Data Security And Privacy Protection For Cloud Storage

Chittumothu Srividhya[1], Deepthi B[2], Dr.M.Preetha[3]
[1, 2] Dept of Information Technology
[3]Professor, Dept of Computer Science and Engineering
[1, 2, 3] Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, Tamil Nadu

Abstract- *In this paper, we focus on the development of cloud computing technology with the explosive growth of unstructured data, cloud storage technology gets more attention and better development. The cloud provider does not have suggestions regarding the information and the cloud data stored and maintained globally anywhere in the cloud. The privacy protection schemes are usually based on encryption technology. There are many privacy preserving methods in the side to prevent data in cloud. We propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Here we are using Hash-Solomon code algorithm is designed to divide data into different parts. If the one data part missing we lost the data information. In this framework we are using bucket concept based algorithms and secure the data information and then it can show the security and efficiency in our scheme. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively Software as a Service (SaaS): Client releases their application on a hosting environment which can be accessed through network from various clients by application users. The client does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings. Google Apps and Microsoft Office 365 are the examples for SaaS.*

Keywords- Data security, privacy of data in each server, bucket concept, recovery of lost data.

I. INTRODUCTION

Cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. By this method, the attacker cannot recover the user's original data even if he gets all the data from a certain server. As for the CSP, they also cannot get any useful information without the data stored in the fog server and local machine because both of the fog server and local machine are controlled by users.

II. LITERATURE SURVEY

In [1] Privacy-preserving security solution for cloud services.A novel privacy-preserving security solution for cloud services. Our solution is based on an efficient nonbilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authentication for registered users. Thus, users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity, and users can use cloud services without any threat of profiling their behaviour. However, if a user breaks provider's rules, his access right is revoked. Our solution provides anonymous access, unlinkability and the confidentiality of transmitted data. We implement our solution as a proof of concept application and present the experimental results. Further, we analyze current privacy preserving solutions for cloud services and group signature schemes as basic parts of privacy enhancing solutions in cloud services. We compare the performance of our solution with the related solutions and schemes.

In [2] A secure data privacy preservation for on-demand cloud service.A novel hand gesture recognition algorithm based on Kinect. Using the depth and skeleton from Kinect, mark-less hand extraction is achieved. The hand

shapes (depth) and corresponded textures (color) are represented in the form of super pixels, which better retain the overall shapes and color of the gestures to be recognized. Based on this representation, a novel distance metric, Super pixel Earth Mover's Distance (SP-EMD), is proposed to measure the dissimilarity between the hand gestures. The effectiveness of the proposed distance metric and recognition algorithm is illustrated by experimental results and a high mean accuracy of 98.8% for hand gesture recognition is achieved based on the joint color-depth SP-EMD.

In [3] A Survey on Secure Storage Services in Cloud Computing. Cloud computing is an emerging technology and it is purely based on internet and its environment. It provides different services to users such as Software-as-a-Service (SaaS), PaaS, IaaS, Storage-as-a-service (SaaS). Using Storage-as-a-Service, users and organizations can store their data remotely which poses new security risks towards the correctness of data in cloud. In order to achieve secure cloud storage, there exists different techniques such as flexible distributed storage integrity auditing mechanism, distributed erasure-coded data, Merkle Hash Tree(MHT) construction etc. These techniques support secure and efficient dynamic data storage in the cloud. This paper also deals with architectures for security and privacy management in the cloud storage environment.

In [4] On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Codes.We try to shed a new insight on Verifiable Secret Sharing Schemes (VSS). We first define a new "metric" (with slightly different properties than the standard Hamming metric). Using this metric we define a very particular class of codes that we call error-set correcting codes, based on a set of forbidden distances which is a monotone decreasing set. Next we redefine the packing problem for the new settings and generalize the notion of error correcting capability of the error-set correcting codes accordingly (taking into account the new metric and the new packing). Then we consider burst-error interleaving codes proposing an efficient burst-error correcting technique, which is in fact the well-known VSS and Distributed Commitments (DC) pair-wise checking protocol and we prove the error-correcting capability of the error-set correcting interleaving codes.

In [5] A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities. With the accelerated process of urbanization, more and more people tend to live in cities. In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. 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. Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation.

In [6] Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things.Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification and resolution raises the demands of computation, communication and storage capabilities. Therefore, we have proposed the fog computing based face identification and resolution framework to improve processing capacity and save the bandwidth. However, there are some security and privacy issues brought by the properties of fog computing based framework. In this paper, we propose a security and privacy preservation scheme to solve above issues. We give an outline of the fog computing based face identification and resolution framework, and summarize the security and privacy issues. Then the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are proposed to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution. Finally, we implement a prototype system to evaluate the influence of security scheme on system performance. Meanwhile, we also evaluate and analyze the security properties of proposed scheme from the viewpoint of logical formal proof and the CIA (confidentiality, integrity, availability) properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation.

