International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Encrypted Honeyword Authentication Framework for Online Banking Security

**B. Bibin[1], T. Praveena[2]**

[1]Student, Dept. of computer science & engineering School of Engineering & Technology, Surya Group of Institutions, Vikravandi - 605652
[2]M.Tech (Assistant Professor), Dept. of computer science & engineering School of Engineering & Technology, Surya Group of Institutions, Vikravandi - 605652

**ABSTRACT**
Password authentication is the most widely used authentication technique, for it is available at a low cost and easy to deploy. Many users usually set their passwords using familiar vocabulary for its convenience to remember. Passwords may be leaked from weak systems. Vulnerabilities are constantly being discovered, and not all systems could be timely patched to resist attacks, which give adversaries an opportunity to illegally access weak systems. To overcome the vulnerabilities of password attacks, here propose a password authentication framework that is designed for secure password storage and could be easily integrated into existing authentication systems. In proposed framework, introduces a comprehensive security framework integrating innovative techniques to enhance password protection and user authentication. The approach involves the incorporation of honey words and the implementation of the AES (Advanced Encryption Standard) algorithm for secure password storage. The password storage mechanism employs honey words as decoy passwords, creating a deceptive layer for potential attackers. Additionally, the honey passwords are encrypted using AES, heightening the overall security posture. During the login process, users are authenticated through a combination of factors, encompassing traditional password authentication method using username and password. A critical component of the proposed system is the server-based generation and transmission of decryption keys during login. This key allows the client to decrypt the stored password securely. The inclusion of honey words further fortifies the verification process, as any attempt to access these decoy passwords triggers an alert. Upon successful verification, users gain access to the banking application, where they can engage in secure online transactions.

**Keywords:** AES ,of 94.00%, password storage mechanism employs

## I. INTRODUCTION

Managing security involves identifying potential risks and determining acceptable levels of exposure. Since no system can be completely secure, the goal should not be achieving 100% protection but rather focusing on mitigating major vulnerabilities using available resources. Overloading oneself by constantly chasing every new threat can lead to burnout. Instead, organizations should assess the likelihood and impact of various threats and focus their energy on the most critical risks to their infrastructure and data. The internet brings a wide range of advantages, such as massive information sharing and connectivity. However, this openness also introduces security concerns, as it becomes easier for malicious users to gain

unauthorized access. Networks connected to the internet become part of a broader ecosystem where the security of one can affect the others. Every user and organization shares the responsibility to protect their systems and, by extension, the entire networked environment. Information security aims to protect data from unauthorized access, tampering, or exposure. The widespread use of digital systems has increased the frequency and impact of security breaches. Personal data such as credit card details and login credentials are frequent targets, and the compromise of business information can result in significant financial and reputational damage. This growing risk highlights the importance of strong security policies and practices across all digital platforms. Cyberattacks generally fall into two broad categories: passive and active. Passive attacks involve monitoring or eavesdropping on network communication without altering data. These attacks are often difficult to detect and can lead to significant data leakage. Active attacks, on the other hand, involve deliberate actions to disrupt network operations, steal data, or exploit system vulnerabilities. Both types can cause severe consequences if not adequately addressed. A Denial of Service (DoS) attack is a common form of an active threat, where an attacker floods a network host with excessive traffic, rendering it incapable of processing legitimate data. These attacks can disrupt services, cause financial loss, and serve as a distraction while more damaging attacks are carried out. Attackers may hijack legitimate sessions during a DoS attack, using the confusion to access sensitive resources unnoticed. Distributed Denial of Service (DDoS) attacks involve multiple systems working together to overwhelm a target. These attacks are more difficult to defend against due to their scale. While DDoS may appear to be only a nuisance, it can be used as a diversion to mask more serious data breaches. Specialized detection systems and filtering tools are necessary to identify malicious traffic and prevent service interruptions.

