RESEARCH ARTICLE OPEN ACCESS

Efficient Auditing Scheme for Secure Data Storage in Fog to Cloud Computing

Dr.E.K VellingiriRaj[1] , Thasleema Nasreen.D

[1]Head of the Department, Department of Computer Applications, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.

[2]Final MCA, Department of Computer Applications, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.

Email: [1] girirajek@gmail.com, [2]thasleemanasreen31@gmail.com

ABSTRACT

Fog-to-cloud computing has now become a new cutting-edge technique along with the rapid popularity of Internet of Things (IoT). Unlike traditional cloud computing, fog-to-cloud computing needs more entities to participate in, including mobile sinks and fog nodes except for cloud service provider (CSP). Hence, the integrity auditing in fog-to-cloud storage will also be different from that of traditional cloud storage. In the recent work of Tian et al., they took the first step to design public auditing system for fog-to-cloud computing.

However, their scheme becomes very inefficient since they use intricate public key cryptographic techniques, including bilinear mapping, proof of knowledge etc. In this paper, we design a general and more efficient auditing system based on MAC and HMAC, both of which are popular private key cryptographic techniques. By implementing MAC and HMAC, we give a concrete instantiation of our auditing system. Finally, the theoretical analysis and experiment results show that our proposed system has more efficiency in terms of communication and computational costs

INTRODUCTION

The expression "distributed computing" is a hot popular expression in the IT world. At the back this extravagant wonderful saying there lies a right photo of the impending of processing for together in specialized viewpoint and social point of view. Still the expression "Distributed computing" is later yet the arrangement of incorporate calculation and capacity in spread server farms keep up with by outsider organizations isn't new one aside from it returned in way in 1990s close to with circulated processing approach like organization registering. Distributed computing is normal at give IT as a support

of the cloud clients on-request premise with better adaptability, accessibility, dependability and versatility with esteem registering model.So the start of distributed computing is exceptionally current peculiarities despite the fact that its root have a place with various old thoughts with new business, specialized and social points of view. According to the structural perspective cloud is clearly make on a current organization-based design and uses the organization administrations and add various advancements like virtualization and a few plan of action. In completely cloud is fundamentally a lot of item PCs network together in comparative or various topographical areas, working mutually to serve various clients with various require and responsibility on request support with the help of virtualization.

DEPLOYMNT MODELS

Sending models distinguish the kind of admittance to the cloud can have any of the four sorts of access: Public, Private, Hybrid and Community. The Public Cloud permit framework and administrations to be essentially accessible to the normal public. Public cloud might be less safeguarded in light of its trustworthiness, e.g., email. The Private Cloud permit framework and administrations to be accessible inside a culture. It offer superior wellbeing as of its private nature. The Community Cloud permit framework and administrations to be accessible by assortment of association. The Hybrid Cloud is blend of public and private cloud. Notwithstanding, the genuine way of behaving is perform involving private cloud as the non-basic way of behaving are perform with public cloud.

SERVICE MODELS

Administration Models are the idea model on which the Cloud Computing is base. These can be order into three fundamental assistance model as planned beneath:

- Foundation as a Service (IaaS)
- Stage as a Service (PaaS)
- Programming as a Service (SaaS)

There are a few other help model all of which can take the structure like XaaS, i.e., whatever thing as a Service. This can be Network as a Service, Business as a Service, uniqueness as a Service, record as a Service or Strategy as a Service. The Infrastructure as a Service (IaaS) is the virtually all fundamental degree of administration. Every one of the help model form utilization of the major assistance portrayal, i.e., each acquire the wellbeing and association instrument from the essential model

INFRASTRUCTURE AS A SERVICE (IaaS)

IaaS give work to essential belongings, for example, actual machines, virtual machines, virtual capacity, etc.In an IaaS structure, an outsider wellspring of hosts equipment, programming, servers, stockpiling and other framework deals with sake of its clients. IaaS supplier likewise mass clients' application and grasp undertakings along with framework insurance, backing and versatility improvement. IaaS stages offer incredibly adaptable assets that can be acclimated on-request. This make IaaS viable for jobs to are temporary, test or adjust out of the blue. Other uniqueness of IaaS climate incorporates the motorization of hierarchical errands, dynamic scale, work

area virtualization and strategy-based administrations.