In [7] Survey on Privacy-Preserving Methods for Storage in Cloud Computing. At present the mankind are progressively relying more on a number of online storage stores to back up our data or for using it in real time which gives an anywhere, anytime access. All these services bring

with it, concerns of security and privacy weaknesses for all the services provided by them since the user‟s data are stored and maintained out of user‟s premises. This paper portrays the various issues associated to privacy while storing the user‟s data on third party service providers, which is more commonly termed as cloud service. Cloud computing refers to the fundamental infrastructure for an up-coming model of service provision that has the benefit of dropping cost by sharing computing and storage resources, united with an on-demand provisioning mechanism depending on a pay-per-use business model. Without appropriate security and privacy solutions designed for clouds this computing paradigm could become a huge failure. There is a lot of research being made to spot out the issues with these cloud service providers and cloud security in general. This paper is on regard of one of the key issue -privacy that occur in the context of cloud computing and analyze the various works being done to solve the issues in privacy and thus to ensure privacy to outsourced data on cloud storage.

In [8] Survey on Secure Storage in Cloud Computing. Cloud Computing is an environment for providing information and resources that are delivered as a service to end-users over the Internet on demand. Thus cloud enables users to access their data from any geographical locations at any time and also has brought benefits in the form of online storage services. Cloud storage service avoids the cost expensive on software, personnel maintenance and provides better performance, less storage cost and scalability. But the maintenance of stored data in a secure manner is not an easy task in cloud environment and especially that stored data may not be completely trustworthy. Cloud delivers services through internet which increases their exposure to storage security vul¬nerabilities. However security is one of the major drawbacks that preventing several large organizations to enter into cloud computing environment. This work surveyed on several existing cloud storage frameworks, techniques and their advan¬tages, drawbacks and also discusses the challenges that are required to implement secure cloud data storage. This survey results help to identify the future research areas and methods for improving the existing drawbacks.

In [9] Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things.Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification and resolution raises the demands of computation, communication and storage capabilities. Therefore, we have proposed the fog computing based face identification and resolution framework to improve processing capacity and save the bandwidth. However, there are some security and privacy issues brought by the properties of fog computing based framework. In this paper, we propose a security and privacy preservation scheme to solve above issues. We give an outline of the fog computing based face identification and resolution framework, and summarize the security and privacy issues. Then the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are proposed to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution. Finally, we implement a prototype system to evaluate the influence of security scheme on system performance. Meanwhile, we also evaluate and analyze the security properties of proposed scheme from the viewpoint of logical formal proof and the CIA (confidentiality, integrity, availability) properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation.

In [10] A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities.With the accelerated process of urbanization, more and more people tend to live in cities. In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. 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. Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation

III. EXISITING SYSTEM

Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. the computer technology has developed rapidly. Cloud computing has gradually matured through so many people effort’s. In current storage schema,

the user's data is totally stored in cloud servers. If the user lose their right of control on data and face privacy risk. The privacy protection schemes are usually based on encryption technology. These kinds of methods cannot effectively resist attack from the inside of cloud server. Changes in the understanding of risk as a result of extending the datacentre into the cloud. Low latency and location awareness

IV. PROPOSED SYSTEM

Cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency.

The framework can take full of cloud storage and protect the privacy of data.Here the cloud computing has attracted great attention from different sector of society.The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.In our system we using a bucket concept so reduce the data wastages and reduce the process timings.

We are using a BCH (Bose–Chaudhuri–Hocquenghem) code algorithm. It's High flexible. BCH code are used in many communications application and low amount of redundancy.

SYSTEM ARCHITECHTURE

A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing. The privacy preservation is our focus, some active attacks are beyond the scope of this work. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms. We are using a BCH code algorithm. It's High flexible.

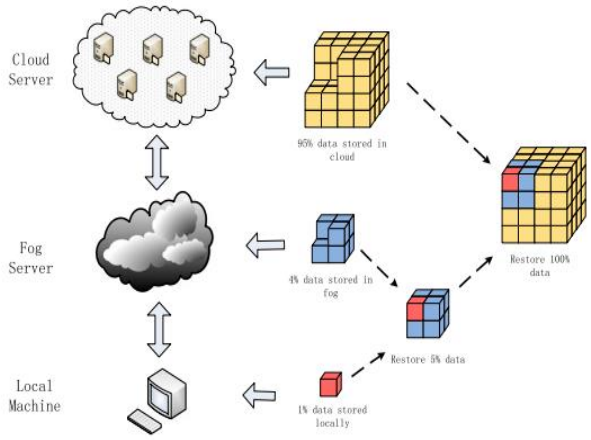

Figure 1: SYSTEM ARCHITECTURE

V. ALGORITHM USED

Cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms

BUCKET

The Bucket Access Controls resource represents the Access Control Lists (ACLs) for buckets within Google Cloud Storage. ACLs let you specify who has access to your data and to what extent.

