Data Security and Privacy Protection for Cloud Storage Using BCH

Sameer. M. Patel [1], Mittal. B. Jain[2], Vaibhav. P. Vasani [3]
[1,2,3]B. Tech, Department of Information Technology K. J. Somaiya College of Engineering Mumbai, Maharashtra, India

Article Information

Received: 15-11-2023
Revised: 30-11-2023
Published: 15-12-2023

Keywords
Data Privacy, Bose Chaudhuri Hocquenghem Code Algorithm, Transport Layer Security framework, Software as a Service , Hash-solomon.

Correspondence Email:
meesalamani2003@gmail.com

Abstract

In recent technology cloud storage technology which is gaining more and more attention.. The protection of the secrecy of the arts relies for the most part on the fact that encryption technology while storing or processing the customer data. Our cloud-based, three-layer storage framework. The proposed framework can use cloud storage and protect secret information. The hash-Solomon coding algorithm is created for distinct portions, and it using data to divide it. The first part received the knowledge, if the knowledge is lacking, and it have lost. In the real world from the human point of view of which are the algorithms secure the data and use the knowledge and assurance of a bucket, and in accordance with what has been designed by the effective cause cannot be in the reason Furthermore, SaaS, According to the computational intelligence algorithm that can compute distribution clouds, fog, and machine, respectively, SaaS , the customer rejected their request in the accessible hosting environment via the network from various clients via application users. The customer was unable or unwilling to submit them to the controlling cloud infrastructure, especially in cloud settings like, with the exception of limited user-specific application configuration. For SaaS models, Google Apps and Microsoft Office 365 are good options.

1. Introduction

Cloud computing is a term used in the IT industry to denote a form of IT outsourcing service, similar to how energy is outsourced. Users are limited to using just. You don't need to say where the anxiety caused by electricity, how it occurred, or to transfer. For each day of the month, give it back. After cloud computing, the idea is similar to: The user can only use storage, computing power, is, or has been called upon with the development of the profession, for them is a work of the anguish of a freedom of those on the outside. Cloud is the Internet computer network diagram metaphor for how the Internet is depicted; how the removal of everything is hiding in the Internet infrastructure. There is a way in which the related count developers are "allowing users of Internet access technology (" cloud ") service is not knowledge or power technologies after servers.

And that the clouds with a great mist can be perceived and the means to count it and to give itself to the works, which is increased by the flow for an example of the difficulty of the thing [1]. The effects of fog on a large computer and computer system vary. However, a frequent approach that can be extracted is a limitation in the distribution of accurate material, and the issue is that developing and reviewing metrics to increase accuracy is difficult. Fog is networked via plane and data control plan in the data plane, for example, cloud computing allows metering to take place at the edge of network information services rather than on central servers. Compared to cloud computing, cloud computing emphasizes proximity to end users and a customer for some, dense geographic distribution and the pooling of local resources, latency for people and savings in bandwidth for mining edge analytics / flow; so that it becomes the top redundancy and user experience, it can only be, even if they did not use the AAL to pass, that the lack of missions.

To protect user privacy, we offer a framework according to the TLS cloud computing model. TSL is a power user management framework that can effectively protect user privacy. With which the interiors were barely able to attack. Traditional approaches to work without, and so on, in the attacks, but with the CSP is proportional to the difficulties, all the traditional ways of being null. In different traditional ways in our program, user data is divided into three sections with encoding technology of different sizes. Between North Korea and some of the key information to the abundance of all things except on their way. The data from the computer model fog will be stored in the cloud server in order of small to large. And recovered by an opponent of old age, if the knowledge is not certain knowledge in this way, it adorns the whole User. CSP and that it will not be useful information Without a cloud server and the name of the local server and whatever machine at the time of the world, and most certainly, only the cloud of users. The framework can make full use of cloud storage while maintaining data privacy. Cloud computing has piqued the interest of many people from various walks of life. The three-layer cloud storage divides data into three parts, and if one of these parts is missing, the data is lost. The bucket concept-based algorithms are used in this proposed framework. In this paper, we discuss the challenges of deep learning security and privacy.

