JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancing Cloud Data Security with Honey Encryption

[1]Dr. V. Maria Antoniate Martin, [2]Sharon Dominick

[1]Assistant Professor, [2]Assistant Professor
[1]Department of Information Technology,
[1]St. Joseph's College, Tiruchirappalli, India
[2]Department of Computer Applications,
[2]Bishop Heber College, Tiruchirappalli, India

Abstract : **This research deals with fraud prevention and detection by using cryptography for encrypting user card details, cryptography is used for storing these encrypted details in an image which is mainly used for carrying out the transaction and finally data mining for detecting major deviations in the user's transaction pattern and accordingly blocking or completing the transaction. The three main concepts involved in the proposed system are thus, data encryption, image cryptography and data mining. A secure transaction is enhanced using this system. Unknown third party will be avoided. Encryption provides a high level secured system.**

IndexTerms **– Cloud computing, security, data mining and honey encryption.**

I. INTRODUCTION

Online banking now a day's plays a crucial role at each level on day-to-day transactions the importance of cryptography, which is primarily used to keep the information secret. The problem of transaction is the data theft which is stored in the open source like server. There is no security in transferring the account number and amount details to bank. Persons that commit online transaction crime largely go unpunished and repeatedly victimize consumers and businesses. Typically, the fraudster causes a credit card and debit card of another person to be charged for a purchase. Today, half of all credit card and debit card fraud is conducted online, meaning that the fraudsters make online purchases with the credit card details of other people.

Cryptosystem which is an encryption and a decryption process, involving the methods of hiding information using keys. The role of keys is to determine the functional output of the cryptographic algorithm. It specifies the transformation of an original message to an encrypted message and vice versa. Consequently, security of cryptographic algorithms relies on secrecy of the key. The whole idea of cryptography is Encryption and Decryption where in Encryption is a process in which plain text data is converted into an unintelligible or unreadable text called cipher text and decryption is the process of transforming data that has been rendered unreadable back to its normal form. The encryption algorithms were used for all the security processes and the algorithms required the use of software-based techniques which provided counter methods to avoid security attacks.

The banks now are incorporating data encryption, based on strong cryptographic methodologies into their communication channels in order to cross check the data transaction and avoid manipulations and have secured network communication and transactions. The review is focused on providing the information associated with technology-based services of banks and the security techniques adapted globally.

II. LITERATURE REVIEW

Ammar Abdul Majed Gharbi et al., provide an analysis of the honey encryption planner. Since two key areas are left open and each key used by a trespasser to decrypt a message is invalid, Honey Encryption is the encryption method that guarantees flexibility against a brute-force attack. However, it is challenging to construct a convincing message trap that is accurate enough to trick the striker even when he thinks he has the message in its original form.[1]

Aritra Dutta et al., put forth a technique that incorporates the Advanced Encryption Standard, proxy re encryption, Honey encryption, and N-th degree Truncated Polynomial Ring Unit (NTRU), also known as a Number Theory Research Unit. AES is a well-known symmetric encryption technique that encrypts and decrypts data using a secret key. A third party can convert cipher messages from one key to another using the proxy re-encryption cryptographic technique without knowing the plaintext. With honey encryption, which is a relatively recent method, messages are encrypted with data that appears realistic but is false, making it impossible for attackers to tell if the message has been decrypted or not. [2]

S. Arun et al., present a combination of the Advanced Encryption Standard and Honey Cryptography as an extension of a public-key cryptosystem to enable a private key cryptosystem. The outcomes were achieved using an Advanced Encryption Standard key length of 128 bits for 10 repetitions. Their study suggests a honey encryption strategy as a way to increase proficiency and decrease downsides. The parameters that will be addressed center on the number of iterations, the length of the key, and the type of side channel attack to be used. [3]

Ms. Hetal Rahul Modi et al., address four types of graphical password techniques: recognition-based, pure recall-based, cued recall-based, and hybrid-based. Alphanumeric passwords are an alternative to graphic passwords because it can be challenging to

remember them. It is considerably simpler to access and use a certain program when a user-friendly authentication mechanism is available for it. One of the key grounds for this method is the fact that pictures are easier for the human mind to recall than alphabets or numbers.[4]

