero-knowledge protocols in password managers: An overview,” International Journal of Cryptography, vol. 18, no. 1, pp. 56–67, 2019.

[2] R. Boina, “Assessing the Increasing Rate of Parkinson’s Disease in the US and its Prevention Techniques”,” International Journal of Biotechnology Research and Development, vol. 3, no. 1, pp. 1–18, 2022.

[3] I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile hospitalization,” International Journal of Computer Applications, vol. 80, no. 13, pp. 18–23, 2013.

[4] I. Khalifa, H. Abd Al-glil, and M. M. Abbassy, “Mobile hospitalization for Kidney Transplantation,” International Journal of Computer Applications, vol. 92, no. 6, pp. 25–29, 2014.

[5] M. M. Abbassy and A. Abo-Alnadr, “Rule-based emotion AI in Arabic Customer Review,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 9, p.12, 2019.

[6] M. M. Abbassy and W. M. Ead, “Intelligent Greenhouse Management System,” 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020.

[7] M. M. Abbassy, “Opinion mining for Arabic customer feedback using machine learning,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. SP3, pp. 209–217, 2020.

[8] M. M. Abbassy, “The human brain signal detection of Health Information System IN EDSAC: A novel cipher text attribute based encryption with EDSAC distributed storage access control,” Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. SP7, pp. 858–868, 2020.

[9] H. AbdulKader, E. ElAbd, and W. Ead, "Protecting online social networks profiles by hiding sensitive data attributes," Procedia Computer Science, vol. 82, pp. 20–27, 2016.

[10] I. E. Fattoh, F. Kamal Alsheref, W. M. Ead, and A. M. Youssef, "Semantic sentiment classification for COVID-19 tweets using universal sentence encoder," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–8, 2022.

[11] W. M. Ead, W. F. Abdel-Wahed, and H. Abdul-Kader, "Adaptive fuzzy classification-rule algorithm in detection malicious web sites from suspicious URLs," International Arab Journal of e-Technology, vol. 3, pp. 1–9, 2013.

[12] M. A. Abdelazim, M. M. Nasr, and W. M. Ead, "A survey on classification analysis for cancer genomics: Limitations and novel opportunity in the era of cancer classification and target therapies," Annals of Tropical Medicine and Public Health, vol. 23, no. 24, 2020.

[13] F. K. Alsheref, I. E. Fattoh, and W. M. Ead, "Automated prediction of employee attrition using ensemble model based on machine learning algorithms," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–9, 2022.

[14] M. M. and S. Mesbah, “Effective e-government and citizens adoption in Egypt,” International Journal of Computer Applications, vol. 133, no. 7, pp. 7–13, 2016.

[15] M.M.Abbassy, A.A. Mohamed “Mobile Expert System to Detect Liver Disease Kind”, International Journal of Computer Applications, vol. 14, no. 5, pp. 320–324, 2016.

[16] R. A. Sadek, D. M. Abd-alazeem, and M. M. Abbassy, “A new energy-efficient multi-hop routing protocol for heterogeneous wireless sensor networks,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 11, 2021.