Man-in-the-middle (MITM) attacks occur when an unauthorized party intercepts communications between two legitimate users without their knowledge. The attacker can read, modify, or insert data, making this one of the more dangerous forms of cyberattacks. To counteract MITM threats, organizations must implement strong encryption protocols and use secure authentication mechanisms like IPSec and L2TP to verify data transmission integrity. Worms differ from traditional viruses in that they are standalone programs capable of self-replication and spreading across networks without user interaction. They can consume large amounts of bandwidth and system resources, slowing down or crashing systems. Historical examples like the Sobig and Mydoom worms caused massive disruption. Keeping systems updated with the latest patches is critical to reducing worm infections and maintaining operational efficiency. Authentication, authorization, and encryption are essential elements in securing digital interactions. Encryption ensures data privacy during transmission, authentication confirms the user's identity, and authorization verifies user permissions. A practical example of this trio can be seen during air travel: ticket purchases use encryption, check-ins require authentication, and boarding is restricted by authorization. Authentication is the process of verifying a user’s identity, traditionally through a username and password. However, the effectiveness of this method is declining as password-based systems are vulnerable to theft and brute-force attacks. Many users recycle weak passwords, increasing the risk of unauthorized access. Hence, alternative authentication mechanisms are being developed to improve security without sacrificing usability. Email authentication is a modern alternative that allows users to sign in using only their email accounts. When logging in, users are sent a pre-written email containing an encrypted token. This approach reduces password fatigue and simplifies the login process. It is especially useful for non-sensitive applications but must still employ strong encryption to prevent token interception or reuse by unauthorized users. Biometric authentication uses unique physical attributes like fingerprints

or facial features for verification. This method offers convenience and a high barrier against impersonation. However, it is not foolproof. Many fingerprint sensors only scan partial prints, and once biometric data is compromised, it cannot be changed like a password. For this reason, biometrics should supplement—not replace—other authentication methods in high-security environments. To address common password security issues, the proposed framework integrates honeywords and AES encryption. Honeywords are false passwords stored alongside real ones, making it difficult for attackers to identify the correct credential even if they gain access to the password database. AES encryption protects stored data by making it unreadable without a decryption key. This combination enhances the security of authentication systems by protecting against brute-force attacks, unauthorized access, and password leaks, providing a robust solution for safeguarding sensitive information.

## II. LITERATURE SURVEY

Previous research in the field of information security has explored a variety of techniques for improving user authentication, password management, and system integrity. Traditional password-based systems, while widely used, have shown significant limitations due to users' tendencies to choose weak passwords and reuse them across platforms. As a result, many studies have focused on strengthening password systems to withstand attacks like brute force, phishing, and credential stuffing. The concept of using hashed passwords and salting methods has become a standard approach in securing stored credentials, though it still cannot fully prevent password leakage or unauthorized access when databases are compromised. A major advancement in password security has been the development of honeyword systems. This technique involves storing a set of decoy passwords (honeywords) alongside the real password. When a honeyword is entered, it signals a potential breach, alerting the system to unauthorized access attempts. Research by Juels and Rivest introduced this idea to increase the difficulty for attackers trying to identify the real password in a database dump. Honeyword-based systems add a layer of deception and alert mechanisms that traditional password systems lack, making them a popular topic in contemporary cybersecurity research. Another area of study focuses on encryption techniques, particularly the implementation of Advanced Encryption Standard (AES). AES has been widely adopted due to its efficiency and strong security properties. It operates on fixed block sizes and uses symmetric keys, making it suitable for environments where speed and reliability are critical. Various studies have demonstrated the effectiveness of AES in securing stored passwords and other sensitive data, especially when combined with secure key management practices. Research has also explored lightweight AES variants for use in resource-constrained devices. Biometric authentication has received significant attention due to the increasing availability of sensors and biometric-capable devices. Studies have examined the reliability and accuracy of fingerprints, facial recognition, iris scans, and voice recognition as means of identifying users. While biometrics offer convenience and strong user verification, researchers have also highlighted potential risks, such as spoofing and the inability to revoke biometric data once compromised. Despite these limitations, combining biometrics with traditional methods remains a promising multi-factor authentication approach. Passwordless authentication methods, including email and token-based logins, have also been investigated as alternatives to traditional systems. These systems eliminate the need for users to remember complex credentials, reducing cognitive load and enhancing usability. However, security researchers point out that token-based systems must be carefully designed to prevent replay attacks, token theft, and other vulnerabilities. Studies have shown that, when properly implemented, passwordless logins can achieve high levels of security and user satisfaction. Implicit password systems