IaaS shoppers pay on a for every utilization base, regularly continuously, week or month. a few supplier likewise charge buyers base on the amount of virtual machine space they use. This pay-more only as costs arise portrayal disposes of the capital cost of convey homegrown equipment and programming. In any case, client ought to notice their IaaS environmental factors straightforwardly to stay away from animal charged for unlawful administrations. Since IaaS supplier own the framework, framework overseeing and screen might form into all the more hard for clients. Additionally, on the off chance that an IaaS source experience personal time, client responsibilities may be impacted. For model, in the event that an industry is fostering another product innovation, it force be additional business to mass and test the capacity through an IaaS source. When the most recent programming is tried and predominant, it very well may be isolates from the IaaS environmental factors for an additional a traditional in-house activity or to set aside cash or free the assets for different ventures. Driving IaaS suppliers incorporate Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM Smart Cloud Enterprise.

RELATED WORK

Towards Trusted Cloud Computing Nuno Santos, Krishna P. Gummadi and Rodrigo Rodrigues propose Cloud processing foundations permit organizations to cut costs by rethinking calculation on-request. Nonetheless, clients of distributed computing administrations presently have no method for confirm the security and trustworthiness of their information and expansion. To address this difficulty to suggest the arrangement of a believed distributed computing stage (TCCP). TCCP empowers Infrastructure as a Service (IaaS) supplier, for example, Amazon EC2 to supply a shut box execution circumstance that ensures private doing of guest virtual machines.

Trust cloud process stage (TCCP) for guarantee the security and reality of calculations that are moved to IaaS administrations. The TCCP supply the idea of an impeded box execution circumstance for buyers VM, ensure that no cloud source advantaged administrator can study or mess with its satisfied. Also, before demand the assistance to open a VM, the TCCP permits a purchaser to continually and remotely decide if the help backend is activity a trust TCCP execution. This capacity stretches out the perspective on proof to the entire help, and along these lines permits a shopper to affirm assuming its computation will run firmly. In the arranged framework, tell the best way to impact the development of trust register innovations to design the TCCP.

SEEDING CLOUDS WITH TRUST ANCHORS

Joshua Schiffman and his co-creators propose the archive for the shoppers security risky information handling prerequisites are opening to push back firmly close to utilizing distributed computing. Cloud merchant run their calculation upon cloud supply VM frameworks, however

purchasers are concerned such host framework will be unable to safeguard themselves from assault, guarantee partition of shopper handling, or burden buyer handling appropriately. To give guarantee of information allotment assurance in mists to shoppers, client advocates technique to get better cloud clearness utilizing equipment based proof components.

The focal association of cloud server farm is ideal for check structures; empower the improvement of a reasonable methodology for shoppers to confide in the cloud stage. extraordinarily, suggest a cloud verifier administration that produce truth evidence for clients to affirm reality and access control authorization capacity of the cloud stage that safeguard the respectability of purchasers demand VMs in IaaS mists. However a cloud-wide verifier administration would there a significant framework be able to bottleneck, make clear that total proof empowers significant upward decrease. As a result, straightforwardness of information insurance assurance can be checked at cloud-scale.

The significant three test has been examine are that cloud supplier face when produce proof that can conciliate a client concerns: First that cloud vender supply a proof of information security assurance of their hosts and purchaser handling; Second proof have an unmistakable meaning to cloud customers; and Third confirmations can be create effectively and expertly in a distributed computing circumstance.

DOMAIN BASED STORAGE PROTECTION WITH SECURE ACCESS CONTROL FOR THE CLOUD

Nicolae Paladi, Antonis Michalas and Christian Gehrmann propose cloud computing has evolve from a talented idea to one of the fastest increasing section of the IT business. However, many industry and personnel continue to view cloud computing as a technology that danger revealing their data to unofficial users. To introduce a data privacy and honesty security machinery for Infrastructure as a Service (IaaS) clouds, which relies on trusted computing morality to provide obvious storage isolation between IaaS clients? The system also address the lack of reliable data sharing mechanism, by provided that an XML-based language framework which enables customers of IaaS clouds to strongly share data and clearly denies access rights approved to peers. The proposed improvement has been prototyped as a code extension for a accepted cloud platform. Full-disk encryption has emerged as a hard solution for data privacy defense and is also mention in as a solution to the “dirty disks" trouble. However, full disk encryptions create hurdle for data sharing, widely accepted as an necessary feature for cloud application. Despite the diversity of accessible open supply cloud organization platforms (e.g. Open Stack, Eucalyptus, Open Nebula), share of read-write permissions for shared data among collaborate tenant still leftovers an open trouble. The system get better and enlarge earlier work by adding up capability to both grant access to data to other IaaS cloud customers and allocate access permissions.