1.1 Literature Review

A new secret preserving cloud services. Our solution is based on the nature of the signature for some of the anonymous in accessing cloud storage services to a group of agents that are not bilinear and that they are shared servers. Offers a new solution for anonymous authentication of registered users. It can be demonstrated without revealing the identity of users and cloud users can use their services without any profiling of threat behavior. However, if the user's provider violates the access right to be revoked. Our solution gives access to anonymous, and is transmitted to the knowledge of the secret of the possibility of dissociating. The proof-of-concept application to implement our solution and the results of this experiment. In addition, privacy solutions for cloud services execute a foolproof rule, and group signing of core skills to the role of privacy enhancing solutions for cloud services. From there, compare our performance with associated solutions and diagrams.[1]. Secret plans are the most widely used type of metric definition code, that is, an error correction code defining a forbidden space by prescription, increasing or decreasing the monotonic set. Then redefine to a new problem package, and the settings fix these errors is usually an opportunity to fix the error, but some code (taking into account this fresh metric and new package).[2]

It brings to light the problems of the disciples, and of the intellectual obfuscation, the finance and insurance industries are confidential information belonging to the name of the. The secret of authoritarian times is information that is hidden, so the danger of misuse of the thing. To be cut out and given to us in the name of the third part of the Software by the services of digital steel its heart and close to its mismanagement causing a preventive breach of confidentiality from the cloud, where enormous amounts of data are stored and maintained. Protecting user privacy is a major concern in today's cloud computing world. even with changes in the field of cloud computing to improve its efficiency, efficiency and optimization among developers. Office, etc., information reliability and cloud user identification and maintainability CPs.[3]. It is done as stated in the user's own information and today's technology is more related to my heart, do they work. No, but they have the cloud provider issue that is most important when it comes to data suggestions for cloud and digital data storage that you do, this way and that, and keep it. , worldwide. The reason for the need for the issues proposed

in cloud computing research. The digital data recorded in the cloud led us to Prevent Loss Model's Privacy offering (ppm, dDLC). This proposal aids the CR's confidence in proprietary data and cloud-based data.[4]. It is simple and its Internet environment can provide users, such as various offices, Software-in-Service, Order-at-Service, the risk of changes in the accuracy of the order of. It represents a consumer technology divided between various arts like Porta integrity of the audit mechanism.[5]. For-use-to-service the security of data with the users interacts and organizations cannot store their data in the cloud, the new commander, plaster encoded form, Merkle-hash-tree, construction. This secure data storage and an efficient storage cloud. This article discusses privacy and security architectures in day-to-day management in cloud storage.[6]. Later trying to kill the participation of new information on verifiable secret plans (vss). Define a new one for us, "metric" (the properties look slightly different from a standard Hamming meter). Error correction technique, of which it is well known that the VSS and distributed commitments in pairs by holding the test protocol and the error correction capability of the error correction codes establish interleaving.[7].

Internet of Things (IoT), smart cities, business digital transformation, and the global digital economy are among the newest emerging trends. On account of the huge data created, the continual expansion of data storage pressure drives the rapid development of the whole storage industry. Responsibility for business continuity in the digital secrecy project and in widely dispersed regions of the world, and close to its mismanagement causing a preventive breach of confidentiality from the cloud [8]. Security vulnerabilities from the past still exist in cloud computing systems. Traditional security techniques are no longer adequate for cloud apps and data as business boundaries have been stretched to the cloud. Cloud computing is having a huge influence on the subject of information security due to its openness and multi-tenant nature.[9]. Later look at a number of data storage security and privacy challenges and techniques in the cloud computing environment in this study the techniques employed in Cloud computing, where data security is a vital component. Integrity, confidentiality, and accessibility of data are all important considerations. As a result, personal data privacy issues and cloud-related technologies are being investigated. Data security and privacy have long been intertwined. By safeguarding data in the cloud, comparative data security and privacy studies may assist enhance user confidence.[10].

2. Research Methods

Cloud storage and to protect the full framework is able to capture secret information. It was cloud computing that caught the attention of another part of society. Stores and three layers of data cloud storage on different parts of the region in a single data point. If lose data and missing information. In this context, the proposed algorithms use the concept in the bucket. In this system is to use a bucket to reduce the time of the data processing concept and reduce waste. Our model used the BCH code algorithm (Bose Chaudhuri Hocquenghem). High, it is not flexible. BCH communication application code and there is only low redundancy shows in Figure 1.

2.1 Algorithm

2.1.1 Bucket

Access control bucket resource represented by access control lists (ACLs), Google cloud storage in the bucket. ACL to specify who has access to the information dump.
Stores and three layers of data cloud storage into three groups to separate parts of the data into one. If the lost the missing data and information.
Within the framework of this concept, according to the algorithms proposed, use the bucket.

2.1.2 BCH code algorithm

- Bose, Chaudhuri and Hocquenghem (BCH) codes to form a large and powerful type of random error correction, cyclic codes.
- This class is exceptional general code for many Hamming code error fixes.