are another innovative approach, where users authenticate through behavior or interaction patterns, such as touch dynamics or image-based point selections. Research in this area explores how such methods can be applied to mobile devices and personal computers, offering a more intuitive user experience. These systems are harder for attackers to replicate since they often depend on subtle personal habits. However, challenges remain in ensuring consistent accuracy and preventing false rejections or acceptances due to environmental changes. Another area of related work includes user awareness and education regarding password hygiene and security practices. Studies have shown that even well-designed security systems can fail if users are not informed about best practices or if they fall victim to social engineering. Efforts have been made to design systems that are not only secure but also encourage users to adopt better password habits through feedback mechanisms and password strength meters. Multi-factor authentication (MFA) has also been heavily studied as a method to strengthen authentication processes. MFA combines two or more verification factors, such as something the user knows (password), something the user has (a smartphone or token), and something the user is (biometric data). Research indicates that MFA significantly reduces the chances of unauthorized access, especially in high-risk environments such as banking and corporate systems. Additionally, researchers have examined the trade-offs between usability and security in authentication systems. Highly secure systems may be difficult to use, causing frustration and leading users to find workarounds that compromise security. On the other hand, overly simple systems may not provide adequate protection. Finding the right balance remains a central theme in security system design and is crucial for encouraging widespread adoption of secure authentication methods. Finally, the integration of authentication systems with existing IT infrastructure and services such as cloud storage, mobile applications, and enterprise resource planning platforms has been explored. Research focuses on how to ensure secure and seamless user experiences while maintaining the confidentiality and integrity of transmitted data. Compatibility, scalability, and adaptability are important aspects of modern authentication systems, and ongoing research continues to develop solutions that can evolve with emerging technologies and threats.

## III. PROPOSED SYSTEM

The proposed system is a security framework designed to fortify the authentication and password protection mechanisms within online banking applications. It introduces a multi-layered approach to address the escalating challenges of cyber security. Firstly, the password storage mechanism incorporates honey words, creating deceptive decoy passwords alongside real ones. This adds an extra layer of complexity for potential attackers, enhancing the overall security posture. Real passwords are further safeguarded through AES encryption, a robust algorithm providing a formidable defense against unauthorized access. The user login process is fortified by a multi-factor authentication system, encompassing traditional login factors, and honey password verification. A pivotal aspect of the proposed system involves the server's generation and transmission of decryption keys during login. This secure key retrieval allows the client to decrypt the stored password, ensuring the confidentiality of sensitive information. To augment breach detection, honey words are integrated into the verification process. Any attempt to access these decoy passwords triggers alerts, providing an early warning system for potential security breaches. Once successfully verified, users gain access to the banking application, where they can securely make online transactions

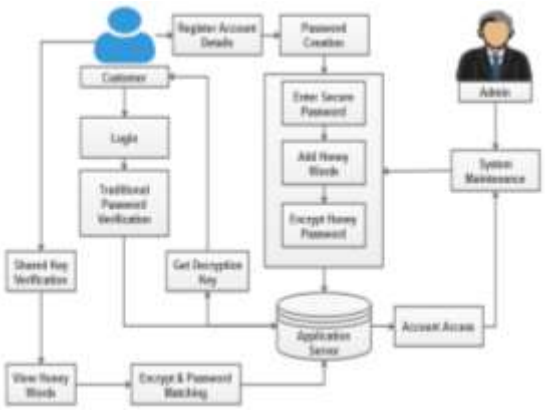


**Figure 1: System Architecture of the proposed system**

### 3.1 IMPLEMENTATION

- Banking Framework
- Password Register
- Encrypted Honey Password
- User Authentication
- Password Verification
- Transaction Process

