A Framework for Securing Decentralized Resources in Cloud Server Using Block-Chain

Dr. U. Nilabar Nisha[1], A.Dineshbabu[2], B.Nandhakumar[3], B.Anithkumar[4], B.Gowtham[5]
[1,2,3,4,5]*Computer Science and Engineering, Mahendra Institute of Technology*

***Abstract* - To handle the protected data set, a worker/hub in CSP must be "engaged" with two highlights preparing a worker secure processor and having the information base encryption key put away inside the processor chip. We allude these "engaged" workers/hubs as secure workers/hubs. A typical worker/hub (without neither worker secure processor nor data set encryption key) isn't equipped for handling the scrambled information base. To question the reevaluated information base, the data set proprietor speaks with a solitary secure worker as though the whole data set is put away in it. In CSP, rethought scrambled data set is parceled and put away in a circulated way, while the protected worker deals with the question handling on such disseminated information base. To address safety efforts of the information that has been circulated in the rethought data set has been prepared with different highlights which have been clarified as; the data set proprietor speaks with a solitary secure worker as though the whole data set is put away in it. In CSP, reevaluated encoded information base is apportioned and put away in a dispersed way, though the protected worker deals with the question handling on such disseminated data set. The ideal information of the client will be appropriated and put away in different number hubs which diminishes the opportunity of getting to information by the assailants. The stores his information in a specific cloud worker from which the worker circulates the client information into different number of hubs dependent on the accessibility and client execution. It expands the security of the client information that has been put away in the cloud. As of that the assailant appeared to be not able to get to the information as it has been disseminated to n - number of hubs which gives zero information about the information to the aggressor or the programmer who attempts to get the data put away by the client. Each client has been given unbalanced keys to get their information. Each time the client the client has been given awry keys for better security reasons. Furthermore, we propose nectar encryption calculation which holds the capacity of giving copy or void information to the assailant, on the off chance that the aggressor recovers the client information from the cloud worker.**

INTRODUCTION

A reasonable ongoing pattern in data innovation is the lease by numerous clients and ventures of the capacity/calculation administrations from different gatherings. With cloud innovation, what was in the past overseen independently now sees the association of workers, frequently in an obscure area, quickly reachable any place an Internet association is available. Today the utilization of these Internet providers commonly expects the presence of a Cloud Service Provider (CSP) dealing with the assistance. There are various components that clarify the current status. As a rule, the acquirement and the board of IT assets display critical scale economies, and huge scope CSPs can offer types of assistance at costs that are not exactly those brought about by more modest players. All things considered, numerous clients have an overabundance of computational, stockpiling, and organization limit in the frameworks they own, and they would be keen on offering these assets to different clients in return of a lease installment. In the old-style conduct of business sectors, the presence of a framework that upholds the gathering of market interest for IT administrations would prompt a critical chance for the making of monetary worth from the utilization of in any case under-used assets. This difference in scene is seen by the expanding consideration of the innovative work local area toward the acknowledgment of Decentralized Cloud Storage (DCS) administrations, portrayed by the accessibility of numerous hubs that can be utilized to store assets in a decentralized way. In such services, individual assets are divided in shards allotted (with replication to give accessibility ensures) to various hubs. Admittance to an asset requires recovering every one of its shards. The principle attributes of a DCS is the helpful and dynamic construction framed by free hubs (giving a multi-authority stockpiling organization) that can join the assistance and offer extra room, normally in return of some award. This advancement has been worked with by blockchain-based advances giving a successful low-rubbing electronic installment framework supporting the compensation for the utilization of the help. On stages like Storj, SAFE Network Vault IPFS, and Sia, clients can lease their unused stockpiling and data transmission to offer a support of different clients of the organization, who pay for this assistance with an organization digital money.