- Then I came back with only a few codices, in the well-known binary BCH this form of reading. Solomon and BCH binary codes that are not in each other, and the Red Sea, like reading books known to all.

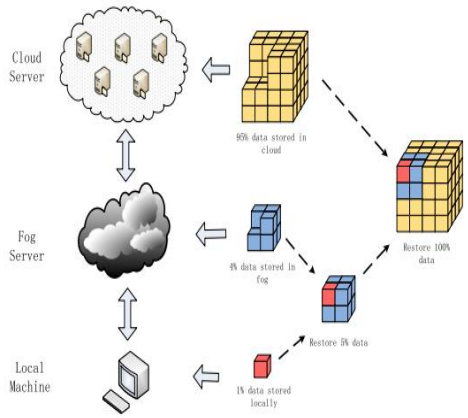

Fig 1. Date Security and System Architecture

To design a three-layer, fog-based storage computing framework. Here use data to divide hash-Solomon code to store data in different parts. First part received the knowledge, if the knowledge is lacking, and lost. In the real world from the human point of view of which are, the algorithms secure the data and use the knowledge and assurance of a bucket, and in accordance with what has been designed by the effective cause cannot be the reason. In addition, according to the computational intelligence algorithm which can calculate the amount of stored data and the 80% darkness distribution of 15% of the data and information on the local machine 5%, respectively.

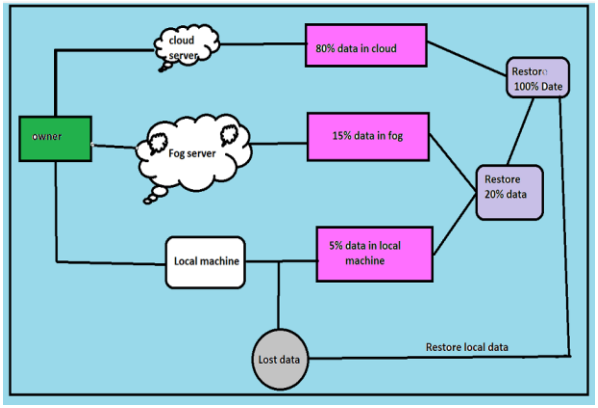

Fig 2. Fog cloud server communication

The frame can be full of cloud storage to protect secret information. This is cloud computing that has caught the attention of another sector of society. Cloud consumption technology treasures are given three places given the number of pieces. If lost the developer alcohol. In this context, the proposed algorithms use the concept in the bucket. In this system is to use a bucket to reduce the time of the data processing concept and reduce waste. Use the BCH code algorithm (Bose-Chaudhuri, Hocquenghem). High, it is not flexible. BCH code communication application, and there is only low redundancy.

As soon as the urge to speak ceases. The number of the contact line, wishing to satisfy the user, and the password, which the user enters there after having, to connect to the site. As a result, if the data contained in the user's information in a database table, it has been well taken care of whether the user's login to the website is something outside the work of the user and let it be known that there is no news from him now, they persist

in the correct login information. The link to register activity is also provided for users. A user who wants to register for the first login to access the web page. By clicking the record button on the connection activity, the operation enters the open registry. The contact number of the first tablets, which come into full swing from the name of the new user and the password. A user must enter confirmation in the confirmation of the box. When he enters information in the text boxes and presses the record button, the data is transferred to the database. Login or activity of the user. Then the user should go to the login web page. Because validations are applied to all text boxes, the proper functioning of the web page. The data is the name of the contact, or to confirm about it anything I understand or out of the textbox, but it's not empty after you have it. If there is blank text box application data in each text box, the report. The password in the password field and the confirmation registration information should also match, because they are in luck. Another healing contact number is true as one is at the root of X. If such registration fails, it will be violated and the user must then register again. When the protractor quickly reproduces a section of the field, that section is empty. If the correct television user login attention should be directed to the website.

