International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

SECURING CLOUD DATA UNDER KEY EXPOSURE

Hemalatha C
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
hemalathaemani2000@gmail.com

Mridula Shukla
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
mca@gmail.com

ABSTRACT

There has been immense increase in cloud use. It also stores and transmits information effectively, assists users at convenient times, and saves users and large organizations money. However, increased use of clouds has made it more difficult to keep things safe. This is so when we discuss the maintenance of the secrecy of keys. It can be bad when such keys get off in the locking or unlocking of data. Unscrupulous individuals may be able to access the information, alter the critical information or even disable the effectiveness of the cloud. This paper explores the possibilities of secret keys leakage in the clouds. It sees where these methods do not apply well in a situation where there are a lot of key holders in one physical area, besides checking how we currently attempt to secure keys. It proposes a more stringent arrangement. This system is applicable wherein new and powerful techniques of locking information are adopted, who enters into the system is verified with sufficient means and the key is admirably taken care of throughout its life. It also includes new things such as switching keys continuously, occurring freaky attempts to view keys, and hooking up with mechanisms developed to cloud security.

Keywords: *Risk of Key Leaks , Codes for Safety Storing Keys Safe, Swapping Keys*, *Spotting Odd Things, Sticking to Rules ,Keys Getting Out*

INTRODUCTION

As the number of persons and locations that use cloud tech increases, they store crucial and critical information on distant servers. Although it is also associated with development, convenience and reduced spending, cloud tools most importantly come with challenging safety concerns. As far as one risk is a leakage of encryption keys, which strikes at data safety and veracity. Lost keys can involve bad people to access important data, alter it or even interrupt services causing lost money and damage to its perceived image. This risk becomes greater in cloud spots accessed by a large number of users, where all the users are on a common setup and any leak has the potential of compromising more than a single user.

Such breaks are not necessarily prevented by old security measures, such as keeping keys in the same way or the use of simple rules to access things. Therefore, it is important to come up with robust systems capable of managing safety, despite partially or fully visibility of keys.

LITERATURE SURVEY

There are numerous researches on cloud safety, particularly, how to encrypt it, and safeguard keys. There are approaches such as Attribute-Based Encryption (ABE) Identity-Based Encryption (IBE) and Proxy Re-encryption (PRE) that have been considered in trying to provide users with a method of sharing data securely without being required to reveal the key. The group action of encryption computation on encrypted data has also been researched whereby we can be able to compute on encrypted data but retain the data and keys secure. The processes are quite useful in securing data and making it manageable and above all when one would like to play around with sensitive data without viewing the data. No matter how good the other areas of loss improvement may be, there remains one big problem which is yet to solve the key loss. The key to the clouds may be difficult to break but only safe key can make information storing there is safe. Weaker hold can be the storage, transmission or control of keys and that can be compromised by the malicious actors with unintended consequences and be used to access the information with undesirable consequences. Cloud web sites have higher chances to be modified to those people who can use them and have a lot of users and combine with third party services, which fail to secure keys. Older techniques such as leaving the keys outside in the same place, easy-to-crack passwords or a single verify of identity are not adequate anymore. This is why there is great need to come up with more mechanisms that can safely store keys. In the woundeds zone. All these have been taken into new designs and many people are addicted to data, part safe locks (HSMs),keys change regularly and keys are also often shared and that is where blockchain happens. Redundant checks, failure to detect anomaly and numerous steps to follow to get to parts of the body are just some of the processes present. Cloud spots have the tendency of removing most of the likelihoods of identification of keys.

EXISTING WORK

The more protection measures there are against cloud data, the more these take advantage of long-lasting and obsolescent measures of data and keystroke policy. The powerfulness and more practical locking systems such as AES (can be said to be an advanced lock improvement) is very effective as it is fast and adequate to grant protection to the larger degree of information in the process of transiting or in a transiting process in the storage medium. They have also deployed RSA lock and ECC lock as a variation of the lock to securely convey keys. Both practices are usually utilized in cloud-based teams to achieve improved performance: cloud-based teams tend to encrypt AES keys with ECC or RSA so that they can enjoy both speed and better security.