We expect the CSP in our model is straightforward however inquisitive. As a rule, it submits to any correspondence convention concurred with the information base proprietor and conveys data set tasks effectively. Any discernible altering can be secured by a legally binding arrangement between them. Nonetheless, this can't secure any detached assault leaving no follow on the framework (for example peruse/duplicate information from capacity circle, primary memory or test processor-to-memory information transport). The objective of an enemy is to peruse the substance of the data set without being identified. In outline, we think about the accompanying dangers and suspicions:

A foe can dispatch a malignant interaction or virtual machine (VM) or even gain admittance to the OS layer to duplicate or peruse the information in off-chip memory. He can likewise test the memory transport to peruse the information in processor-to-memory traffic. The correspondence channels between the information base proprietor and secure worker or among secure workers and secure hubs are largely open and subject to listening in. Code DB processor is thought to be the solitary confided in equipment in the framework. Other off-chip equipment parts are thought to be vindictive. The DBMS (with CypherDB programming support) is thought to be safely booted by utilizing secure boot innovation. Run-time Execution Validate can likewise be utilized to guarantee that the DBMS is running true to form. Side-channel assaults, for example, timing-assault or force investigation assault are not considered in this paper in light of the fact that these assaults are restrictively exorbitant to execute in a normal server farm climate. For sure, to dispatch these assaults, the assailant needs to penetrate actual security of the server farm, and this is profoundly improbable to occur. Any equipment altering on the processor is additionally thought to be infeasible in the cloud climate.

RELATED WORKS

K. Getgen: A way to deal with probabilistic danger evaluation of electrical framework establishing is proposed. The strategy utilizes all critical elements that influence the danger of electric shock at substations and considers their probabilistic nature. The methodology executes an exact factual portrayal of IEC479-1 fibrillation and body impedance information, and it utilizes nitty gritty PC reproductions of the demonstrated establishing framework to give security voltage appropriations that consider the person's quality at a site as an irregular variable. Variety in the force framework issue level is represented, and broad information of real framework flaw leeway time are incorporated. It is recommended that the probabilistic danger appraisal is used as a second phase of the establishing framework evaluation when the primary stage deterministic investigation requires costly or unreasonable alleviation. Execution of the second stage probabilistic danger appraisal yields a proportion of individual danger. This is then benchmarked against industry-acknowledged "as low as sensibly practicable" qualities to decide if interest in relief is required. To show the materialness of the proposed approach, the probabilistic danger evaluation is applied to a functional contextual analysis of a transmission substation.

C. Nobility: In this paper, another engineering for speeding up homomorphic work assessment on FPGA is proposed. The engineering depends on an equal reserved NTT calculation with a general time intricacy O(√N log √N). The engineering has been carried out on Xilinx Virtex 7 XC7V1140T FPGA that accomplishes a 60% usage proportion. The execution performs 32-digit 2 16 - point NTT calculation in 23.8μs which is a 2x speedup over the cutting-edge models. The design has been assessed by figuring a square of every one of the AES and SIMON-64/128 on the LTV and YASHE plans. The proposed design can assess the AES circuit utilizing the LTV conspire in a short time while preparing 2048 squares in equal. This prompts an amortized execution of 117 ms/block, which is the quickest exhibition answered apparently.

R. A. Popa: Open EHR is an open standard particular for creating adaptable electronic wellbeing record

(EHR) the executives framework. It characterizes the standard assistance models and APIs and offers an entire lifetime information stockpiling technique to the patient's record. As a significant OpenEHR framework segment, EHRServer assumes the part of back-end administrations vault for information stockpiling and question. It follows the openEHR details and embraces MySQL information base. Be that as it may, current EHRServer has numerous restrictions. For instance, its authority prerequisite burdens that one association can't get to the EHR possessed by different associations. The first EHRServer data set is in plaintext design. It can prompt the danger of electronic record spillage. Encryption is one normal assurance technique, yet the current EHRServer APIs do not uphold encoded information question. That confine building EHRServer on the cloud. In addition, the bother of data dividing between various associations may likewise upset the augmentation of OpenEHR inclusion to more spaces and nations. To tackle the above open issues, in this paper, we investigate two methodologies which ensure the security and adaptability of sharing EHR on the cloud and subsequently propose another design called Crypt-EHRServer. First and foremost, we use trait-based encryption to acknowledge adaptable EHR access expert for various approved associations. Also, we gain from an effective ciphertext question model, CryptDB, and embrace their onion encryption way to deal with help standard SQL inquiries on the scrambled EHR. The aftereffect of our work could give an adaptable, versatile and secure EHR framework. Tomb EHRServer will profit OpenEHR's far reaching appropriation on the planet and will likewise excite individuals' mindfulness about consolidating security standards into the plan of electronic wellbeing records the executives frameworks.