SECURITY ASPECTS OF E-HEALTH SYSTEMS MIGRATION TO THE CLOUD

Antonis Michalas et al future as endorsement of e-wellbeing arrangement advance, new registering standards, for example, distributed computing convey the plausible to get better proficiency in association clinical wellbeing report and assist with diminishing expenses. In any case, these valuable open doors present new

assurance risk which can't be unseen. In light of our expertise with convey a piece of the Swedish electronic wellbeing report association framework in a foundation cloud, we make an impression of principle supplies that should be estimated when move e-wellbeing framework to the cloud. Likewise, top to bottom another annoyance vector inbuilt to cloud organizations and there an original information protection and uprightness security gadget for framework mists. This installment intends to push supplant of best practice and training instructed in move community e-wellbeing framework to the cloud.

Representation of an electronic medical care framework are over twenty years of age. Scientists expected for a paperless clinical framework where patients and specialist's office can book courses of action by means of the Internet, make electronic solution and store their clinical record in a focal information base, effectively available from anybody with adept access privileges. During these years, there has been a steady raise in concentrate on center and monetary help plan to change available medical care frameworks and supply trustworthy and cost valuable e-wellbeing administrations. Both individual association, like Microsoft, Google and IBM, and city association bodies have being used strides towards e-wellbeing.

For model, top of the United States B. Obama, endorsed $38 billion to digitize the American medical care and figure that toward the finish of 2014 the country's wellbeing explanation will be completely electronic. Likewise, the Australian government put $20.3 million in "telehealth" project, Tasmania submit $1.8 million to refresh the data frameworks at risk for four of its public clinics, while Germany has presented the electronic wellbeing card a requesting mission in which generally guarantee Germans got a brilliant card among they can safely be in contact with various medical services partners (specialists, medical clinics, drug specialists and so forth) through telemetric.

SECURELY LAUNCHING VIRTUAL MACHINES ON TRUSTWORTHY PLATFORMS IN A PUBLIC CLOUD

Mudassar Aslam et al future the Infrastructure-as-a-Service (IaaS) cloud duplicate which permit cloud client to run their own virtual machines (VMs) on open distributed computing property. IaaS gives endeavors the choice to reevaluate their training jobs with negligible exertion and cost. Notwithstanding, one principle issue with open methodology of cloud rental, is that the client can get legally binding assurance concerning the respectability of the realistic stages. Reality that the IaaS client oneself can't affirm the source guarantee cloud stage trustworthiness, is an insurance peril which takes steps to stop the IaaS business in wide The creator address this issue and suggest a novel safeguarded VM send off convention utilizing trust Computing methods. VM send off convention permit the cloud IaaS client to safely join the VM to a trust PC game plan to such an extent that the undeniable message VM just will run on a stage that has been booted into a reliable state. The limits fabricate customer affirmation and can serve up as a huge empowering agent for make trust out in the open mists. To survey the possibility of our future convention through a full scale framework fruition and play out a framework assurance study. IaaS gives

undertakings the choice to rethink their technique jobs with littlest exertion.

A little organization without security ability or an ordinary IT administration client could trust a public cloud administration source and at times wish cloud administrations over self-facilitated administrations with a thought that their cloud provider can offer better insurance by select specific staff and tackle. In distinction, the larger part immense or normal size venture has higher security supplies for their own or their business client's delicate information; and assuming that their information is split the difference because of an insurance break in the cloud source organization, it will outcomes in serious lawful and business mishaps. Hence, these ventures are reluctant to pack their administrations in a public cloud except if they get trust ways of validating the authoritative insurance ensure give by the cloud source.

The focal point of our work is to start specialized method for affirming the security ensures give by the cloud administration source. To accomplish this by permit the cloud customer to cryptographically tie the purchaser virtual machine (VM) to a solid condition of the provisioned cloud stage. Likewise, to make sure that the absolute send-offs improvement meets generally expected principle assurance supplies of an excellent public help regarding confirmation and safeguarded move. As indicated by discretionary VM send off convention, a demanding VM isn't shipped off the source organization assuming no stage with the projected insurance assurances can be presented by the IaaS cloud.