BCH CODE ALGORITHM

The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes.This class of codes is a remarkable generalization of the Hamming code for multiple-error correction.We only consider binary BCH codes in this lecture note. Non-binary

BCH codes such as Reed-Solomon codes will be discussed in next lecturenote.

VI. RESULT

Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively Software as a Service (SaaS): Client releases their application on a hosting environment which can be accessed through network from various clients by application users. The client does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings. Google Apps and Microsoft Office 365 are the examples for SaaS.

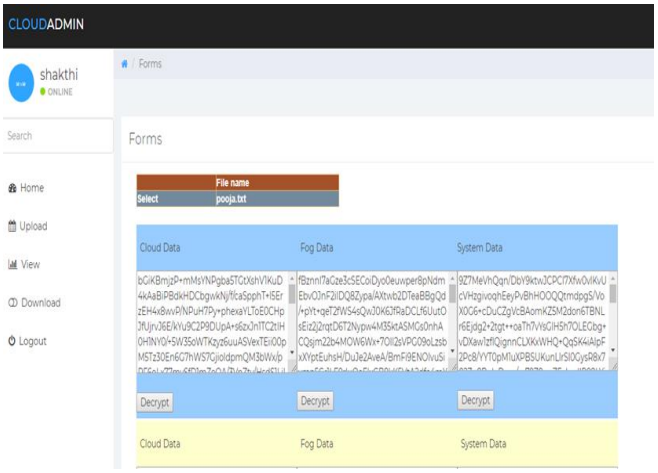

Figure 2: STORAGE SCHEME

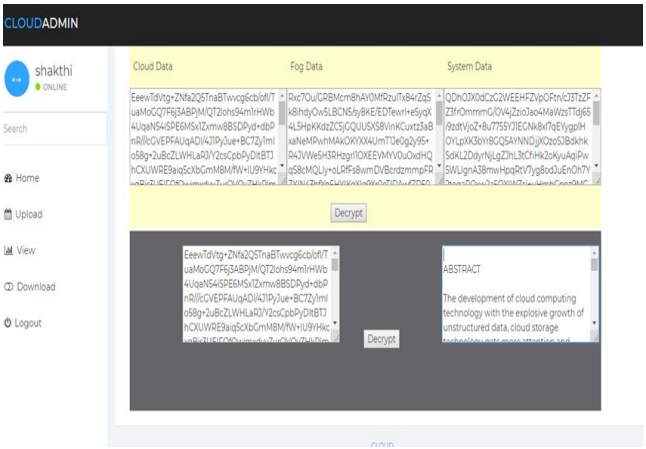

Figure 3: RECOVERY MODULE

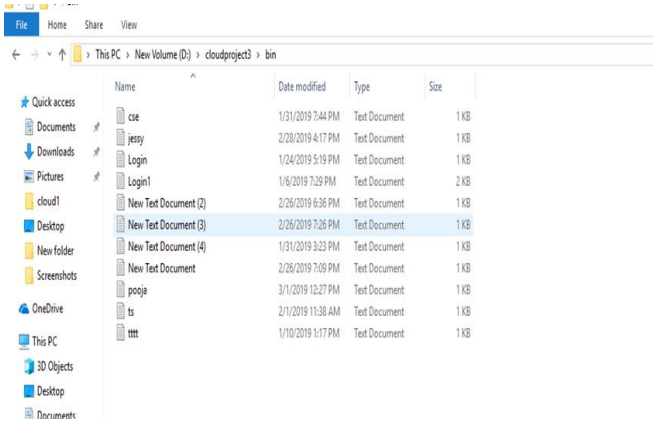

Figure 3: BUCKET MODEL

VII. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and itresultsintheseparationofownershipandmanagementofdata.Ino rdertosolvetheproblemofprivacyprotectionincloud storage, we propose a TLS framework based on fog computing model and design a BCH Code algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. Furthermore, we design a reasonable comprehensive efficiency index, in order to achieve the maximum efficiency, and we also find that the Cauchy matrix is more efficient in coding process.

In future, we are going to implement real-time cloud in this concept like amazon web services for additional security.

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 cloudcomputing: Architecture, applications, and approaches,” Wireless Commun.MobileComput., 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 datastorage 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 collectionin 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. DataAcquis.Process., vol. 31, no. 3, pp. 464–472, 2016.

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

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

[9] 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.

[10] 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.