M. F. Kaashoek: Data mining is an incredible new method to find information inside the huge measure of the information. Various hypothetical and useful answers for question preparing have been proposed under different situations. With the new fame of distributed computing, information proprietors presently have the chance to re-appropriate their information as well as information preparing functionalities to the cloud. Due to information security and individual protection concerns, touchy information (e.g., clinical records) ought to be encoded prior to being moved to a cloud, and the cloud ought to perform inquiry handling assignments on the scrambled information as it were. These assignments are named as Privacy Preserving Query Processing (PPQP) over scrambled information. These conventions ensure the privacy of the put away information, client inquiries, and information access designs from cloud specialist co-ops and other unapproved clients. A few questions were considered trying to make a very much characterized scope. These inquiries incorporated the k-Nearest Neighbor (kNN) inquiry, progressed scientific question, and connected reach question. This paper presents conventions use an added substance cryptography base protection safeguarding information mining procedure at various phases of inquiry handling to accomplish the best presentation everything calculations should be possible on the encoded information.

S. Infuriate: With the quick increment of the Internet clients, network security turns out to be fundamental. Cryptography assumes a significant part in network security. In any case, cryptographic frameworks burn-through extensive measures of assets, similar to memory, CPU time, encryption and decoding time. In this paper, we analyzed the most well-known square code methods of activity on AES as per the suggestions of the National Institute of Standards and Technology (NIST). The correlation is done regarding encryption time, unscrambling time, and throughput with variable information parcel sizes. The aftereffects of the examination are summed up and our perceptions are featured to help settling on useful choice while picking the method of activities for various applications with symmetric-key codes.

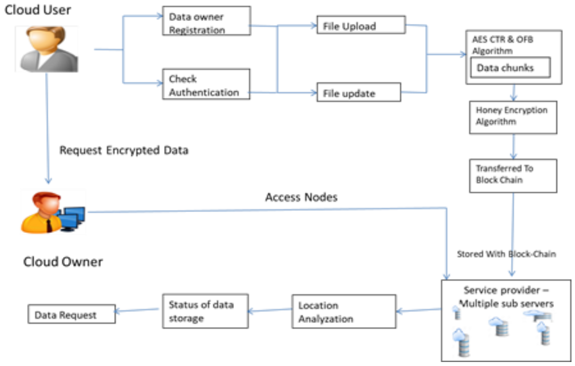
PROBLEM AND MODEL DESCRIPTION

Apparently, we propose the main protection safeguarding reevaluated LBS framework with multi-area inquiries and per-question security limit. We propose a novel inquiry conspire in which the client indicates areas of interest alongside a base protection degree and for every area A, the CSP returns a region B containing A that is adequately huge to fulfill the limitation on the base entropy. Critically, the CSP can't construe data about A past the way that it is contained in B. The proposed structure upholds search by area credits notwithstanding areas themselves. To empower proficient hunt over the encoded information, the LBSP readies a helper record construction and moves it to the CSP, which uses it during the inquiry. To develop it, the LBSP fabricates a various leveled file, which intently copies the geographic chain of importance of the areas. At that point, every hub in the list is supplanted by a Bloom channel addressing both the area and its ascribes. To shroud the looked through information and the example of the Bloom channel from the CSP, we encode the Bloom channel utilizing capacity concealing internal item encryption (FHIPE). The test, notwithstanding, is to permit the CSP to look by the area or area ascribes over the scrambled Bloom channel addressing both. To this end, we use the capacity of FHIPE to figure the quantity of coordinating with bits. Along these lines, the CSP decides if an inquiry vector coordinates with a list vector by independently contrasting the quantity of coordinating with bits for the area and for the ascribes. Because of this plan, the CSP can understand the pursuit without learning the conveyance of components in the Bloom channel. The epic acknowledgment of accessible protection safeguarding various leveled record for LBS information is a critical specialized commitment of this work. We investigate area protection given by the proposed strategy in Section 6. Our examination shows that the proposed conspire keeps area hidden from the LBSP under the semi-fair danger model. Moreover, our answer permits check of client membership (i.e., access control) without disregarding his protection. For this, we use daze marks to permit the LBSP to sign the inquiry without learning any data about it. We likewise utilize key approach attribute-based encryption (KPABE) to acknowledge fine-grained admittance control.