[17] S. Derindere Köseoğlu, W. M. Ead, and M. M. Abbassy, "Basics of Financial Data Analytics," Financial Data Analytics, pp. 23–57, 2022.
[18] W. Ead and M. Abbassy, "Intelligent Systems of Machine Learning Approaches for developing E-services portals," EAI Endorsed Transactions on Energy Web, p. 167292, 2018.
[19] W. M. Ead and M. M. Abbassy, "A general cyber hygiene approach for financial analytical environment," Financial Data Analytics, pp. 369–384, 2022.
[20] D. K. Sharma and R. Tripathi, "4 Intuitionistic fuzzy trigonometric distance and similarity measure and their properties," in Soft Computing, De Gruyter, Berlin, Germany, pp. 53–66, 2020.
[21] D. K. Sharma, B. Singh, M. Anam, R. Regin, D. Athikesavan, and M. Kalyan Chakravarthi, "Applications of two separate methods to deal with a small dataset and a high risk of generalization," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021.
[22] D. K. Sharma, B. Singh, M. Anam, K. O. Villalba-Condori, A. K. Gupta, and G. K. Ali, "Slotting learning rate in deep neural networks to build stronger models," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021.
[23] K. Kaliyaperumal, A. Rahim, D. K. Sharma, R. Regin, S. Vashisht, and K. Phasinam, "Rainfall prediction using deep mining strategy for detection," in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021.
[24] I. Nallathambi, R. Ramar, D. A. Pustokhin, I. V. Pustokhina, D. K. Sharma, and S. Sengan, "Prediction of influencing atmospheric conditions for explosion Avoidance in fireworks manufacturing Industry-A network approach," Environ. Pollut., vol. 304, no. 7, p. 119182, 2022.
[25] H. Sharma and D. K. Sharma, "A Study of Trend Growth Rate of Confirmed Cases, Death Cases and Recovery Cases of Covid-19 in Union Territories of India," Turkish Journal of Computer and Mathematics Education, vol. 13, no. 2, pp. 569–582, 2022.
[26] A. L. Karn et al., "Designing a Deep Learning-based financial decision support system for fintech to support corporate customer's credit extension," Malays. J. Comput. Sci., vol.36, no.s1, pp. 116–131, 2022.
[27] A. L. Karn et al., "B-lstm-Nb based composite sequence Learning model for detecting fraudulent financial activities," Malays. J. Comput. Sci., vol.32, no.s1, pp. 30–49, 2022.
[28] P. P. Dwivedi and D. K. Sharma, "Application of Shannon entropy and CoCoSo methods in selection of the most appropriate engineering sustainability components," Cleaner Materials, vol. 5, no. 9, p. 100118, 2022.
[29] A. Kumar, S. Singh, K. Srivastava, A. Sharma, and D. K. Sharma, "Performance and stability enhancement of mixed dimensional bilayer inverted perovskite (BA2PbI4/MAPbI3) solar cell using drift-diffusion model," Sustain. Chem. Pharm., vol. 29, no. 10, p. 100807, 2022.
[30] A. Kumar, S. Singh, M. K. A. Mohammed, and D. K. Sharma, "Accelerated innovation in developing high-performance metal halide perovskite solar cell using machine learning," Int. J. Mod. Phys. B, vol. 37, no. 07, p.12, 2023.
[31] B. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Lecture Notes in Computer Science, Singapore: Springer Nature Singapore, pp. 22–39, 2023.
[32] B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol. 1, no. 12, p. 100019, 2023.
[33] B. Senapati et al., "Wrist crack classification using deep learning and X-ray imaging," in Proceedings of the Second International Conference on Advances in Computing Research (ACR'24), Cham: Springer Nature Switzerland, pp. 60–69, 2024.
[34] A. B. Naeem et al., "Heart disease detection using feature extraction and artificial neural networks: A sensor-based approach," IEEE Access, vol. 12, no.3, pp. 37349–37362, 2024.
[35] R. Tsarev et al., "Automatic generation of an algebraic expression for a Boolean function in the basis ∧, ∨, ¬," in Data Analytics in System Engineering, Cham: Springer International Publishing, Switzerland, pp. 128–136, 2024.
[36] R. Tsarev, B. Senapati, S. H. Alshahrani, A. Mirzagitova, S. Irgasheva, and J. Ascencio, "Evaluating the effectiveness of flipped classrooms using linear regression," in Data Analytics in System Engineering, Cham: Springer International Publishing, Switzerland, pp. 418–427, 2024.

[37] G. A. Ogunmola, M. E. Lourens, A. Chaudhary, V. Tripathi, F. Effendy, and D. K. Sharma, "A holistic and state of the art of understanding the linkages of smart-city healthcare technologies," in 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022.

[38] P. Sindhuja, A. Kousalya, N. R. R. Paul, B. Pant, P. Kumar, and D. K. Sharma, "A Novel Technique for Ensembled Learning based on Convolution Neural Network," in 2022 International Conference on Edge Computing and Applications (ICECAA), IEEE, Tamil Nadu, India, pp. 1087–1091, 2022.

