Reducing Cloud Data Breaches and Improving Data Security using Honey Encryption Algorithm

Latha.K, Sheela.T

Abstract: Data security is the most predominant measure that should be followed in any organization to prevent uncertified access to user's data. A data breach is a security event in which sensitive data is viewed, transmitted, stolen or used by an unauthorized individual. A number of breaches include compromised password files which reveal the passwords of millions of users in an organization. The paper is intended to identify such password breaches through honey encryption technique. Using the concept of honey words, each user has a list of sweet words corresponding to their account, out of which only one is original password and remaining are fake passwords. During Honey Encryption, Distribution-transforming encoder (DTE) is applied on the password to acquire the seed space which is then encrypted by using secret key. The proposed model can be efficiently implemented in cloud applications to highly reduce cloud data breaches.

Keywords: Honey Encryption technique, Distribution Transforming Encoder, Password breach, Honey words.

I. INTRODUCTION

The features of cloud computing and storage facilities provideusers with the capability to reserve and process their data in available third party data centers. Many organizationsemploy cloud with variety of service models (includingPaaS, SaaS, and IaaS clouds) and various deploymental models (such as public,private, hybrid, and community clouds). The major security problemsconcerned with cloud computing include: issues regarding security faced by cloud service providers (organizations which provideservice through the cloud) and security concerns encountered by the customers (clients which host their applications and data on the cloud). Cloud security is process of safeguarding data, applications, and infrastructures in the cloud. Some of the critical security concerns in cloud include unauthorized data access, weak access controls, compromised attacks, and denial of availability.Security in cloud is a major issue for cloud service and storage providers. They not only have responsibility of satisfying their customers but also must follow undeniable regulations for storing confidential data.

Revised Manuscript Received on September 22, 2019.

Latha.K, Research scholar, Faculty of computer science and engineering, SathyabamaInstitute of Science & Technology. Assistant Professor, Department of Computer Science and Engineering, Sri Sai Ram Engineering College, klathasn@gmail.com.

Sheela.T, Professor & HOD, Deptof ,IT, Sri Sai Ram Engineering College, Chennai 600 044,Tamil Nadu, India, klathasn@gmail.com.

II. ENCRYPTION AND DECRYPTION

Data Encryption algorithms are considered to be the most secure way to secure sensitive data in real world systems. Encryption is the process of converting information in to a code, to prevent illegal access. Encryption of passwords involves encrypting passwords with an encryption key. Encryption keys are generated by encryptionalgorithms to ensure that every key is unique and unpredictable. The encrypted cipher text may be decrypted using the corresponding encryption key to obtain the plaintext back.

III. CURRENT ENCRYPTION STANDARDS

Strength of encryption is measured by the size of cipher key generated from encryption algorithm. Few of the encryption algorithms used are elliptic curve cryptography(ECC), RSA, PBE. Some of the encryption algorithms commonly used are Advanced encryption standard (AES), Data Encryption Standard (DES),RC4 and 3DES.

A. Password Based Encryption

Password based Encryption is a data scrambling technique that transforms an input data into binary encryption key. PBE uses additional parameters like salt and iteration count to derive the secret cipher. Salts are random numbers added to prevent dictionary attacks. This technique is prone to brute-force attacks.

IV. HONEY ENCRYPTION

One of the ways to provide security for passwords is with Honey Encryption. Ari Juels and Thomas Ristenpartdeveloped the honey encryption technique in 2014. The method Honey encryption outputs a cipher text, which if supplied and decrypted with any incorrect decryption key will be producing a believable plaintext.Therefore by providing with a false plaintext, Honey

Encryptionprovides assurance against Brute force attack. A brute force attack is one which involves continuous decryption attempts using random keys.This act is similar to selectingrandom plain textdata from the feasible plaintext space with a uniform distribution.