The system architecture utilized by SMs must be such

that keys are generated and stored in safe locations, and that these places are non-affected by the occurrence of tampering. Such system is applied to minimize the risk of unwanted access and meet laws and regulations, including GDPR and HIPAA. However, it is also possible to face enormous risks in the situation of leaking keys. To bring out the point when a component of KMS is compromised due to misconfiguration or through insider problems, or through attack and in the process steals the key, all the files that are locked concurrently then become exposed. SMS may be used to protect the keys against the physical attacks only but not against the software attack or the malicious insider attack.but it cannot be used to defend keys against software attacks and malicious insider attacks. Even the old methods of locking cannot avoid the leaks in case when the keys themselves are stolen and the groups are under great threat of losing the information

PROPOSED SYSTEM

The new plan means some approach to data lockup in steps or level, and sets some important use rules that are meant to decrease loss, in the case keys are found in cloud segments. That is not the way it works in the old systems whereby there is one key, one master key to everything because in this system we have hundreds of good stable places having keys, of high caliber codes and life changing key policies. This is possible where there is an attempt to make it strong enough that in the event involving the leakage of all or some of keys the cloud data is retained.

The significant thing about this suggestion is the multi level lock-up.

Instead of a key there is a huge set of keys the model and key actually dominant at a time.

These keys will be generated in secure, hit or miss, manner and distributed and stored in secure sites at a discreet distance of a KMS, HSMs and even block based key storage. This avoids the risks of a vulnerable piece in the sense that there is no module or even flawed It is possible to find this share that can leak absolute information. The interesting one additional fact is the keys are not fixed. They are already set up to wind up. This way the bad character cannot be able to wait when provided with a key. The destruction of the displayed key cannot be a time-consuming procedure since the keys are changed repeatedly. These are the basic changes that are assigned and enrolled and satisfied with strict rules. There are also more strident alternatives of who to screen in the case of users and bosses which are raised by the plan also. Such things as entry of keys and other sensitive tasks, are not merely pass codes but in addition also necessitate such things as body checks, one time codes or checks that involve, kit check, location and performance of the person. Not only does it build a redder door it also tracks out-of-pattern behavior things go haywire and produce a warning that give a hint that there is something wrong within or rough events to brute force a way inside that do not succeed. The last of interest is that keys are not eternal. More substantial ways of screening who comes and goes are also more in evidence, in the case of those users and bosses, who are also initially released by the plan. To

get keys and key tasks more than simple pass codes are needed body checks, one time codes, or checks that contain key, location, and how is the person acting. This is not only complicated to gain entry, but it also tracks any anomalous activity further warning things that hint to there is, or can be, trouble inside or brute force attempts at gaining entry that can be tracked.

METHODOLOGY:

The layout of the set is showed a clear framework that combines a lot of layers of code lock, script-based key management, strong in check-in and always watching. It enables embed key risk in cloud locations.

Step 1:Data lock with many Layers codes key data locked with heir many layer write styles, in that lot of 1 way and 1 key is used 1 by 1. For example AES will be used for swiftness information lock after that RSA or ECC for Key encryption.

Step 2: Key Split And Share Rather than storing whole keys in one place, the set-up employs secret share methods to split each key into fragments. These bits are stored essentially into isolated safe servers through such as KMS, HSMs or blockchain locations.

Step 3: Frequent Keys and Time Limited Change risks are reduced while keys have short period to be good and changed often. Old keys become null grounded, new keys render as safe and be distributed. Shifting of keys in accordance with the set plan saves the risk time and complies with the rules of the field.

Step 4 Numerous-checks for Key go-in Getting to the keys request numerous checks (MFA), body marks blended, OTP, & its verify for place. This ensures that even if fixed ways in leak, wrong people can access the lock key.

Step 5: Always Watching Looking Out for Stray Things The set-up installs in real-time viewing with correcting missteps Machine thinking examines how people and keys interaction, identify and detect weird acts, like unusual logs-in, or too many data probes. We handle matters that appear off, window blocks, or ask for new checks.