In the module as a module, the user can store one of the tribes from his file server. This is what Our Lord was not given to the power of it was given after it was uploaded in cloud. The cipher gets three different layers. The data in each layer can use a different cryptographic algorithm that is encrypted and stored data . Sometimes users can recover from these three different files from cloud storage server to Local Fog server, server and machine. Here our model use data to divide code into different parts. The first part received the knowledge, if the knowledge is lacking. As cloud computing becomes more popular, it necessitates a new architecture for security purposes. As a result, users have access to all computer environments and may join or disconnect at any moment. Cloud data storage, like any other technology, will endure growing pains. It is still in its infancy and needs standards. Cloud computing, an emerging technology with tremendous computational and storage capabilities, breathes fresh life into wireless sensor networks (WSNs) and inspires a slew of new applications. However, due of WSNs' weak communication ability, especially for delay-sensitive applications, data transfer from WSNs to Cloud becomes a bottleneck, limiting their further development and uses. Many existing methods rely on multi-keyword exact matches or single-keyword fuzzy searches. In comparison to the multikeyword fuzzy search approach over encrypted data, they have very little practical importance in real-world applications. Wangg et al. proposed locality-sensitive hasing functions and bloom filtering to satisfy the purpose of fuzzy search in their first attempt to design a multi-keyword fuzzy scheme. Wang's throey worked for a single letter, but not all common spelling errors. Furthermore, his plan is to handle out-of-order issues during the renk process, and he hasn't considered the consequences shows in fig. 3.

3. Result and Discussion

Table 2. Performance Analysis and Result

TITLE	ALGORITHM	FUNCTION	LIMITATION
Data security and privacy protection for cloud storage	Bose chaudhuri Hocquenghem code algorithm	code was employed in this technique because cyclic codes can be used to create a large and strong type of random error repairs.	cloud data can be encrypted in three different ways, data stored in the cloud is more safe than data stored using conventional algorithms.
A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-citie	Attribute-based encryption	It is a technique which can be used in the cloud to solve many security issues. it can be concluded that our scheme is secure and can resist possible attacks	Since the cloud service is provided by the third party, the cloud is semi-trusted. Due to the features of cloud computing, there are many security issues in cloud computing.

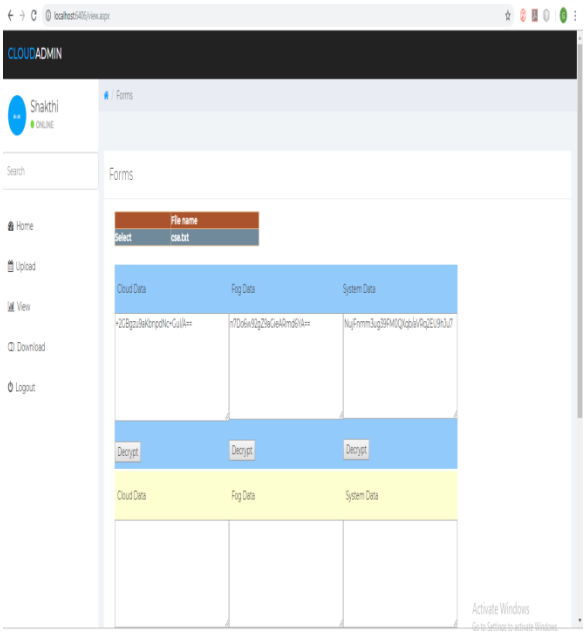

Fig 3. Encryption and Decryption process

The data that have stored in the cloud can be encrypted into three storage schemes (cloud, fog, and local machine) as shown in the diagram, with the data being more secure in the three storage schemes. When we need the data later, we can decrypt it using the decryption mechanism.

4. Conclusions

In a cloud computing program office, ts.Cloud, Here , to protect our data privacy in a cloud of fog under the TLS computer model to design the BCH algorithm by the analysis of theoretical mastery, the knowledge of the safety of such a man is, so that when an asset is achievable. During the experimental test, that can measure this formula, if unreliable encoding and decoding defines cloud storage. Otherwise, if you efficiency the index in order to design it reasonably and complete, so as to achieve the highest reliability, it is suitable for the rectilinear and to lure them into the coding matrix of Cauchy.

5. References

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Commun.Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments,” in Proc. IEEE Int. Conf. Commun., 2014,

pp. 2969–2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving data storage service in public cloud,” J. Comput. Res. Develop., vol. 51, no. 7,pp. 1397–1409, 2014.

[5] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, “Efficient data collection in sensor-cloud system with multiple mobile sinks,” in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.

[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[8] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.

[9] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.

[10] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), 190903.

[11] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.

[12] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.

[13] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), 190903.

[14] Shariati, S. M., & Ahmadzadegan, M. H. (2015, November). Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection. In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI) (pp. 1078-1082). IEEE.

[15] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, ''Simultaneous hardcore bits and cryptography against memory attacks,'' in Proc. TCC, San Francisco, CA, USA, 2009, pp. 474–495.

[16] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ''Provable data possession at untrusted stores,'' in Proc. ACM-CSS, New York, NY, USA, 2007, pp. 598–609.