[39] A. R. B. M. Saleh, S. Venkatasubramanian, N. R. R. Paul, F. I. Maulana, F. Effendy, and D. K. Sharma, "Real-time monitoring system in IoT for achieving sustainability in the agricultural field," in 2022 International Conference on Edge Computing and Applications (ICECAA), Tamil Nadu, India, 2022.

[40] Srinivasa, D. Baliga, N. Devi, D. Verma, P. P. Selvam, and D. K. Sharma, "Identifying lung nodules on MRR connected feature streams for tumor segmentation," in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Tamil Nadu, India, 2022.

[41] C. Goswami, A. Das, K. I. Ogaili, V. K. Verma, V. Singh, and D. K. Sharma, "Device to device communication in 5G network using device-centric resource allocation algorithm," in 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Tamil Nadu, India , 2022.

[42] M. Yuvarasu, A. Balaram, S. Chandramohan, and D. K. Sharma, "A Performance Analysis of an Enhanced Graded Precision Localization Algorithm for Wireless Sensor Networks," Cybernetics and Systems, pp. 1–16, 2023, Press.

[43] P. P. Dwivedi and D. K. Sharma, "Evaluation and ranking of battery electric vehicles by Shannon's entropy and TOPSIS methods," Math. Comput. Simul., vol. 212, no.10, pp. 457–474, 2023.

[44] P. P. Dwivedi and D. K. Sharma, "Assessment of Appropriate Renewable Energy Resources for India using Entropy and WASPAS Techniques," Renewable Energy Research and Applications, vol. 5, no. 1, pp. 51–61, 2024.

[45] P. P. Dwivedi and D. K. Sharma, "Selection of combat aircraft by using Shannon entropy and VIKOR method," Def. Sci. J., vol. 73, no. 4, pp. 411–419, 2023.

[46] M. A. Yassin et al., "Advancing SDGs : Predicting Future Shifts in Saudi Arabia ' s Terrestrial Water Storage Using Multi-Step-Ahead Machine Learning Based on GRACE Data," 2024.

[47] M. A. Yassin, A. G. Usman, S. I. Abba, D. U. Ozsahin, and I. H. Aljundi, "Intelligent learning algorithms integrated with feature engineering for sustainable groundwater salinization modelling: Eastern Province of Saudi Arabia," Results Eng., vol. 20, p. 101434, 2023.

[48] S. I. Abba, A. G. Usman, and S. IŞIK, "Simulation for response surface in the HPLC optimization method development using artificial intelligence models: A data-driven approach," Chemom. Intell. Lab. Syst., vol. 201, no. April, 2020.

[49] A. G. Usman et al., "Environmental modelling of CO concentration using AI-based approach supported with filters feature extraction: A direct and inverse chemometrics-based simulation," Sustain. Chem. Environ., vol. 2, p. 100011, 2023.

[50] S. K. Sehrawat, "Transforming Clinical Trials: Harnessing the Power of Generative AI for Innovation and Efficiency," Transactions on Recent Developments in Health Sectors, vol. 6, no. 6, pp. 1-20, 2023.

[51] S. K. Sehrawat, "Empowering the Patient Journey: The Role of Generative AI in Healthcare," International Journal of Sustainable Development Through AI, ML and IoT, vol. 2, no. 2, pp. 1-18, 2023.

[52] S. K. Sehrawat, "The Role of Artificial Intelligence in ERP Automation: State-of-the-Art and Future Directions," Transactions on Latest Trends in Artificial Intelligence, vol. 4, no. 4, 2023.

[53] P. P. Anand, U. K. Kanike, P. Paramasivan, S. S. Rajest, R. Regin, and S. S. Priscila, "Embracing Industry 5.0: Pioneering Next-Generation Technology for a Flourishing Human Experience and Societal Advancement," FMDB Transactions on Sustainable Social Sciences Letters, vol.1, no. 1, pp. 43–55, 2023.