To address this security issue, there have been many proposed arrangements: utilizing homomorphic encryption or utilizing a trusted coprocessor. Notwithstanding, they are either inadequate or infeasible (with low productivity). In this paper, we propose a novel cloud framework engineering called Cipher-DB, which depends on re-planning the processor design to help subjective calculation on scrambled information. Our plan firmly couples data set encryption with our proposed engineering. With our technique, the scrambled information from the data set can be worked in our novel processors in a circulated and equal way. Our fundamental commitments are as per the following: apparently, this is quick to utilize processor structural plan to effectively secure distant procedure on scrambled data set against any legit however inquisitive director. We acquaint a novel methodology with scramble the data set that permits data set activity to be performed effectively and safely on secure processor in an appropriated data set framework. We propose a run-time memory apportioning framework to get on-the-fly execution with a novel utilization of programming straightforward reserve line encryption and for every question irregular key. We show that it is having the option to help discretionary data set activities, requires just an insignificant programming changes and accomplishes well execution with just 10% execution overhead all things considered.

DCS depends on re-planning the design to help security includes on scrambled information that has been put away in worker. It firmly couples information base encryption with this design. With this technique, the encoded information from worker/hubs can be worked in a safe way and inclined to assailants. Therefore, information are scrambled and moved to hubs, in which nectar encryption has been executed. As nectar encryption has been carried out assailants are denied from getting to information and aggressor gets a vacant document. Because of the presence of cryptographic measures alongside nectar encryption DCS has been gotten profoundly when contrasted and the current highlights. Square chain approach can be added to the DCS which guarantees the information security and keeps aggressors from getting to in an unapproved way. The data set proprietor demands a safe inquiry administration from CSP and indicates the assets required. The CSP assigns the assets as mentioned and sends every one of the public keys of the protected processors required to the information base proprietor. The information base proprietor sends all encoded data set encryption key inquiry encryption key and the computerized mark to the CSP.

SYSTEM IMPLEMENTATION



The cloud storage provider provides the storage space to the desired cloud owner. To access that storage the cloud owner has to register their required details and acquires the login details. After acquiring the details the owner can provide storage space the users. Each cloud owner has an individual and unique ID to access the account. Each user who can access the cloud storage can upload their desired data to the cloud storage server. The entire data will be in an encrypted format in the cloud server. The admin i.e.: the cloud owner can view the file details such as size, location and as well as the user can retrieve their data from the cloud server. The cloud owner verifies the secret key provided by the user to access the data. The user maintains the data privacy by using the honey encryption algorithm. Hence in case of attack of data the breacher cant access the user data. It has been done by the cloud owner i.e.: the server to gain the knowledge about the tracker or the attacker. After knowing the attacker details the cloud owner can block or make unavailable status to the attacker for accessing the data of the user. The data of the user has been stored with quiet higher security level. The cloud server transfers the user data into secure nodes to make the security of the user data. The data has been stored in multiple secure nodes so that the gains zero knowledge about the user data. If the user sends the request to the server to retrieve the stored data the server accesses the secure node and provides the data to the user. The cloud owner can view and block the attacker who tries to breach the data that has been stored in the secure node. The tracking of the attacker can be done based on identifying the IP or MAC address of the attacker. So that the data breacher can't access the data that has been stored in the secure node.

The Advanced Encryption Standard (AES), likewise known by its unique name Rijndael is a detail for the encryption of electronic information set up by the U.S. Public Institute of Standards and Technology (NIST) in 2001.AES is a subset of the Rijndael figure created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who presented a proposition to NIST during the AES determination measure. Rijndael is a group of codes with various key and square sizes. For AES, NIST chose three individuals from the Rijndael family, each with a square size of 128 pieces, yet three diverse key lengths: 128, 192 and 256 pieces.

The AES encryption calculation characterizes various changes that are to be performed on information put away in an exhibit. The initial step of the code is to placed the information into an exhibit; after which the code changes are rehashed over various encryption adjusts. The quantity of rounds is controlled by the key length, with 10 rounds for 128-digit keys, 12 rounds for 192-piece keys and 14 rounds for 256-bit keys. After duplication check is done, the deduplicated record is scrambled and transferred in the cloud. Encryption and decoding is accomplished for security reason. Unscrambling is accomplished for downloading the record. Public Key Cryptography, Or Asymmetrical Cryptography, is any cryptographic framework that utilizations sets of keys, public key which might be dispersed broadly, and private key which are known uniquely to the proprietor. This achieves two capacities: verification, where the public key confirms that a holder of the matched private key sent the message, and encryption, where just the combined private key holder can unscramble the message encoded with the public key.

