International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Special Issue 2; March 2018; Page No. 09-13

Confidential and secure key exposure in cloud environments

Pooja Vijay Bankar
Department of Computer Engineering, GH Raisoni College of Engineering, Ahmednagar, Maharashtra, India

Abstract

Present day statistics display a powerful attacker which breaks information confidentiality with the useful resource of acquiring cryptographic keys, thru the use of using way of coercion or backdoors in cryptographic software program application. On this paper, we positioned statistics confidentiality in opposition to an adversary to know the encryption key and has get admission to a massive fraction of the cipher text blocks. We've studied statistics confidentiality in opposition to an attacker who would possibly understand the encryption key. To this end, we endorse Bastion and modified RSA algorithm, a singular and green scheme that guarantees data confidentiality even supposing the encryption keys leaked and the adversary has access to almost all cipher text blocks. We have re-encrypted the cipher text formed by way of Bastion using modified RSA set of rules and encryption key have divided inside the blocks which might be on distinct servers. In order that although the adversary attempts to get the encryption key, he'll get half a part of the key and statistics confidentiality is preserved.

Keywords: encryption key, cryptographic, cloud

1. Introduction

Storage structures are hastily growing in degree the usage of an increasing number of and more disks, and through distribution over a system. With larger frameworks, the shot of phase disappointment additionally expands, so strategies to comfortable data become greater crucial. New plans are expected to at ease facts in opposition to diverse disappointments in a dispersed stockpiling framework. A general take a look at of appropriated scheme is to give information consistency at the same time as allowing screw ups and concurrent get admission to. In the meantime, one may need to get practical execution, to scale with number of clients, and to allow extension of capacity restrict readily. These issues are all around perceived, comprehended, and sensibly tended to for replication-based totally ability. For deletion coded capability, be that as it can, numerous plans are as but being proposed, as analysts inspect higher processes to manipulate the more complexity made by erasure codes. Usually, this many-sided first-class is because of a function coupling of facts in erasure codes, as we make clear similarly in the paper.

In this paper, we examine statistics confidentiality against an adversary which is aware of the encryption key and has got right of entry to a massive fraction of the cipher text blocks. The adversary can acquire the key both by exploiting flaws or backdoors within the key-generation software or by compromising the devices that shop the keys (e.g., on the user-side or within the cloud). As a long way as we are conscious, this adversary invalidates the safety of maximum cryptographic solutions, which includes those who guard encryption keys by way of mystery-sharing (considering the reality that those keys may be leaked as quickly as they may be generated). In present machine, fine Bastion is used to encrypt the statistics. To counter such an adversary, we recommend Bastion in addition to modified RSA, a unique and green scheme which guarantees that plaintext records cannot be recovered as long as the adversary has access to at most all but re-encrypted cipher text blocks, even when the encryption secret's exposed. Bastion achieves this by combining the usage of fashionable encryption capabilities with an efficient linear rework with modified RSA algorithm which ensures the high safety of the statistics. On this experience, Bastion stocks similarities with the belief of all-or-nothing transform and modified RSA set of rules generates a big bit encryption key for you to provide greater safety to touchy information.

Our contributions on this paper may be summarized as follows:

- We recommend Bastion in addition to changed RSA set of rules, a green scheme which guarantees statistics confidentiality against an adversary that is aware of the encryption key and has get entry to a huge fraction of the re-encrypted cipher text blocks.
- We analyze the safety of Bastion, and we show that it prevents leakage of any plaintext block so long as the adversary has get admission to the encryption key and to all but cipher text blocks. As well as modified RSA set of rules will re-encrypt the cipher text generated through Bastion and gives extra protection to the blocks.
- We compare the overall performance of Bastion and changed RSA set of rules analytically and empirically in contrast to a number of present encryption techniques. Our outcomes show that Bastion and modified RSA set of rules notably improves (through more than 50%) the overall performance of current Bastion encryption schemes, and most effective incurs a negligible overhead while as compared to existing semantically comfy encryption

modes (e.g., the CTR encryption mode).

- We discuss sensible insights with respect to the deployment of Bastion and modified RSA set of rules inside current storage structures, along with the HYDRA stor grid garage machine.