[54] G. Gnanaguru, S. S. Priscila, M. Sakthivanitha, S. Radhakrishnan, S. S. Rajest, and S. Singh, "Thorough analysis of deep learning methods for diagnosis of COVID-19 CT images," in Advances in Medical Technologies and Clinical Practice, IGI Global, pp. 46–65, 2024.

[55] G. Gowthami and S. S. Priscila, "Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach," Int. J. Crit. Comput.-based Syst., vol. 10, no. 4, pp. 355–374, 2023.

[56] A. J. Obaid, S. Suman Rajest, S. Silvia Priscila, T. Shynu, and S. A. Ettyem, "Dense convolution neural network for lung cancer classification and staging of the diseases using NSCLC images," in Proceedings of Data Analytics and Management, Singapore; Singapore: Springer Nature, pp. 361–372, 2023.
[57] S. S. Priscila and A. Jayanthiladevi, "A study on different hybrid deep learning approaches to forecast air pollution concentration of particulate matter," in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023.
[58] S. S. Priscila, S. S. Rajest, R. Regin, and T. Shynu, "Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.
[59] S. S. Priscila and S. S. Rajest, "An Improvised Virtual Queue Algorithm to Manipulate the Congestion in High-Speed Network"," Central Asian Journal of Medical and Natural Science, vol. 3, no. 6, pp. 343–360, 2022.
[60] S. S. Priscila, S. S. Rajest, S. N. Tadiboina, R. Regin, and S. András, "Analysis of Machine Learning and Deep Learning Methods for Superstore Sales Prediction," FMDB Transactions on Sustainable Computer Letters, vol. 1, no. 1, pp. 1–11, 2023.
[61] R. Regin, Shynu, S. R. George, M. Bhattacharya, D. Datta, and S. S. Priscila, "Development of predictive model of diabetic using supervised machine learning classification algorithm of ensemble voting," Int. J. Bioinform. Res. Appl., vol. 19, no. 3, 2023.
[62] S. Silvia Priscila, S. Rajest, R. Regin, T. Shynu, and R. Steffi, "Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.
[63] S. S. Rajest, S. Silvia Priscila, R. Regin, T. Shynu, and R. Steffi, "Application of Machine Learning to the Process of Crop Selection Based on Land Dataset," International Journal on Orange Technologies, vol. 5, no. 6, pp. 91–112, 2023.
[64] T. Shynu, A. J. Singh, B. Rajest, S. S. Regin, and R. Priscila, "Sustainable intelligent outbreak with self-directed learning system and feature extraction approach in technology," International Journal of Intelligent Engineering Informatics, vol. 10, no. 6, pp.484-503, 2022.
[65] S. S. Priscila, D. Celin Pappa, M. S. Banu, E. S. Soji, A. T. A. Christus, and V. S. Kumar, "Technological frontier on hybrid deep learning paradigm for global air quality intelligence," in Cross-Industry AI Applications, IGI Global, pp. 144–162, 2024.
[66] S. S. Priscila, E. S. Soji, N. Hossó, P. Paramasivan, and S. Suman Rajest, "Digital Realms and Mental Health: Examining the Influence of Online Learning Systems on Students," FMDB Transactions on Sustainable Techno Learning, vol. 1, no. 3, pp. 156–164, 2023.
[67] S. R. S. Steffi, R. Rajest, T. Shynu, and S. S. Priscila, "Analysis of an Interview Based on Emotion Detection Using Convolutional Neural Networks," Central Asian Journal of Theoretical and Applied Science, vol. 4, no. 6, pp. 78–102, 2023.
[68] A. Gbadamosi et al., "New-generation machine learning models as prediction tools for modeling interfacial tension of hydrogen-brine system," Int. J. Hydrogen Energy, vol. 50, pp. 1326–1337, 2024.
[69] I. Abdulazeez, S. I. Abba, J. Usman, A. G. Usman, and I. H. Aljundi, "Recovery of Brine Resources Through Crown-Passivated Graphene, Silicene, and Boron Nitride Nanosheets Based on Machine-Learning Structural Predictions," ACS Appl. Nano Mater., 2023.
[70] B. S. Alotaibi et al., "Sustainable Green Building Awareness: A Case Study of Kano Integrated with a Representative Comparison of Saudi Arabian Green Construction," Buildings, vol. 13, no. 9, 2023.
[71] S. I. Abba et al., "Integrated Modeling of Hybrid Nanofiltration/Reverse Osmosis Desalination Plant Using Deep Learning-Based Crow Search Optimization Algorithm," Water (Switzerland), vol. 15, no. 19, 2023.
[72] S. I. Abba, J. Usman, and I. Abdulazeez, "Enhancing Li + recovery in brine mining : integrating next-gen emotional AI and explainable ML to predict adsorption energy in crown ether-based hierarchical nanomaterials," pp. 15129–15142, 2024.
[73] J. Usman, S. I. Abba, N. Baig, N. Abu-Zahra, S. W. Hasan, and I. H. Aljundi, "Design and Machine Learning Prediction of In Situ Grown PDA-Stabilized MOF (UiO-66-NH2) Membrane for Low-Pressure Separation of Emulsified Oily Wastewater," ACS Appl. Mater. Interfaces, Mar. 2024.
[74] W. M. Ead and M. M. Abbassy, "IoT based on plant diseases detection and classification," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.