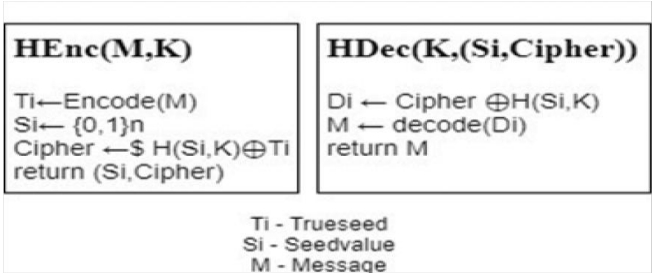

Fig 1: Honey Encryption and Decryption

V. HONEY WORDS

Honeywords are fake passwords which are savedalong with the true password to deceive the hacker. The core idea of using honey words is to confuse the attacker. In order to generate honeywords of an original password, different techniques such as Chaffing-with-tweaking, Chaffing-with-password model, passwords from leaked data sets can be applied.When attacker gets hold of the password file, they will be unable to distinguish between original password and honey words. These honey words are stored along with the original passwords and together they are referred as sweet words. Honeyencryption technique which is more efficient in terms of secure encryption of passwords.The honeyword generation method is implementedas following way: For every user Ui, the sweet words list Pi is produced or generated using the honeywords generation algorithm Generate (n).

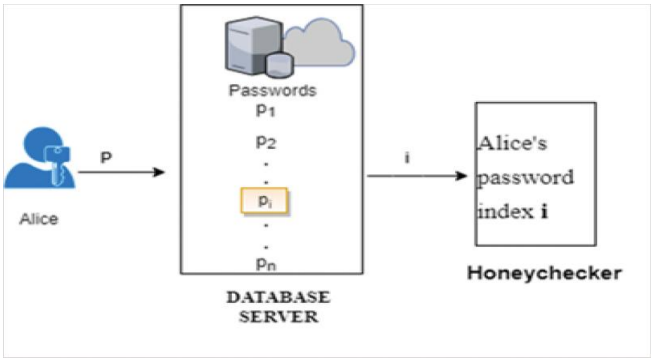

Fig 2: Honey words in database and Honeychecker validation

This function takes value of 'n' as input which is the number of sweetwords to be formedand then outputs the list of passwords Pi = (pi,1, pi,2,…. pi,n) and value Ci, where Ci refers the index of the user's original password. Username and the hashed values of the sweetwords are kept stored in the database of main server, whereas theindexCiis kept saved in another supplementary server known as honey checker.

A. Chaffing by tweaking method

This method involves tweaking or modifying theuserpassword in selected character positions to produce the honeywords. Each character in the user's password in a predefined locality is changed by a character of the similar typewhich is chosen randomly. For instance, digits, letters and special characters are identified and replaced with corresponding character respectively. The honey words generated using this scheme usually resemble original passwords.

B. Chaffing using a password model

In this model, the generator inputs the true password of the user and produces honey words using a probabilistic model. Herethe password is split into set of characters. For example, mypassword@123 issplitted as 10-letters+ 1-special character + 3-digits⇒L10+S1+D3 and replaced with the same composition like goldenring!209.

VI. EXISTING SYSTEM

Password Security is most essential in any organization since it is concerned about the privacy of its users and the reputation of the organization. Nowadays, it has become veryuncomplicatedtask to break a password hash with the recent improvements in Graphical process unit (GPU) technology. Any adversary can acquire access to a user's password by performing brute force attack on the password hashed value. On event of recovering the password, no server can detect the login attempt by illegitimate user (taking into account of usage of no extra mechanism). The existing system stores a single hashed password for a user in the database. The authentication system may use any hashing technique to hash user passwords. Still there are continuous hacker intrusions detected. Some of the biggest password breaches in Yahoo!, LinkedIn, eHarmony and Adobe were identified only after a large number of user data had been compromised.

This was because hackers perform offline password cracking attacks. They are aware of the password pattern and henceforth the number of combinations of a brute force attack is reduced.

VII. MOTIVATION FOR HE SCHEME

The following reasons are the main motivation for developing the HE scheme.

A. Use of weak passwords

Users tend to select weak passwords. A strong password must contain combination of letters (uppercase and lowercase), digits and special characters. The length of the password also reflects the strength. According to recent survey, most of the users have “password”, “123456”, “qwerty” as their passwords. These passwords can be easily cracked by dictionary attacks. Users also set the same password for multiple accounts. So if one of the site’s database is compromised, the hacker may apply the passwords for other sites also.

B. Vulnerability of weak hashing techniques

Weak hashing algorithms are the next reason for password cracking. LinkedIn passwords were easily cracked since they were hashed using the SHA-1 algorithm. EHarmonyused poor cryptographic techniques and passwords were MD5 hashed values. The company Yahoo!saved the password files as plain texts which is a very vulnerable method for storing passwords. A strong security mechanism is important for minimizing risks of breach. For this purpose the proposed work involves Honeyencryption over SHA_2 hashes.