To improve the data security of the cloud against viruses and attacks, Mercy Joseph et al., created the new Hybrid Bat and Cuckoo-based Pallier Homomorphic Encryption (HBC-PHE) technique. Datasets are initially transferred into the created HBC-PHE framework after being initially stored on the cloud using a Python program. Create a key for each dataset separately and then separate a private key for each dataset. Moreover, use PHE's bat and cuckoo fitness function to ciphertext-encode the plain text. Finally, cloud-stored data are effectively encrypted, and the proposed framework's performance results are compared to those of other methods in terms of confidentiality rate, decryption time, encryption time, efficiency, and throughput.[5]

Propose that when using honey encryption, ciphertext is produced. If the wrong decryption key is used, this ciphertext can be decrypted to create plausible plaintext. In order to protect against brute force attacks, Honey Encryption delivers fake plaintext. Additionally, SRM (Secure Repository Manager) separates the material into small bits after encryption before uploading it to cloud servers.[6]

To combat shoulder surfing attacks Pathik Nandi et.al.,[7] have suggested the idea of using a graphical password as if offers security against brute force attacks where the user makes a new registration. Later one logs in with a valid user ID and password. The password is a grouping of characters and numbers. Then the user uses a cross image-based authentication where user can chooses their password and this method has higher chances to offset each other. In colour based authentication, there should be several colour base passwords and depending on the colour, one needs to remember the password sequence.

Rahul Midha et al.,[8] present the secure storage of data from unauthorized access by giving access to garbage files. To detect the authenticity of the person, Honeypot Technology is used. This technology detects and counter attacks the unauthorized access by generating a garbage file. Data security is improved by using cryptographic algorithm.

Dr. V Vasanthi et al.,[9] have examined Honey Encryption (HE), a novel encryption technique that resists brute force attacks by assuring that messages decoded with false keys produce messages that appear to be genuine. They demonstrate the implementation of honey encryption and use practical real-world examples like credit cards and fundamental text messaging to illustrate its utility. They also add public-key encryption capability to the fundamental honey encryption technique.

Mrs. R. Yamini et al.,[10] proposed a system to predict the click based graphical password system that not only guides and helps the user for password selection but also encourages the user to pick more random distributed password. The secure internet banking is predicated on Persuasive Technology which motivates and influence people to behave during a desired manner.

III. Research Methodology

Web application security has become an important concern for every user. This research implements a secure transaction platform that helps users to make secure bank transactions. In the communication between bank and merchant, every time merchant must be verified to prevent fraudulent transactions. Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. Many encryption algorithms are available for encryption and decryption. These can be categorized in two groups, symmetric key encryption algorithms and asymmetric key encryption algorithms. In symmetric key encryption, only one key is used for both encryption and decryption, whereas in asymmetric key encryption (also known as public key encryption), two keys are used: public key and private key. The public key is used to encrypt data and the private key to decrypt.

In figure (a) the honey encryption is applied to all the transactions. Before sending the money the sender applies the encryption algorithm, at the receivers end the receiver views the transaction and then applies and decryption algorithm and receives the money safe and securely.

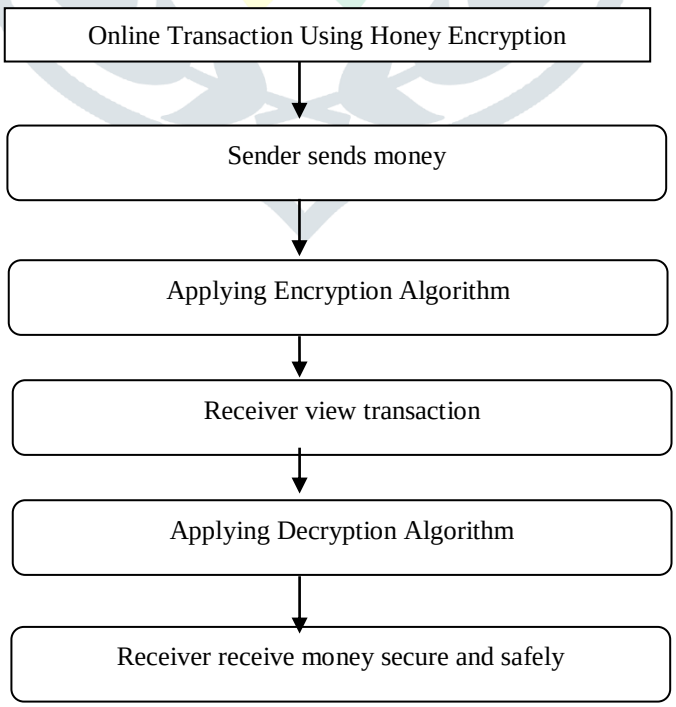

Fig. (a) Methodology Diagram

IV. Result and Discussion

4.1 Admin Login

A login is a set of credentials used to authenticate a user. Most of these consist of a username and password. They are a security measure designed to prevent unauthorized access to confidential data.