2. Review of literature

Ghassan O. Karame, Claudio Soriente, Krzysztof Lichota, Srdjan Capkun *et al*. [1] studied information confidentiality against an adversary which is aware of the encryption key and has get admission to a big fraction of the cipher text blocks. To this stop, they have got proposed Bastion, a unique and efficient scheme that guarantees statistics confidentiality regardless of the reality that the encryption key is leaked and the adversary has get admission to nearly all cipher text blocks. They analyze the safety of Bastion, and we look at its performance through a prototype implementation. Additionally they talk sensible insights with recognize to the integration of Bastion in business dispersed garage structures. This evaluation outcomes advocate that Bastion is properly-appropriate for integration in existing systems because it incurs less than five% overhead in comparison to existing semantically comfy encryption modes.

Sneha Singha, S. D. Satav *et al*. [2] introduces a concept of lessening the customer's secret key disclosure. On this paper, authors proposed a machine wherein de-duplication method of statistics is adopted and it will check the duplicacy of statistics and put off the redundant one using MD5 hashing. Also, it makes use of tile bitmap technique wherein it will test the previous and the modern-day variations of the statistics to ease the auditor's workload and to make the device more green.

L. Jagajeevan Rao *et al*. [3] shows that they have an inclination to research a manner to cut back the damage of the consumer's key exposure in cloud garage auditing, and presents the number one sensible decision for this new disadvantage putting. They formalize the definition and therefore the security version of auditing protocol with key exposure resilience and advocate the sort of protocol. They will be inclined to apply the binary tree structure and therefore the pre-order traversal approach to update the key keys for the patron. They conjointly develop a completely unique appraiser production to support the ahead safety and consequently the property of block much less verifiability. The protection proof and consequently the performance analysis display that the projected protocol is relaxed and competitively priced.

Prerna Yadav, Mrunal Badade, Swati Patil *et al*. [4] have proposed visitors and strength saving Encrypted seek (TEES), wherein with more bandwidth and better power green encrypted seek over a cellular cloud. The proposed structure gets rid of the computation from cell devices to the cloud, and consequently they in addition can optimize the communications of the mobile customers and the cloud.

Rongmao Chen, Yi Mu, Fuchun Guo and Xiaofen Wang *et al*. [5] investigated the security of a cryptographic primitive, namely Public Key Encryption with key-word search (PEKS) and suggest a brand new PEKS framework named twin-Server Public Key Encryption with key-word seek (DS-PEKS). As another predominant contribution, they define a logo new edition of the easy Projective Hash features (SPHFs) known as linear and homomorphic SPHF (LH-SPHF) and display a typical manufacturing of cozy DS-PEKS from LH-SPHF.

Hao Jin, Hong Jiang and Ke Zhou *et al*. [6] proposed a public auditing scheme with records dynamics guide and equity arbitration of capability disputes. Particularly, authors designed an index switcher to put off the drawback of index utilization in tag computation in cutting-edge schemes and advantage green handling of information dynamics. To deal with the equity trouble so that no celebration can misbehave without being detected, they similarly increase present danger fashions and undertake signature alternate idea to layout fair arbitration protocols, so that any feasible dispute may be fairly settled. The security evaluation shows this scheme is provably cozy, and the performance assessment demonstrates the overhead of information dynamics and dispute arbitration are reasonable.

Ayad F. Barsoum and M. Anwar Hasan *et al*. [7] proposed a map-primarily based provable multicopy dynamic facts possession (MB-PMDDP) scheme that has the subsequent features: 1) it presents an proof to the clients that the CSP isn't always dishonest via storing fewer copies; 2) it supports outsourcing of dynamic statistics, i.e., it supports block-stage operations, including block amendment, insertion, deletion, and append; and 3) it allows authorized users to seamlessly get admission to the document copies stored by way of the CSP. We provide a comparative analysis of the proposed MB-PMDDP scheme with a reference version acquired by way of extending current provable ownership of dynamic single-replica schemes.

Amos Beimel et al. [8] a secret-sharing scheme is a method by way of which a provider distributes stocks to events such that most effective legal subsets of events can reconstruct the name of the game. mystery-sharing schemes are an important tool in cryptography and they're used as a building box in lots of secure protocols, e.g., fashionable protocol for multiparty computation, Byzantine agreement, threshold cryptography, access manage, attribute-primarily based encryption, and generalized oblivious switch. In this survey, we describe the maximum critical structures of secret-sharing schemes; specially, we provide an explanation for the connections among secret-sharing schemes and monotone formulae and monotone span packages. We then speak the principle problem with known secret-sharing schemes - the huge percentage size, That is exponential in the number of events. We conjecture that that is unavoidable. We present the regarded lower bounds on the percentage length. Those decrease bounds are pretty susceptible and there is a massive hole between the decrease and higher bounds. For linear mystery-sharing schemes, that's a class of schemes based on linear algebra that consists of most recounted schemes, polynomial decrease bounds on the percentage duration are acknowledged. We describe the proofs of those decrease bounds. We additionally gift two effects connecting secret-sharing schemes for a Hamiltonian get admission to shape to the NP vs. coNP hassle and to a primary open trouble in cryptography - constructing oblivious-switch protocols from one-manner functions.

Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa *et al*. [9] the increasing recognition of cloud storage offerings has lead corporations that cope with important data to consider the usage of those services for his or her storage wishes. Scientific report databases, power gadget historic information and monetary records are a few examples of vital records that would be moved to the cloud. However, the reliability and safety of information saved inside the cloud nonetheless continue to be main worries. On this paper we present DEPSKY, a device that improves the deliver, integrity and confidentiality of statistics saved inside the cloud via the encryption, encoding and replication of the records on diverse clouds that shape a cloud-of-clouds. We deployed our machine the use of 4 business business enterprise clouds and used Planet- Lab to run customers getting access to the issuer from particular worldwide locations. We determined that our protocols advanced the perceived availability and, in most cases, the access latency when in comparison with cloud companies individually. Moreover, the economic charges of the use of DEPSKY, in this state of affairs is twice the cost of the usage of a single cloud, that is choicest and seems to be a reasonable price, given the blessings.

Charnes, J. Pieprzyk, and R. Safavi-Naini *et al*. [10] the techniques for changing thresholds in the absence of relaxed channels after the setup of threshold mystery sharing schemes. First, we construct a perfect (t, n) threshold scheme this is threshold changeable to t′ > t, that's ideal with recognize to the percentage size. This improves the scheme of Wang and Wong via enjoyable the requirement from q ≥ n + v to q > n with the secret-area F v q. However those threshold changeable schemes together with maximum formerly acknowledged schemes grow to be insecure beneath the collusion attack of gamers protecting preliminary shares. By including a published enforcement time period we enhance the model with collusion protection and N alternatives of threshold trade. Then we construct a computationally cozy scheme under the improved version, which involves an awful lot shorter stocks and broadcast messages than the best schemes. Ultimately, we talk the way to recognize the enrollment and disenrollment of gamers, and especially, how to deal with L-fold changes of get admission to polices.

3. System Overview

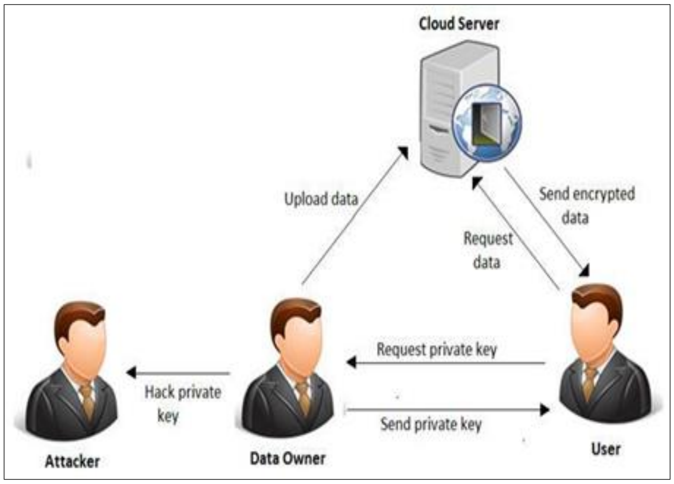

Fig 1: System Architecture

Fig. 1 shows system architecture which includes Data owner, User, Cloud server and Attacker or adversary. Information proprietor or Data Owner upload the statistics that is in encrypted form. It stores the records and while person request for statistics, cloud server ship it to the user. Once data uploaded on Cloud server, Data owner generates his public and private keys the usage of Bastion and RSA algorithms. Proprietor encrypt the information together with his private key the use of Bastion then it will likely be in cipher text form. Then the usage of modified RSA, this cipher text will be re-encrypt and new cipher text is stored on cloud server. When consumer request for private key, Data owner verifies the person's authority and send him private key. User, also known as consumer who consumes data uploaded by Data owner once he get the private key from owner. User is an authenticated person of cloud server. After authentication, user send private key request to the facts owner. After getting private key of the owner, he is capable of send the facts request to the cloud server. While cloud server send the information to the user, it will likely be in encrypted form. User decrypt the records the usage of private key and may get entry to the facts inside the file. Attacker is the individual that can breaks information confidentiality via obtaining cryptographic keys. He tries to hack the private key of the proprietor as owner generates his keys. And use the proprietor's personal key to get the statistics to expose the confidentiality of the data.