As of late, many distributed storage administrations, for example, Box, Drop box, Media Fire, Sky Drive, Sugar Sync, have been accessible to little to-medium business, and person. These cloud-based capacity could be especially alluring for buyers by giving on request limit, minimal effort administration, and long haul chronicle. Besides, cloud administrations have carried incredible comfort to individuals' lives since shoppers can get to applications and information from the cloud anyplace on the planet and by means of any accessible gadget, like PCs, tables, and cell phones. Consequently, a lot more ventures and people have moved their information, like individual information and enormous file framework, into the cloud each day. The cloud has become a need to a considerable lot of us for individual, endeavor, and government use.

The cloud plans to lessen expenses and helps the clients center around their center business as opposed to being blocked by IT snags. The fundamental empowering innovation for distributed computing is virtualization. Distributed computing embraces ideas from Service Oriented Architecture (SOA) that can help the client break these issues into administrations that can be coordinated to give an answer.

In current period, burning-through interactive media is progressively turning into a fundamental piece of the everyday life for end clients to get to various frameworks, administrations, and applications. As increasingly more media content is by and large dangerously produced, content suppliers presently generally resort to distributed computing for media facilitating and sharing, as it can give efficient and on-request utilization of plentiful stockpiling and calculation assets. Regardless of the conspicuous advantages, sending the cloud media focus denies content suppliers' immediate power over the re-appropriated media content what's more, raises security concerns. Indeed, information divulgence regularly happens in certifiable distributed storage administrations. Thus, it is basically essential to install security in the cloud-based media sharing help plan from the earliest starting point, upholding access control so that solitary approved admittance to the rethought media content is permitted. To help access control for secure media partaking in the scrambled cloud media focus, fundamentally there are two generally well-known methodologies in the writing.

The primary sort of approach depends on property-based encryption (ABE), where a substance supplier can determine a related admittance structure over qualities, and subsequently the code text put away in the cloud must be unscrambled by clients whose credits fulfill that entrance structure. The last kind depends on intermediary re-encryption (PRE) where the cloud goes about as an intermediary to help delegate the decoding rights to approved clients in a controllable way. Contrasted and ABE, PRE could be more favorable as in, in ABE the substance supplier needs to download, decode, and re-encode information when access strategies change often. This work centers around PRE for secure media partaking in the scrambled cloud media focus.

Be that as it may, authorizing access control alone for secure media sharing would neglect to completely ensure the substance supplier's business advantages. Specifically, replicating media content is nearly sans cost, and the business interests of the substance suppliers would be hurt whenever approved clients later become double crossers that illicitly reallocate the media substance to people in general after they are approved with the decoding rights. For instance, reallocating a recently delivered film from a bought in client to the public damages the relating studio's benefit. Such danger ought to have been truly treated at this point is generally neglected by existing chips away at secure cloud-based information sharing. Along these lines, it is basic to invest secure cloud-based media offering to the ability of following illicit substance rearrangement.

RESULTS AND DISCUSSION

Decentralized distributed storage administrations address a promising chance for an alternate cloud market, satisfying the inventory and need for IT assets of a broad local area of clients. The dynamic and free nature of the subsequent foundation presents security worries that can address an easing back factor toward the acknowledgment of such a chance, in any case obviously engaging and promising for the normal monetary advantages. In this paper, we present a methodology empowering asset proprietors to viably ensure and safely erase their assets while depending on decentralized cloud administrations for their capacity. Our answer joins All-Or-Nothing-Transform for solid asset security, and painstakingly planned procedures for cutting assets and for their decentralized allotment in the capacity organization. We address both accessibility and security ensures, mutually considering them in our model and empowering asset proprietors to control their setting.

We introduced a methodology for giving successful secure insurance to assets in decentralized distributed storage administrations. Our methodology empowers asset proprietors to ensure their assets and to control their decentralized assignment to various hubs in the organization. We examined various procedures for parting and dispersing assets, investigating their attributes as far as accessibility and security ensures. We likewise gave a displaying of the issue empowering proprietors to control the granularity of cutting and enhancement of portion to guarantee pointed accessibility and security ensures. Empowering viable control for asset proprietors, our answer helps in eliminating regular hesitance because of safety concerns, furthermore, pushes a stride ahead in the acknowledgment of novel administrations successfully profiting by innovative advancement. Our work leaves space for augmentations, for example, the thought of mistake rectifying codes and data dispersal calculations to lessen the spatial overhead.