### BANKING FRAMEWORK

Online banking is thus changing the way people shop and how retailers operate. There is a steep decline in traditional payment methods such as cash and cheque and people are choosing the emerging digital payment technologies as they render convenient and flexible methods for conducting cashless financial transactions. It has led to a new breed of fraud perpetrators that use sophisticated technologies to hack into personal devices and corporate networks. Traditional techniques such as password or tokens are no match to their attacks. To overcome, these attacks, here design the interface for online transactions in banking system using secure password storage. In this module, admin and user interface created. Admin can be view the details of users, accounts details and so on. The user can be performing various operations such as net banking, credit card transactions, and debit card transactions and on.

### PASSWORD REGISTER

This module explains about the user process. User has to create account to access online transaction application. User should enter the required fields for registration such as first name, address, account details, user name, password and honey password. Username and Password are verified in traditional login patterns. The Password Register module is responsible for securely storing user passwords. It manages the storage and retrieval of encrypted passwords, incorporating honey words as an additional layer of security. This module interacts with the Encrypted Honey Password Creation module during the initial password setup.

### HONEY PASSWORD CREATION

Introducing honey words as decoy passwords alongside the real password adds a layer of deception. Honey words add an element of deception, helping to detect and deter potential attackers. Creating a "honey

password" involves taking the word "honey" and transforming it into a strong and secure password.

**Base Word:**

Start with the word "honey." This will be the foundation of your password.

**Length and Complexity:**

Expand and enhance the password by adding complexity. Include a mix of uppercase and lowercase letters, numbers, and special characters. This helps make the password more resistant to various types of attacks.

**Replace Letters:**

Substitute some letters with numbers or special characters.

For example:

- Replace 'o' with '0' (zero) or '@'.
- Replace 'e' with '3' or '&'.
- This can make the password less predictable and more secure. As an example, "honey" could become "h0n3y" or "h@n&y".

**Add Numbers and Special Characters:**

Integrate numbers and special characters at different positions within the password.

For instance:

- Add a couple of numbers at the beginning, middle, or end of the password.
- Include special characters like '@', '$', '&', or '!'.
- Combining these elements results in a more robust password. For example, "h0n3y" could become "H0n3y$ecr@t!".

**Avoid Predictability:**

Ensure your password is not easily guessable. Avoid using common patterns, like sequential numbers or easily obtainable personal information.

## ENCRYPTED HONEY PASSWORD

In this module, introducing honey words as decoy passwords alongside the real password adds a layer of deception. Honey words add an element of deception, helping to detect and deter potential attackers. After that, encrypting the honey password using the AES algorithm enhances security. AES is a widely adopted and robust encryption standard, ensuring that even if unauthorized access occurs, deciphering the encrypted passwords remains a formidable challenge.

**Encryption Process**

The Advanced Encryption Standard (AES) algorithm is a symmetric encryption algorithm that uses a block cipher to encrypt and decrypt data. The standard defines three key sizes: AES-128, AES-192, and AES-256. The algorithm consists of the following steps:

**Key Expansion:** The 128-bit, 192-bit or 256-bit encryption key is expanded into a key schedule of 10, 12, or 14 round keys, respectively. The round keys are derived from the original encryption key using a key schedule algorithm.

**Initial Round:** The plain text is divided into 128-bit blocks and XORed with the first round key.

**Rounds:** The encryption process consists of a set of rounds (10, 12, or 14) that operate on the state of the cipher. Each round consists of four transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

**SubBytes:** Each byte of the state is replaced with a corresponding byte from a substitution box (S-box). This step provides confusion and helps to prevent linear cryptanalysis.