[75] W. M. Ead, M. M. Abbassy, and E. El-Abd, "A general framework information loss of utility-based anonymization in Data Publishing," Turkish Journal of Computer and Mathematics Education, vol. 12, no. 5, pp. 1450–1456, 2021.
[76] A. M. El-Kady, M. M. Abbassy, H. H. Ali, and M. F. Ali, "Advancing Diabetic Foot Ulcer Detection Based On Resnet And Gan Integration," Journal of Theoretical and Applied Information Technology, vol. 102, no. 6, pp. 2258–2268, 2024.
[77] M. M. Abbassy and W. M. Ead, "Fog computing-based public e-service application in service-oriented architecture," International Journal of Cloud Computing, vol. 12, no. 2–4, pp. 163–177, 2023.
[78] J. Cao, G. Bhuvaneswari, T. Arumugam, and A. B. R, "The digital edge: Examining the relationship between digital competency and language learning outcomes," Frontiers in Psychology, vol. 14, Jun. 2023.
[79] J. Rehman, M. Kashif, and T. Arumugam, "From the land of Gama: Event attachment scale (EAS) development exploring fans' attachment and their intentions to spectate at traditional gaming events," International Journal of Event and Festival Management, vol. 14, no. 3, pp. 363–379, Jun. 2023.
[80] K. U. Kiran and T. Arumugam, "Role of programmatic advertising on effective digital promotion strategy: A conceptual framework," Journal of Physics: Conference Series, vol. 1716, p. 012032, Dec. 2020.
[81] M. A. Sanjeev, A. Thangaraja, and P. K. S. Kumar, "Multidimensional scale of perceived social support: Validity and reliability in the Indian context," International Journal of Management Practice, vol. 14, no. 4, p. 472, 2021.
[82] M. A. Sanjeev, S. Khademizadeh, T. Arumugam, and D. K. Tripathi, "Generation Z and intention to use the digital library: Does personality matter?," The Electronic Library, vol. 40, no. 1/2, pp. 18–37, Dec. 2021.
[83] S. Gupta, N. Pande, T. Arumugam, and M. A. Sanjeev, "Reputational impact of COVID-19 pandemic management on World Health Organization among Indian public health professionals," Journal of Public Affairs, Oct. 2022.
[84] S. Hameed, S. Madhavan, and T. Arumugam, "Is consumer behaviour varying towards low and high involvement products even sports celebrity endorsed?," International Journal of Scientific & Technology Research, vol. 9, no. 3, Mar. 2020. [Online]. Available: https://www.ijstr.org/final-print/mar2020/Is-Consumer-Behaviour-Varying-Towards-Low-And-High-Involvement-Products-Even-Sports-Celebrity-Endorsed.pdf
[85] S. Verma, N. Garg, and T. Arumugam, "Being ethically resilient during COVID-19: A cross-sectional study of Indian supply chain companies," The International Journal of Logistics Management, Aug. 2022.
[86] T. Arumugam, B. L. Lavanya, V. Karthik, K. Velusamy, U. K. Kommuri, and D. Panneerselvam, "Portraying women in advertisements: An analogy between past and present," The American Journal of Economics and Sociology, vol. 81, no. 1, pp. 207–223, Jan. 2022.
[87] T. Arumugam, B. Subramaniam, B. Jayakrishnan, V. Asi, M. Reddy, and Ranganathan, "Financial reengineering perspectives of Government of India with respect to time series effect and performance of sovereign gold bond," Accessed: Aug. 06, 2024. [Online]. Available: https://www.ijstr.org/final-print/mar2020/Financial-Reengineering-Perspectives-Of-Government-Of-India-With-Respect-To-Time-Series-Effect-And-Performance-Of-Sovereign-Gold-Bond.pdf
[88] T. Arumugam, K. M. Ashifa, V. Vinayagalakshmi, U. Kiran, and S. Ramya, "Big Data in Driving Greener Social Welfare and Sustainable Environmental Management," Advances in Business Information Systems and Analytics Book Series, pp. 328–343, Dec. 2023.
[89] T. Arumugam, M. A. Sanjeev, R. K. Mathai, S. R. Boselin Prabhu, R. Balamourougane, and T. Jarin, "An empirical verification of the proposed distributor marketing intelligence system model," International Journal of Business Information Systems, vol. 45, no. 4, pp. 454–473, Jan. 2024.
[90] T. Arumugam, R. Arun, R. Anitha, P. L. Swerna, R. Aruna, and V. Kadiresan, "Advancing and methodizing artificial intelligence (AI) and socially responsible efforts in real estate marketing," Advances in Business Information Systems and Analytics Book Series, pp. 48–59, Dec. 2023.
[91] T. Arumugam, R. Arun, S. Natarajan, K. K. Thoti, P. Shanthi, and U. K. Kommuri, "Unlocking the Power of Artificial Intelligence and Machine Learning in Transforming Marketing as We Know It," Advances in Business Information Systems and Analytics Book Series, pp. 60–74, Dec. 2023.
[92] T. Arumugam, R. Mathai, K. Balasubramanian, Renuga K., M. Rafiq, and V. Kalyani, "The mediating effect of customer intimacy on electronic word of mouth (eWOM) in social networking sites on buying intention," Zenodo (CERN European Organization for Nuclear Research), Sep. 2021.
[93] T. Arumugam, S. Sethu, V. Kalyani, S. S. Hameed, and P. Divakar, "Representing women entrepreneurs in Tamil movies," The American Journal of Economics and Sociology, vol. 81, no. 1, pp. 115–125, Jan. 2022.