4. System Analysis

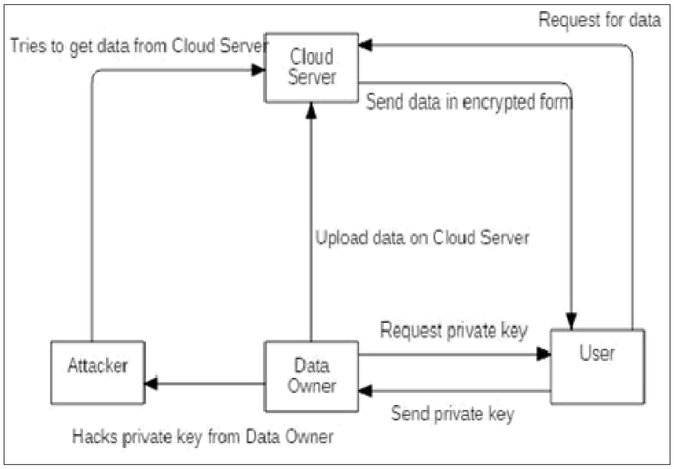
Request for data
Tries to get data from Cloud Server
Cloud Server
Send data in encrypted form
Upload data on Cloud Server
Request private key
User
Attacker
Data Owner
Send private key
Hacks private key from Data Owner

Fig 2: Block Diagram of Proposed System

Fig. 2 shows the block diagram of the proposed system which includes 4 modules as given below:

1) Cloud Server

In this module, Data owner upload the data which is in encrypted form. It stores the data and when user request for data, cloud server send it to the user.

2) Data Owner

Data owner generates his public and private keys using Bastion and RSA algorithms. Data owner encrypt the data with his private key using Bastion then it will be in cipher text form. Then using modified RSA, this cipher text will be re-encrypt and new cipher text is stored on cloud server. When user request for private key, data owner verifies the user's authority and send him private key.

3) User

User is an authenticated person of cloud server. After authentication, user send private key request to the data owner. After getting private key of the owner, he is able to send the data request to the cloud server. When cloud server send the data to the user, it will be in encrypted form. User decrypt the data using private key and can access the information in the file.

4) Attacker

Attacker is the person who can breaks data confidentiality by acquiring cryptographic keys. He tries to hack the private key of the owner as owner generates his keys. And use the owner's private key to get the data to expose the confidentiality of the data.

4. Mathematical Model

Let S, be a system such that,
$S = \{s, e, X, P, Mk, Sk, IDo, Ti, C1\ Y, f_{me}, DD, NDD, f_{friend}, MEM_{shared}, CPUCoreCnt, ф\}$
Where,
S - Proposed System
S - Initial state at T<init> i.e. constructor of a class.
Suppose the data owner wants to upload a file, the owner must be privileged user
k - Security parameter
msk - master secret key
ID - identity
Fi - file block
A1 - Adversary
C1 - Challenger
Ido - Original Client
s= {User, Data owner, cloud, key} Authentication involves following process
1) User must be a privileged one with valid username
2) He generates a key which he can use that for Decryption, another kind of authentication
3) The generated key will be stored at PKG with hiding
user's identity using his pseudonym.
e- End state of destructor of a class.

- Upload_Data().

X- Input of System. -Input files data.
Y- Output of System.

- Upload file successfully on cloud. Process= {user, file data, key}

Anonymization/encrypt and upload

-Once the file is checked in the cloud, if the cloud does not the file content, the file will be encrypted using Bastion algorithm and then re-encrypted using modified RSA algorithm before it got uploaded in the file.

De-Anonymization/decrypt and download

If the user wants to download contents from the cloud. User must specify the Private key used while uploading and download the file contents of the data It involves following procedures
1) Anonymized/encrypted data
2) User Private key

5. Result Analysis

Table 1: Result Analysis between Existing and Proposed System

Performance Measure	Existing Results	Proposed Results
Time cost required for encryption	For existing system it is recorded that the time required for encryption is more than proposed system due to algorithms used in existing is Bastion algorithm.	It is expected that for proposed system time cost required for encryption would not increases exponentially as re-encryption of data is shown but will scale accordingly keeping the time almost constant.
Time cost required for decryption	For existing system it is recorded that the time required for decryption is more than proposed system.	For proposed system it is recorded that the time required for decryption is less than proposed system.