VIII. PROPOSED SYSTEM

In our proposed system, the main key feature is the concept of Distributed Security. Here instead of using a single server to store the password data, we are going to make use of an additional supplementary server called Honey checker. The Honey checker database stores the correct index of the user password. The Honey word generation algorithm Generate(n) generates ‘n’ bogus passwords based on the user password. These passwords are hashed using SHA-2 hashing technique. Distribution Transformation Encoder (DTE) is arandom message encoding technique used to perform honey encryption on passwords. A DTE is a pair of DTE (Enc, Dec) algorithms. The Enc (encode) algorithm takes ainput as message M ∈M and gives outputs a value in a seed set S. This algorithm Dec (decode) will takea input as value S ∈S and gives as output a message M ∈M from the message space. A good DTE algorithm is correct if for any message M ∈M, Prob[Dec(Enc(M))=M]=1. When an incorrect decryption key is supplied to the ciphertext, a plausible honeyword corresponding to the seed is decrypted.The proposed model can be efficiently implemented in cloud applications to highly reduce cloud data breaches.

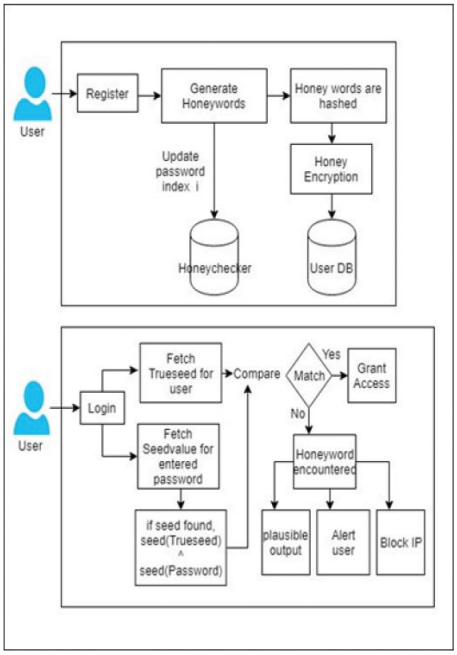

Fig 3. System Architecture of Proposed model

IX. SYSTEM DESIGN

The proposed model of Honey encryption involves password distribution and a seed space to decrypt the user password. Hence it is highly impossible for the attacker to figure out the seedvaluecorresponding to the password.It makes use of the concept of distributed security to ensure a more secure system. The proposed system model has the following modules.

A. Registration and Honey word Generation

When a user registers in the system, honey words are generated and hashed. The seed value of each sweet word is generated and stored in the Password Distribution database.

User	pwd1	pwd2	pwd3	pwd4	pwd5	pwd6
Alice	alice@123	Alice@892	Alic0$89	@lice@378	ALICE$58	alice0076
Bob	iambob67	iambob12	IAMbob30	i@mbob9456	iambob@123	iamb0b0

Fig 4. Generation of Honey words

The Honey encryption algorithm is applied over the message space and obtain the cipher text. Key space refers to the list of sweet words which are mapped to the seed space, which in turn is mapped to the message space (honey index of fake profiles).

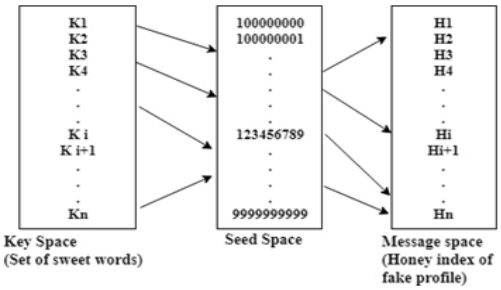

Fig 5. Password distribution table

B. Updating of Honey checker database

The Honey checker database is updated with index I of the true password. During login, this index for the user is fetched from the honeychecker databaseand passwords are validated. The honeychecker database must also be updated whenever the user changes their password.

User	Pwd_index
Alice	4
Bob	3
David	6
George	1

Fig 6. Update Honeychecker database

C. Authenticate login using honeychecker

The user logins using credentials. The Honeychecker validates for the true index of the password and validates the user. The hash value of the password given is matched with the password hash saved in database. If the match is found, then the user is allowed to login. If a honeyword is encountered, a potential possibility of an attack is identified and the page is redirected to a honeypot account.