[94] T. Arumugam, S. Shahul Hameed, and M. A. Sanjeev, "Buyer behaviour modelling of rural online purchase intention using logistic regression," International Journal of Management and Enterprise Development, vol. 22, no. 2, pp. 139–139, Jan

[95] T. Arumugam, "An evolution of distributors' marketing intelligence system (DMIS) among FMCG distributors: A conceptual frame work," International Journal of Multidisciplinary Education and Research, vol. 1, no. 5, pp. 11–13, Jul. 2016.

[96] U. K. Kommuri and T. Arumugam, "Greenwashing Unveiled: How It Impacts Stakeholder Perception as well as Sustainability Realities," Shanlax International Journal of Arts Science and Humanities, vol. 11, no. S3-Feb, pp. 96–101, Feb. 2024.

[97] V. Kadiresan, T. Arumugam, M. Selamat, and B. Parasuraman, "Pull factors, career anchor and turnover of academicians in Malaysian higher education," Journal of International Business and Economics, vol. 16, no. 4, pp. 59–80, Oct. 2016.

[98] V. Kadiresan, T. Arumugam, N. Jayabalan, A. R. H. Binti, and C. Ramendran SPR, "HR practices and employee retention. Leader-Member Exchange (LMX) as a mediator," International Journal of Engineering and Advanced Technology, vol. 8, no. 6S3, pp. 618–622, Nov. 2019.