[17] N. Attrapadung and H. Imai, ''Attribute-based encryption supporting direct/indirect revocation modes,'' in Proc. IMACC, Cirencester, U.K., Dec. 2009, pp. 278–330.

[18] J. Baek, R. Safavi-Naini, and W. Susilo, ''Public key encryption with keyword search revisited,'' in Proc. ICCSA, Perugia, Italy, 2008, pp. 1249–1259.

[19] M. Bellare, A. Boldyreva, and A. O'Neill, ''Deterministic and efficiently searchable encryption,'' in Proc. CRYPTO, Santa Barbara, CA, USA, 2007, pp. 535–552.

[20] F. Berti, O. Pereira, T. Peters, and F. X. Standaert, ''On leakage-resilient authenticated encryption with decryption leakages,'' IACR Trans. Symmetric Cryptol., vol. 2017, no. 3, pp. 271–293, 2017.

[21] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-policy attributebased encryption,'' in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, May 2007, pp. 321–334.

[22] T. Bhatia and A. K. Verma, ''Data security in mobile cloud computing paradigm: A survey, taxonomy and open research issues,'' J. Supercomput., vol. 73, no. 6, pp. 2558–2631, Jun. 2017.

[23] A. Boldyreva, V. Goyal, and V. Kumar, ''Identity-based encryption with efficient revocation,'' in Proc. ACM CCS, Alexandria, VA, USA, 2008, pp. 417–426.

[24] D. Boneh and X. Boyen, ''Efficient selective-ID secure identity based encryption without random oracles,'' in Proc. Adv. Cryptol. (Eurocrypt), Interlaken, Switzerland, vol. 3027, 2004, pp. 223–238.

[25] D. Boneh and X. Boyen, ‘‘Secure identity-based encryption without random oracles,’’ in Proc. CRYPTO, vol. 3152. Berlin, Germany: Springer, 2004, pp. 443–459.

[26] D. Boneh and M. Franklin, ‘‘Identity-based encryption from the Weil pairing,’’ in Proc. CRYPTO, vol. 2139. Berlin, Germany: Springer, 2001, pp. 213–229.

[27] D. Boneh, G. Di Crescenz, R. Ostrovsky, and G. Persiano, ‘‘Public key encryption with keyword search,’’ in Proc. EUROCRYPT, vol. 3027. Berlin, Germany: Springer, 2004, pp. 506–522.

[28] Z. Brakerski, ‘‘Fully homomorphic encryption without modulus switching from classical GapSVP,’’ in Proc. CRYPTO, Santa Barbara, CA, USA, 2012, pp. 868–886.

[29] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, ‘‘(Leveled) fully homomorphic encryption without bootstrapping,’’ ACM Trans. Comput. Theory, vol. 6, no. 3, pp. 1–36, Jul. 2014.

[30] Z. Brakerski and V. Vaikuntanathan, ‘‘Efficient fully homomorphic encryption from (standard) LWE,’’ SIAM Journal on Computing, vol. 43, no. 2, pp. 831–871, Jan. 2014.

[31] Z. Brakerski, Y. T. Kalai, J. Katz, and V.Vaikuntanathan, ‘‘Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage,’’ in Proc. IEEE 51st Annu. Symp. Found. Comput. Sci. (FOCS), Las Vegas, NV, USA, Oct. 2010, pp. 501–510.

[32] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ‘‘Privacy-preserving multikeyword ranked search over encrypted cloud data,’’ IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[33] B. Casemore, ‘‘Network modernization: Essential for digital transformation and multicloud,’’ IDC, Framingham, MA, USA, White Paper US45603019, Nov. 2019. [20] J. H. Cheon, A. Kim, M. Kim, and Y. Song, ‘‘Homomorphic encryption for arithmetic of approximate numbers,’’ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Hong Kong, 2017, pp. 409–437.

[34] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[35] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[36] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments,” in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.

[37] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving data storage service in public cloud,” J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.

[38] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, “Efficient data collection in sensor-cloud system with multiple mobile sinks,” in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.

[39] L. Xiao, Q. Li, and J. Liu, “Survey on secure cloud storage,” J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[40] R. J. McEliece and D. V. Sarwate, “On sharing secrets and reed-solomon codes,” Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[41] J. S. Plank, “T1: Erasure codes for storage applications,” in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[42] R. Kulkarni, A. Forster, and G. Venayagamoorthy, “Computational intelligence in wireless sensor networks: A survey,” IEEE Commun. Surv. Tuts., vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[43] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, “A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.