4.2 View Transaction

In this module admin can view the user details and user transaction details these module can help us the admin can view and check the user details and transaction details.

4.3 View User

In this module admin will view the details of the user registered in this module.

4.4 Bank Registration

In this module help us every bank user first every user can enter the registration details after complete the registration the bank user can get a unique user name and password.

Bank users can view and check the user details how many users are entered in the web sites and entered in our bank sites and the bank user view the amount transaction details.

4.5 User Registration

The user can register in the website for personally using this money transaction application after they complete the registration, they will get login permission.

These modules help us the user. User can enter in bank details and deposit the amount. User can use this module for the users transaction like user deposit and withdrawn.

4.6 Honey Encryption

A brute-force attack involves repeated decryption with random keys; this is equivalent to picking random plaintexts from the space of all possible plaintexts with a uniform distribution. This is effective because even though the attacker is equally likely to see any given plaintext, most plaintexts are extremely unlikely to be legitimate i.e., the distribution of legitimate plaintexts is non-uniform. Honey encryption defeats such attacks by first transforming the plaintext into a space such that the distribution of legitimate plaintexts is uniform. Thus, an attacker guessing keys will see legitimate-looking plaintexts frequently and random-looking plaintexts infrequently. This makes it difficult to determine when the correct key has been guessed. In effect, honey encryption serves up fake data in response to every incorrect guess of the password or encryption key.

V. Conclusion

Based on the analysis done one can conclude that the system has been successfully implemented and provides a secure E-Banking experience for every user. The system provides a strong mechanism to prevent online frauds by using cryptography and on the client side. On the server side of the system Data mining ensures fraud detection. Based on all the tests conducted on the image generated honey encryption one can deduce that the image satisfies all the necessary criteria in terms of quality and efficiency. The testing done on the data mining module with two different datasets ensures that all the normal and extreme cases are satisfactorily handled by the algorithm. The motive of the research was to deliver a safe and protected online banking experience and based on the analysis and testing conducted one can reckon that it has been efficaciously achieved.

VI. Acknowledgment

First and foremost, I thank GOD for his blessings. I thank my family members for helping me in this research.

References

[1] Ammar Abdul Majed Gharbi, and Ahmed Sami Nori. 2022. Honey Encryption Security Techniques: A Review Paper. Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM), Vol. 16, No. 1, (1-14).

[2] Aritra Dutta et.al. 2023. Hybrid Encryption Technique to Enhance Security of Health Data in Cloud Environment. Archives of Pharmacy Practice, Volume 14 , Issue 3.

[3] Arun S, and N. R. Shanker. 2019. Data Security In Cloud Storage Using Advanced Encryption Standard And Honey Cryptography. Asian Research Publishing Network (ARPN), Vol. 14, No. 7.

[4] Hetal Rahul Modi and Dr. Nayan Soni. 2023. Comparison Techniques Of Graphical Password. Journal of Emerging Technologies and Innovative Research (JETIR), Volume 10, Issue 2.

[5] Mercy Joseph, and Gobi Mohan. 2022. Design a hybrid Optimization and Homomorphic Encryption for Securing Data in a Cloud Environment. International Journal of Computer Networks and Applications (IJCNA), Volume 9, Issue 4.

[6] Navneet Singh Khurana. 2021. Security in cloud computing using honey encryption. International Journal of Advance Research, Ideas and Innovations in Technology, Volume 7, Issue 1.

[7] Pathik Nandi, and Dr. Preeti Savant. 2022. Graphical Password Authentication System. International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 10, No. IV.

[8] Rahul Midha. 2019. Secure Data Protection in Cloud Computing. International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04.

[9] Vasanthi V Dr., and J Logeshwaran. 2023. Honey Encryption Algorithms To Protect Data. Journal of Emerging Technologies and Innovative Research (JETIR), Volume 10, Issue 3.

[10] Yamini R et.al. 2020. Secure Internet Banking Using Graphical Password With Otp. International Journal of Creative Research Thoughts (IJCRT), Volume 8, Issue 3.