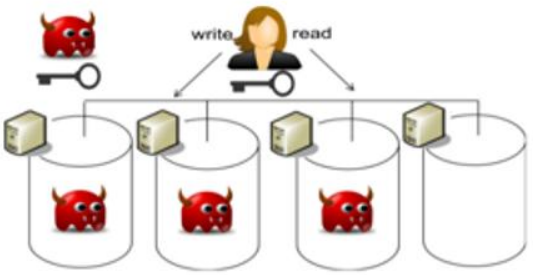

Fig.1. Block Diagram

Test Case	Purpose	Inputs	Expected Output	Postcondition
File Upload Test	Verify secure encryption before storing file in cloud.	File name, file data, user key	File is encrypted using multi-layer cryptography and successfully stored in cloud.	Data stored in encrypted form.
File Download Test	Ensure correct decryption with valid key.	Encrypted file, valid key	File is decrypted successfully and original data retrieved.	User gains access to data only with valid key.
Wrong Key Access	Prevent unauthorized access with invalid key.	Encrypted file, wrong/invalid key	Access denied, decryption fails, and error message displayed.	Unauthorized user cannot retrieve data.
Key Rotation Test	Validate smooth transition between old and new keys without downtime.	Encrypted file, rotated new key	File remains accessible with new key after rotation; old key becomes invalid.	System continues functioning securely.
Intrusion Simulation	Test system resilience under attack or anomaly.	Simulated intrusion/attack attempt	Unauthorized access detected, alert generated, and countermeasures triggered.	System logs intrusion and maintains data confidentiality.

Fig.2 Test case

EXPERIMENTAL RESULTS

The experiments conducted on the new system demonstrate that it functions satisfactorily to remedy the problem of key leakages in cloud locations. The findings demonstrate that the safety of data is enhanced by locking it with many codes, which cannot be accessed by anybody despite someone having a single key. That is, when one key is observed, it does not imply that all the information is lost and thus prevent a big risk in the old methods of locking by codes.

therefore separation of keys and placement in different locations were effective in preventing the failures all at once of all weak points. The fabricated attacks produced on the test could never enable the attackers to construct whole keys unless they had sufficient and sufficient key sections and thus the resilience of the secret sharing. The practice of super switching keys as well and having its key to become obsolete in the immediate course was useful in the system as well. With the speed factor, less work is added to the new format as compared to the first one. Operation to be keyed and lock and unlock was not too slow, especially when cloud was used. The other aspect that the system disputes is the whole time viewing and the weird attempts to have a swift entry. The experiments typically indicate that the new system was used to strengthen the security of the cloud when the keys were leaked.

Fig.3. Data Owner Registration

Fig.4. File Upload

Fig.5 Key Generation

CONCLUSION

This paper shows the massive challenge presented by keys leakage in the cloud systems which brings instability to the source of data security. Due to increased use of cloud services by organisations holding important information, encryption has become the main protective tool. Newer installations, though quite well in terms of hiding data, and trouble free key handling fall short when the keys are found. One leak can reflect substantial data loss, the undesirable access, and the loss of trust, which shows the real sufficiency of new techniques. These concerns apply well to the proposed plan which is highly encrypted and the control

of keys dissemedated and not on the reliance of a single key, or the boss. The likelihood that all the leaks occur despite the possibility that one of the keys may be intercepted becomes less likely because the information is encoded in multiple layers and keys that are encoded along with a secret procedure.Some of the cases involve an alternative that does not involve the biometrics At all, but are merely an added layer that is not there to enhance the maintenance of integrity parameters of elections on a permanent basis. The weight of both transparency and security rests upon the election officials in a pro portion to the ease of verification of the system. More to the point, keys that could be used over a period of time and which would be changeable on a regular basis would be more desirable. Useless keys are easily found by the threaten part, and this reduces the number of times these bad people end up using the keys. All these together helps to make the privacy, integrity and isolation of the data in the cloud superior and the best alternative compared to the customary set-ups. The second outstanding aspect of this research is its security design. Other than covering and control of keys, avenues of surveillance and detection of peculiar behaviour can be identified in many ways. Riding towards a tide which the future represents a great occasion in the further consolidation of such a blend.Future studies will be to further expand smart learning to pre-emptively identify main leaks being looked at and properly localize before location. Traditional ways of detecting threats are not able to detect new types of threats, which are easy to identify. by smart track. Aside from that, its security against new threats will be assured by considering the utilization of vital storage that has been developed based on blockchain and code-breaking techniques that are quantum-attack-resistant.

REFERENCES

[1] Boneh, D., & Franklin, M. "Identity-Based Encryption from the Weil Pairing". Zwischen Politik und populärer Kultur. This work shared a new way to lock and unlock info called Identity-Based Encryption (IBE) with the Weil pairing.

[2] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006).

The writers put forth Attribute-Based Encryption (ABE), which lets you set tight rules on who can see data based on their traits. This method lets you open info only if the user's traits match set rules.

[3] Hussain, Azham. "Securing Cloud Data under Key Exposure." *IIRJET* 3.4 (2018).

This talks about problem of losing secret keys in cloud use cases. It looks at the weak spots in current ways to lock and keep keys safe, shows their weak points when keys get out. The study puts forward better ways to lock and manage keys, aiming to make cloud data safer.