EXISTING SYSTEM

In Existing framework a Data circulation framework model, there are complex client insurance that might encode as per their own particular manners, conceivably utilizing different arrangements of cryptographic keys. Renting every client achieve keys from every proprietor who's Their focal idea conversation in regards to the difficulty of totally Homomorphism Encryption (FHE) alone for VM Cloud seclusion. Their classification progressive system of VM Cloud Computing isn't average model and has not many inadequacies as we would discuss appropriately. The framework express the insurance and seclusion issue from a typical VM Cloud work out clarification and banter the difficulties convoluted for FHE as well as for a great deal of different procedures, yet this require an excess of trust on a lone power (i.e., bring the key escrow hardship).

RSA is a course of action wherein the keys needed to unscramble encoded information are confined in cryptography so that, underneath persuaded conditions, an authority outsider might develop admittance to people's keys. These outsiders might contain organizations, who might need admittance to laborers private associations, or legislatures, who might expect to be keen to vision the substance of scrambled interchanges.

PROPOSED METHODOLOGY

In this undertaking work we utilize Elliptical Curve Diffie Hellman algorithm(ECDH) as a Proposed System endeavor to learning the patient driven resolve the difficulty of assess a reason similarly by a few gatherings on their own bits of feedbacks safeguarded sharing of record partaking in VM Cloud put away on semi-confided in servers, and spotlight on

tending to the troublesome and testing key association issues. It additionally no notions are made on computational assets realistic with the gatherings. Every one of the gatherings would take out same measure of work which is in opposition to VM Cloud Computing setting.

To adjust these strategies for a deviated setting like VM Cloud Computing where the server has colossal amount of work out power comparative with the clients, In sort to safeguard the private wellbeing information put away on a semi-believed server, we acknowledge Diffie Hellman is improved than ECC as the primary encryption early stage.

Exact sub-par limits on hard calculations, however trouble scholars have had restricted accomplishment in laying out lesser limits by and large, so all things considered we reason relatively: we show that the hard computation are at littlest sum as hard as resolve some difficulty known or vague (generally the last option, because of motivations to be made sense of at the appointed time) to be hard.

The proof framework for making statements about the intricacy of one difficulty on the wellspring of another is referred to diminish as "Utilizing DH, access strategies are communicated in light of the characteristics of clients or information, which permit a persevering to specifically share her document circulation among a bunch of clients by encoding the record under a bunch of qualities, without the need to know a total rundown of clients. The intricacies per encryption, key creation and unscrambling are just direct with the quantity of qualities included.

SYSTEM METHODOLOGY

A total gathering key understanding arrangement commitment handle adjustment to bunch privileged insights resulting to all enrollment change act in the basic gathering correspondence framework. We recognize single and a few part tasks. Single part changes incorporate part join or leave. Leave happens when a part needs (or is compelled) to leave a gathering. While there strength be various purposes behind part leave - like deliberate leave, compulsory detach or constrained removal - we accept that gathering key understanding be expected to just give the instruments to change the gathering insider facts and surrender the rest to the higher-layer (application subordinate) assurance systems.

Various partner changes can likewise be additive and subtractive. We allude to the previous interaction as gathering converge, in which case at least two assortment converge into a solitary gathering. We allude to the last option as gathering divider, by which a gathering is parted into lesser gatherings. A gathering divider can happen for a long time two of which are genuinely normal: 1. Network disappointment - an organization occasion causes separation inside the gathering. Thus, a gathering is parted dependent on pieces some of which are singletons while others (those that safeguard common network) are sub-gatherings. 2. Unequivocal (application-driven) segment the application decide to part the gathering into numerous parts or prohibit different individuals on the double. equally, a gathering blend be in addition deliberate or compulsory:

1. Network shortcoming recuperate - an organization occasion makes before cut off network allotments reconnect. along these lines, bunches on all sides (and there may be multiple sides) of a past divider are converted into a solitary gathering.

2. Express (application-driven) join together - the solicitation settles on a choice to consolidate various prior bunches into a singular gathering. (The instance of concurrent different part expansion isn't covered.)

MODULES

- Registration and Encryption
- Database Storage
- Group Key Generation within the workgroup
- Keying and rekeying the group key
- Sharing the data within workgroup

Registration and Encryption:

The client module the client program was executed utilizing Java servers and a J Frame page that conjures the served. The client come in the information to be sent by means of the J Frame page which then, at that point, conjures the Client servlet. The servlet then scrambles this information utilizing the common key thing created by the Diffie-Hellman Key congruity calculation and the Data Encryption Standard (in ENCRYPT mode) and send it over to the server. The client present purposes URL Redirection to send the encoded message from the client to the head server.