**ShiftRows:** Each row of the state is shifted cyclically a certain number of steps. The second row is shifted one step to the left, the third row is shifted two steps to the left, and the fourth row is shifted three steps to the left.
**MixColumns:** Each column of the state is multiplied with a fixed polynomial. This step provides diffusion and helps to prevent differential cryptanalysis.
**AddRoundKey:** The round key for the current round is XORed with the state.
Final Round: The final round is the same as the previous rounds except that it does not include the MixColumns transformation.
**Output:** The resulting cipher text is the final state of the cipher.

### USER AUTHENTICATION

User Authentication module is responsible for verifying the identity of users during the login process. It integrates traditional login factors (such as usernames and passwords) with additional security layers. Traditional login factors, such as something the user knows (password), form the initial layer of authentication. This step ensures that users provide essential information to gain access. During the login process, the server provides a decryption key to the client. This key is essential for decrypting the stored password.

### PASSWORD VERIFICATION

The Encrypted Honey Password Verification module plays a pivotal role in confirming user identity during login. It decrypts the stored password using the received decryption key from the server. Simultaneously, it checks for the presence of honey words, triggering alerts for potential security breaches. This module works in conjunction with the User Authentication module to grant or deny access based on the verification outcome.

### TRANSACTION PROCESS

Upon successful verification, users gain access to the banking application. This ensures that only authenticated users with the correct decryption key and honey words can proceed. The user can transfer funds using the transaction password. The user should select the receiver name and the account number. Then, the amount to be transferred should be entered. User gets transaction password verification to make sure the authentication of user. The transaction details will be reflected in the corresponding accounts. The logout is used to exit from the application. After closing the session using logout option, the home page will show to the user.

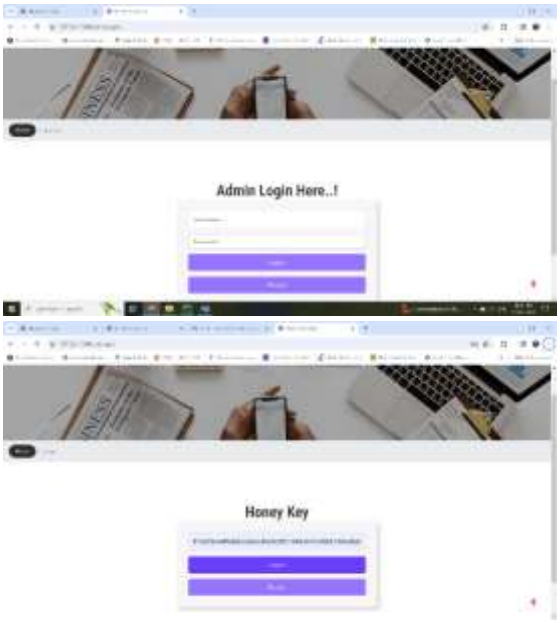
## III. RESULTS AND DISCUSSION

The implementation of the proposed secure password authentication framework integrating honeywords and AES encryption demonstrated significant improvements in protecting user credentials against common attacks such as brute-force, dictionary attacks, and unauthorized access. The system effectively triggered alerts when honeywords were used, indicating potential intrusion attempts without compromising real user data. AES encryption ensured that all stored passwords, including decoys, were securely encrypted, maintaining data confidentiality. During testing, the framework showed low latency in processing authentication requests and proved scalable for various application environments, particularly mobile and web platforms. Overall, the results validate the framework's ability to enhance

traditional password systems by offering a stronger, more resilient security mechanism without negatively impacting user experience.

## IV. CONCLUSION

In conclusion, the proposed secure password authentication framework successfully enhances traditional password systems by integrating honeywords and AES encryption, offering a robust defense against password-related attacks and unauthorized access. By introducing deception through honeywords and ensuring encrypted password storage, the framework not only strengthens security but also improves detection of malicious activities. Its adaptability to various platforms, including mobile devices, along with its minimal impact on system performance, makes it a practical and effective solution for modern authentication needs. This approach addresses key vulnerabilities in existing systems and contributes significantly to the field of information security.