CONCLUSION

This paper presents a novel processor structural plan to perform secure and productive question preparing on a scrambled data set. With insignificant alterations to the data set application programming, our proposed processor design, CypherDB, can accomplish a higher security and execution productivity when contrasted and arrangements utilizing homomorphic encryption or trusted coprocessor. Our reproduction results show that it presents on normal 10% execution overhead and 14% executed guidance check overhead and 28% stockpiling overhead. Further decrease in the exhibition and guidance check overhead might be conceivable through register sharing of the trait seed and the program execution. Our work is being reached out in a few ways. One intriguing bearing is fuse our framework into an In-Memory information base climate, which conceivably is more proficient in getting to information. Another heading identifies with the utilization of vector handling in the advanced processor frameworks. At long last square chain has been carried out for better security and to keep up the whole framework and its information in a classified way.

FUTURE ENHANCEMENT

Re-planning the processor design to scramble the off-chip memory was additionally broadly contemplated. These methodologies use exclusively equipment component to scramble the whole off-chip memory, including the code and information, all in all. This intensely forbids information base virtualization in the cloud since re-encryption is required when the information moves from one stockpiling/ computational hub to another. Code DB, which scrambles the information base in its intelligent diagram, empowers the virtualization through a joined programming and equipment plan. So, in future the proposed plan might be utilized in mixture and local area cloud frameworks which is an effective worldview to keep up the client data and information in a proficient way. Because of unfathomable expansion in innovation the distributed storage clients has been massively expanded which makes the assailants just as the programmers to enjoy with the client information. All things considered the Cipher DB the proposed blueprint can be utilized for better execution assessment.

REFERENCES

[1] S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes,P. Hutchins, C. Pollard, and V. Buterin, “Storj: a peer-to-peer cloud storage network (v2.0),” https://storj.io/storjv2.pdf, Storj Labs Inc., Tech. Rep., 2016.

[2] D. Irvine, “Maidsafe distributed file system,” MaidSafe, Tech. Rep.,2010.

[3] G. Paul, F. Hutchison, and J. Irvine, “Security of the maid safe vault network,” in Wireless World Research Forum Meeting 32, Marrakesh, Morocco, May 2014.

[4] J. Benet, “IPFS-content addressed, versioned, P2P file system,” ProtocolLabs, Tech. Rep., 2014.

[5] D. Vorick and L. Champine, “Sia: Simple decentralized storage,” https://sia.tech/sia.pdf, Nebulous Inc., Tech. Rep., 2014.

[6] C. Patterson, “Distributed content delivery and cloud storage,” https://www.smithand crown.com/distributed-content-delivery-cloud-storage/, Smith and Crown, Tech. Rep., 2017.

[7] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, “Executing SQL overencrypted data in the database-service-provider model,” in Proc. of ACMSIGMOD, Madison, Wisconsin, June 2002.

[8] A. Shamir, “How to share a secret,” Communications of the ACM,vol. 22, no. 11, pp. 612–613, September/December 1979.

[9] E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, “Mix&Slice: Efficient access revocation in the cloud,” in Proc. of ACM CCS, Vienna, Austria, October 2016.

[10] N. Lambert and B. Bollen, “The SAFE network - a new, decentralised internet,” http://docs. maidsafe.net/Whitepapers/pdf/TheSafeNetwork. pdf,MaidSafe, Tech. Rep., 2014.

[11] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, “A survey on security andprivacy issues of bitcoin,”

IEEE Communications Surveys & Tutorials,vol. 20, no. 4, pp. 3416–3452, 2018.

[12] D. A. Patterson, G. Gibson, and R. H. Katz, “A case for redundant arraysof inexpensive disks (RAID),” ACM SIGMOD Records, vol. 17, no. 3, pp. 109–116, Jun. 1988.

[13] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability andintegrity layer for cloud storage,” in Proc. of ACM CCS, Chicago, IL, USA, November 2009.

[14] “Proofs of retrievability: Theory and implementation,” in Proc. Of ACM CCSW, Chicago, IL, USA, November 2009.

[15] M. Albanese, S. Jajodia, R. Jhawar, and V. Piuri, “Dependable and resilient cloud computing,” in Proc. of IEEE SOSE, Oxford, UK, March2016.