DATABASE STORAGE:

The actual server is a straightforward servlet that is joined to a data set. It acknowledges the scrambled message from the client and unscrambles it utilizing the common key item make by the Diffie-Hellman calculation and Diffie Hellman (in DECRYPT mode).one time the message has been ecrypted the server will store the correspondence into the information base, which can be return at a later stage.

GROUP KEY GENERATION WITHIN THE WORKGROUP

The hubs in the workgroup resolve structure a gathering key. Each gathering part will cooperatively contribute its part to the widespread gathering key. The gathering key is produce in a common and causative style and there is no weak link. we are vanishing to create a gathering key. The gathering partner is organized in a legitimate key order known as a key tree. In the scattered key arrangement conventions we accept, nonetheless, there is no focal key server accessible. Additionally, a benefit of scattered conventions over the focal conventions is the increase in framework trustworthiness, in light of the fact that the gathering key is making in a common and causative design and there is no weak link.

To effectively save the gathering key in a functioning friend bunch with in excess of two partner we utilize the tree-based bunch Elliptic circular segment Diffie Hellman convention. Each part keeps a bunch of keys, which are concurred in a progressive double tree.

Each leaf hub in the tree stays discreet and dazed keys of a gathering part Mi. therefore, the mystery key held by the root hub is shared by all the part and is view as the gathering key. Key tree utilized in the tree-support bunch Elliptic Curve Differ Hellman convention.

Rekeying the gathering key which assets reestablishing the keys associated with the

hubs of the key tree, this is execute at whatever point there is any gathering participation change including any cluster of constituent joins the gathering. Rekeying implies another assortment key will be make by individuals in the gathering. Rekeying is additionally complete at whatever point there is any gathering participation change counting any clump of existing individuals takeoff the gathering. We track down that the previous advance toward play out all rekeying ventures at the kickoff of each rekeying time. This outcomes in high handling load during the update event and in that manner postpones the beginning of the safe gathering message. Consequently, we propose a more solid calculation which we call the Elliptic Curve Diffie Hellman calculation. Its nature is to lessen the rekeying transfer by pre-handling the joining individuals through the inactive rekeying time.

The Elliptic Curve Diffie Hellman calculation is isolated into two stages, in other words the Queue-sub tree section and the Queue-blend part. The primary section happens when in the world another part joins the correspondence bunch through the rekeying time. For this situation, we add this new part in a temporary key tree. The subsequent section occur at the initiation of each re key stretch and we combine the fleeting tree (which contains all recently joining individuals) to the realistic key tree.

With the help of gathering key produce by the individuals in the gathering, the information will be shared immovably among the gathering. The assortment individuals will divide the assets, in particular induction the records. We are applying this with RMI (Remote Method Invocation). This quality guides in building scattered demand

A far off object is one whose strategy can be appeal to from an extra Java virtual machine, possibly on an assorted host. A thing of this kind is portray by at least one far off interfaces written in the Java programming language. A direction to a far off item can be endorsed as a contention or return to accordingly in any procedure summon.

RESULTS AND DISCUSSIONS

Our Algorithm foster essential logical contemplations simplifying execution and likewise getting away from normal Attacks. Insurance adjust is helpful considering the way that future Algorithm is the premise of a couple of security principles and administrations on the web, and if the assurance. Diffie Hellman key compromise approach for key sharing gives a thought of being one of the special frameworks used as a component of training today.

The under tables from 4.2 to 4.11 show the system of making the directing table at each one hub these tables are build by trade of hi bundles at the hour of introduction of the organization to append dynamic bunch head. The test system utilized in the break down the Cloud in this undertaking is Java. This part gives impersonation arrangement to show execution of Energy Efficient weighted bunched Routing in the Communication sensor organizations. 50 Communication sensor hubs are conveyed haphazardly in a square area of 500m by 500 m, with uniform circulation. The parcel age rate is one bundle each second.

The proposed directing convention ECDH shows critical improvement over the current energy effective steering conventions like RSA, DSA as far as start to finish postponement and organization life time..

To assess the presentation of our calculation, we do the reenactment utilizing Net Beans(Java). A heterogeneous Cloud with 100 and 200 hubs for arbitrary reasons scattered in a glade with aspects 1000m× 1000m is determined.