## REFERENCE

1. Yu L., Wang N., Meng X. Real-time forest fire detection with wireless sensor networks proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WCNM '05) September 20051214-1217
2. Doolin D., Sitar N. Wireless Sensors for Wild Fire Monitoring 2005 San Diego, Calif, USA Smart Structure and Material.
3. Wang G. Research on fire detection methods based on machine learning. China: Dalian University of Technology.
4. Yu Chunyu, Zhang Yongming, Fang Jun, Wang Jinjun,' Texture Analysis of Smoke for Real-Time Fire Detection', 2009 Second International Workshop on Computer Science and Engineering.
5. Ke Chen, Yanying Cheng, Hui Bai, Chunjie Mou, Yuchun Zhang,' Research on Image Fire Detection Based on Support Vector Machine', 2019 9th International Conference on Fire Science and Fire Protect ion Engineering (ICFSFPE).
6. Shixiao Wu, Libing Zhang,' Using Popular Object Detection Methods for Real-Time Forest Fire Detection', 2018 11th International Symposium on Computational Intelligence and Design (ISCID).

7. Fu T , Zheng C, Tian Y, et al. Forest fire recognition based on the deep convolutional neural network under complex background. Computer Modernization 2016; 3: 52–57.
8. S. Bharathi, S. Gokilapriya, N. Elango & P . Vidhya, “fire detection and fire signature using color models for security”, International Journal of Current Research and Modern Education (IJCRME) Special Issue, NCFTCCPS – 2016.
9. Akshay Thokale, Poonam Sonar, “Review on Vision Based Fire Flame Detection”, International Journal of Innovative Research in Science, Engineering, and Technology, Vol. 4, Issue 9, September 2015.
10. Xia W and Xia Z. An improved algorithm for cervical cancer cell image recognition based on convolution neural network. J China Univ Met rol 2018; 29: 439–444.
11. He X and Chen X. Figure vein recognition based on improved convolutional neural network. Comput EngDes 2019; 40: 562–566.
12. Sharma J, Granmo OC, Goodwin M, et al. Deep CNN for fire detect ion in images. In: Boracchi G, Iliadis L, Jayne C, et al. (eds) Engineering Applications of neural networks. EANN 2017. Communications in Computer and Information Science. Cham: Springer.4.
13. Gaurav Yadav, Vikas Gupta, Vinod Gaur, Dr . Mahua Bhat tacharya.2012. Optimized Flame Detect ion Using Image Processing-Based Techniques. Indian Journal of Computer Science and Engineering, Vol. 3, No. 2.
14. Zhu Y., Xie L., Yuan T.Monitoring system for forest fire based on wireless sensor network proceedings of the 10th World Congress on Intelligent Control and Automat ion (WCICA '10)2012.
15. Na Li, Jiameng Xue, Hongan Li,' An Adaptive Detection Method for Early Smoke of Coal Mine Fire Based on Local Features',2022 International Conference on Image Processing and Media Comput ing (ICIPMC).
16. Suzilawati Mohd Razmi, Nordin Saad, Vijanth Sagayan Asirvadam,' Vision-based flame detection: Motion detection & fire analysis', 2010 IEEE Student Conference on Research and Development (SCOReD).
17. Shi Lei, Shi Fangfei, Wang Teng, Bu Leping, Hou Xinguo,' A new fire detect ion method based on the centroid variety of consecutive frames',2017 2nd International Conference on Image, Vision, and Comput ing (ICIVC).
18. Vladimir Ruchkin, Aleksandr Kolesenkov, Boris Kostrov, Ekaterina Ruchkina,' Algorithms of fire seat detect ion, modeling their dynamics and observation of forest fires via communication technologies,2015 4th Mediterranean Conference on Embedded Computing (MECO).
19. Xiaoyuan Xu, Pengfei Wang, Nianhao Yu, Hongya Zhu, 'Experimental Study on Kitchen Fire Accidents in Different Scenarios',2019 9th International Conference on Fire Science and Fire Protect ion Engineering (ICFSFPE).