D. Alert user about malicious login

If the Honey checker rejects that the user is not authentic, then the main authentication server initiates an alarm to user to change password.Notification is sent to the user with a mail whenever the action of an intruder is encountered. Notification will be sent to the user's mail either if the account is blockedor if any entry of honey words is detected. After three unsuccessful tries by intruder to access the account, the account is blocked. The admin may either monitor the hacker activities or block the IP address of the hacker to prevent from further access until necessary security actions are taken. During an attack scenario, the hacker performs an offline attack to guess the passwords and revert the hashes. When he tries to login to the user account using honey words a specified number of times, all the users password may be reset by the admin as a first aid measure.

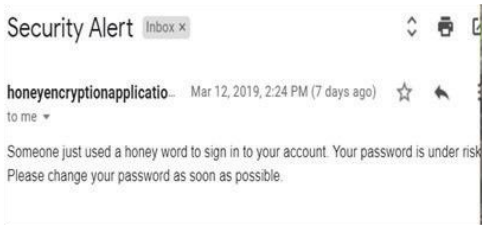

Fig 7. Alert user about malicious login

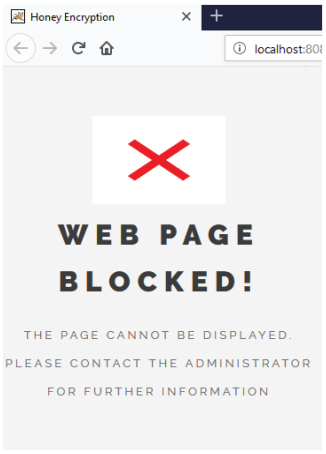

Fig 8. Blocked IP address

X. RESULT AND CONCLUSION

Thus, the complete description of the performance of encrypting algorithms is explained with the help of existing system. The brute-forcing attack is the main problem in password security and it is eliminated in the proposed system. The proposed model will provide a better data security to the user's password and can be effectively implemented in cloud platforms. The Honey encryption facility can be added as an additional feature of security in PaaS services in cloud. Our methodology also helps in early detection of password breaches and monitor the hacker behavior upon any hacking activity.

REFERENCES

1) Akshima,DonghoonChang,Aarushi Goel,SwetaMishra,Somitra Kumar Sanadhya "Generation of Secure and Reliable Honeywords, Preventing False Detection"IEEETransactions on Dependable and Secure Computing.
2) VasundharaR.Pagar, Rohini.GPise "Strengthening Password Security through Honeyword and HoneyEncryption Technique"International Conference on Trendsin Electronics and Informatics ICEI 2017.
3) NileshChakraborty,SamratMondal , "Towards Improving Storage Cost &Security Features of Honeyword Based Approaches",6thInternational Conference On Advances in Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India
4) Manisha JagannathBhole "Honeywords:A New Approach For Enhancing Security," International Research Journal of Engineering and Technology (IRJET) , Volume: 02 Issue: 08 | Nov-2015

5) Venkadesh.S,K.Palanivel, " A Survey on Password Stealing Attacks and ItsProtecting Mechanism", International Journal of Engineering Trends and Technology(IJETT)– Volume 19 Number 4 ,Jan 2015.
6) Ari Juels, Ronald L.Rivest "Honeywords:Making Password-Cracking Detectable"; International Conference on Science and Technology 2015, RMUTT,ACM SIGSAC Conf Compute.Commun. Security, 2013
7) Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords",IEEE Transactions On Dependable And Secure Computing, Vol. 13, No. 2, March/April 2016
8) Kelly Brown," The Dangers of Weak Hashes ",SANS InstituteInfoSec Reading Room
9) Ari Juels ,ThomasRistenpart, "Honey Encryption :Security Beyond Brute Force Bound",January 29, 2014,Version 1.1
10) Juels, A.; Ristenpart, T.,;Honey Encryption: Encryption beyond the Brute-Force Barrier ; Security Privacy, IEEE,vol.12,no.4,pp.59,62,JulyAug.2014
11) Vance, "If Your Password is 123456,Just Make It Hackme, " The New York Times,vol.20, 2010.
12) Prashant Dhas, Ismail Mohammed Efficient Approach for High Level Security Using Honeywords," IJARCSSE.
13) NirvanTyagi,Jessica Wang ,Kevin Wen ,DanielZuo"Honey Encryption Applications, " 6.857 Computer ;Network Security, Massachusetts Institute of Technology, Spring 2015