For ease, to accept the Receiver is arranged in the focal point of the organization. The crash brought about by arbitrary factors, for example, signal impact and Communication direct point of interaction in all recreation tests, N was shifted somewhere in the range of 10 and 100 sensor hubs.

The hubs enthused for arbitrary reasons in every likely guidance. To work out the introduction of our strategies, we perceive loads to sensor hubs, w1 = 0.3, w2 = 0.2, w3 = 0.2, w4 = 0.2 and w5 = 0.1. To assess the introduction of the methods, we carried out the transmission assortment on the typical number of sensor hubs and deficient number of gatherings.

Bundles of 1000 bytes each, are moved among source and objective sets for a reproduction season of 150 seconds. The affirmation parcel size is 40 bytes. All the sensor hubs in the organization are store with a unique force of 50 Joules. The power depleted by a sensor hub in broadcast of information is the greater part of 0.38 Joules, in getting is 0.36 Joules. The hub consume a least sum force of 0.003 Joules, when it is out of gear state. The way of behaving of the organization is noticed for normal End-to-End delay, most extreme End-to-End postponement and organization lifetime. In these 50 hubs, 9 divergent sources to objective pair are with no obvious end goal in mind chose for one-bounce, two-jump, and more than two-jump foundation.

The Cloud processing as an innovation would be acknowledged whether the area of nervousness like insurance of the information will be encased with full confirmation component. The power of distributed computing is the fitness to oversee risk in demanding to somewhere safe issues. Our discretionary portrayal will introduce a diagram sketch of working to be acknowledge by planners worried in execute the distributed computing. Insurance calculations state for encryption and unscrambling and ways future to get to the media content can be execute in prospect to further develop security system over the organization.

The future framework finds our work by given that calculation executions and creating results to legitimize our ideas of assurance for distributed computing. For this way to deal with fill in as future, the cloud administration source need to co-work with the client in execute arrangement. Some cloud administration source base their business portrayal on the offer of client information to sponsors. These sources likely might want to consent to the client to involve their capacity in manners that monitor client security.

CONCLUSION

REFERENCES

[1] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, ‘‘Charm: A framework for rapidly prototyping cryptosystems,’’ J. Cryptogr. Eng., vol. 3, no. 2, pp. 111–128, Jun. 2013.

[2] S. Agrawal and D. Boneh, ‘‘Homomorphic MACs: MAC-based integrity for network coding,’’ in Applied Cryptography and Network Security, (Lecture Notes in Computer Science), vol. 5536. Berlin, Germany: Springer, 2009, pp. 292–305.

[3] G. Ateniese, R. Burns, R. Curtmola, Joseph Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, 2007, pp. 598–609.

[4] G. Ateniese, S. Kamara, and J. Katz, ‘‘Proofs of storage from homomorphic identification protocols,’’ in Advances in Cryptology. Berlin, Germany: Springer, 2009, pp. 319–333.

[5] A. F. Barsoum and M. A. Hasan, ‘‘Provable multicopy dynamic data possession in cloud computing systems,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485–497, Mar. 2015.

[20] H. Shacham and B. Waters, ‘‘Compact proofs of retrievability,’’ J. Cryptol., vol. 26, no. 3, pp. 442–483, 2013.

[21] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ‘‘An efficient public auditing protocol with novel dynamic structure for cloud data,’’ IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[22] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, ‘‘Dynamic-hash-table based public auditing for secure cloud storage,’’ IEEE Trans. Serv. Comput., vol. 10, no. 5, pp. 701–714, Sep. 2017.

[23] H. Tian, F. Nan, C.-C. Chang, Y. Huang, J. Lu, and Y. Du, ‘‘Privacypreserving public auditing for secure data storage in fog-to-cloud computing,’’ J. Netw. Comput. Appl., vol. 127, pp. 59–69, Feb. 2019.

[24] T. Wang, Y. Li, G. Wang, J. Cao, M. Z. A. Bhuiyan, and W. Jia, ‘‘Sustainable and efficient data collection from WSNs to cloud,’’ IEEE Trans. Sustain. Comput., vol. 4, no. 2, pp. 252–262, Apr. 2019.

[25] C. Wang, K. Ren, W. Lou, and J. Li, ‘‘Toward publicly auditable secure cloud data storage services,’’ in IEEE Netw., vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010.