Performance evaluation

Our proposed system solves the problem of security of documents while uploading implementing a secure and efficient access control mechanism across cloud platform with N users.

For overall performance degree we evaluate the computational overhead this is included in enforcing comfy re-encryption of information and get right of entry to manipulate mechanism. Computational overhead is involved in method of records re-encryption that's measured in terms of time price required to generate N blocks for report D uploaded through N users. As document length increases the number of blocks increases which incurs more security to be created thus increasing the time required for encryption.

For existing system it is recorded that the time required to generate the N blocks for document D will depend on size of document D as size increases time cost increases exponentially.

It is expected that for proposed system time cost required to generate N blocks would not increases exponentially but will scale accordingly keeping the time almost constant.

6. Some common mistakes

As per survey we have done, in existing papers data is not much secure as it can be in proposed system. In existing system only priority is given to the data and not to the encryption key. So that adversary or attacker can easily get the secure keys and can try to get the sensitive information from cloud. So in proposed system will resolve all the problems of existing system with Bastion and modified RSA as generated keys will be divided in blocks and data as well.

7. Conclusion

On this paper, we addressed the problem of securing statistics outsourced to the cloud against an adversary which has get admission to the encryption key. For that cause, we delivered a singular security definition that captures facts confidentiality against the new adversary. We then proposed Bastion and changed RSA set of rules, a scheme which ensures the confidentiality of encrypted records even if the adversary has the encryption key, and all however re-encrypted cipher text blocks. Bastion is maximum appropriate for settings where the cipher text blocks are saved in multi-cloud garage structures and modified RSA generates long bit encryption key so that statistics should remain relaxed even the adversary tries to decrypt it. As well as encryption key could be divided and can be saved within the blocks for more security. In these settings, the adversary could need to accumulate the encryption key, and to compromise all servers, in order to get better any single block of plaintext. We analyzed the security of Bastion and changed RSA and evaluated its overall performance in practical settings. Bastion and changed RSA drastically improves (through greater than 50%) the performance of present primitives which offer comparable security under key exposure, and best incurs a negligible overhead (much less than five%) when as compared to current semantically comfortable encryption modes (e.g., the CTR encryption mode). eventually, we showed how Bastion and changed RSA can together be practically included inside present dispersed storage systems.

In future, we will use more asymmetric algorithms to re-encrypt the records and might divide the information and keys in more range of blocks.

8. References

1. Ghassan, Claudio, Krzysz, Srdjan. Securing Cloud Data under Key Exposure‖, IEEE Transactions on Cloud Computing, 2017.
2. Sneha Singha, SD Satav. A Survey Paper on Cloud Storage Auditing with Key Exposure Resistance‖, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor 2014: 5.611.
3. JagajeevanRao L. Key Exposure in Cloud Data Services‖, International Journal of Big Data Security Intelligence. 2017; 4(1):15-20.
4. Prerna Yadav, Mrunal Badade, Swati Patil. TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud TEES (Traffic and Energy saving Encrypted Search)‖, International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified 2016; 5(10).
5. Rongmao Chen, Yi Mu, Fuchun Guo, Xiaofen Wang. Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage‖, IEEE Transactions on Information Forensics and Security, DOI 10.1109/ TIFS.2015.
6. Hao Jin, Hong Jiang, Ke Zhou. Dynamic and Public Auditing with Fair Arbitration for Cloud Data‖, IEEE Transactions on Cloud Computing, 2014; 13(9).
7. Ayad F Barsoum, Anwar Hasan M. Provable Multicopy Dynamic Data Possession in Cloud Computing Systems‖, IEEE Transactions on information forensics and security, 2015; 10(3).
8. Beimel A. Secret-sharing schemes: A survey, ‖ in International Workshop on Coding and Cryptology (IWCC), 2011, 11-46.
9. Bessani A, Correia M, Quaresma B, André F, Sousa P. DepSky: Dependable and Secure Storage in a Cloud-ofclouds,‖ in Sixth Conference on Computer Systems (EuroSys), 2011, 31-46.
10. Charnes, Pieprzyk, Safavi. Conditionally secure secret sharing schemes with disenrollment capability,‖ in ACM Conference on Computer and Communications Security (CCS), 199.