

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

## Achieving Secure Cloud Data Using AES Algorithm

A. S. Roshini, P. Vithya, S.S.Sugania

B.E Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Old  
Mamallapuram Road, Padur, Chennai, India

Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Old  
Mamallapuram Road, Padur, Chennai, India

**ABSTRACT:** Secure pursuit strategies over encoded cloud information enable an approved client to inquiry information documents of enthusiasm by submitting scrambled question catchphrases to the cloud server in a protection safeguarding way. In any case, practically speaking, the returned question results might be mistaken or deficient in the exploitative cloud condition. For instance, the cloud server may deliberately preclude some qualified outcomes to spare computational assets and correspondence overhead. In this manner, a well-working secure inquiry framework ought to give a question comes about check system that enables the information client to confirm comes about. In this paper, we outline a protected, effectively incorporated, and fine-grained question comes about confirmation instrument, by which, given an encoded inquiry comes about set, the question client not exclusively can check the rightness of every information record in the set yet in addition can additionally check what number of or which qualified information documents are not returned if the set is inadequate before unscrambling. The check plot is free coupling to concrete secure inquiry procedures and can be effectively coordinated into any safe question conspires. We accomplish the objective by building secure check question for scrambled cloud information. Moreover, a short mark strategy with greatly little stockpiling cost is proposed to ensure the credibility of confirmation protest and a check question ask for method is introduced to enable the inquiry client to safely get the coveted check protest. Execution assessment demonstrates that the proposed plans are down to earth and proficient.

**KEYWORDS:** Cloud Computing, Query results verification, Secure query, Verification object.

### I. INTRODUCTION

In a search process, for a returned query results set that contains multiple encrypted data files, a data user may wish to verify the correctness of each encrypted data file (thus, he can remove incorrect results and retain the correct ones as the ultima query results) or wants to check how many or which qualified data files are not returned on earth if the cloud server intentionally omits some query results. This information can be regarded as a hard evidence to punish the cloud server. This is challenging to achieve the fine-grained verifications since the query and verification are enforced in the encrypted environment. We proposed a secure and fine-grained query results verification scheme by constructing the verification object for encrypted outsourced data files. When a query ends, the query results set along with the corresponding verification object are returned together, by which the query user can accurately verify: (a) the correctness of each encrypted data file in the results set; (a) how many qualified data files are not returned and 3) which qualified data files are not returned. Furthermore, our proposed verification scheme is lightweight and loose-coupling to concrete secure query schemes and can be very easily equipped into any secure query scheme for cloud computing.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

However, some necessary extensions and important works need to be further supplied to perfect our original scheme such as detailed performance evaluation and formal security definition and proof. More importantly, in the dishonest cloud environment, the scheme suffers from the following two important security problems: (a) Just as possibly tampering or deleting query results, the dishonest cloud server may also tamper or forge verification objects themselves to make the data user impossible to perform verification operation. Specially, once the cloud server knows that the query results verification scheme is provided in the secure search system, he may return in veracious verification object to escape responsibilities of misbehavior. (b) When a data user wants to obtain the desired verification object, some important information will be revealed such as which verification objects are being or have been requested before frequently, etc. This information may leak query user’s privacy and expose some useful contents about data files. More importantly, this exposed information may become temptations of misbehavior for the cloud server.

## System Objective and Scope

Essentially, the secure search is thus a technique that allows an authorized data user to search over the data owner’s encrypted data by submitting encrypted query keywords in a privacy-preserving manner and is an effective extension of traditional searchable encryption to adapt for the cloud computing environment and motivated by the effective information retrieve on encrypted outsourced cloud data.

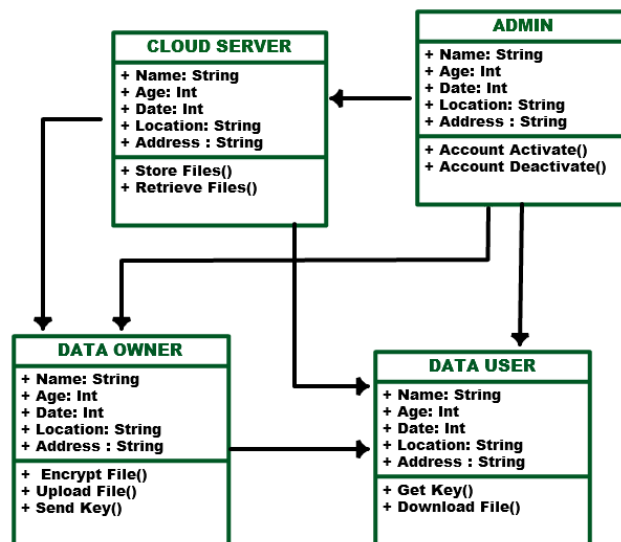


Fig.1 Proposed System Working Block Model

The secure keyword search issues in cloud computing have been adequately researched which aim to continually improve search efficiency, reduce communication and computation cost, and enrich the category of search function with better security and privacy protection. A common basic assumption of all these schemes is that the cloud is considered to be an "honest-but-curious" entity as well as always keeps robust and secure software/hardware environments. As a result, under the ideal assumption, the correct and complete query results always are unexceptionally returned from the cloud server when a query ends every time.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

## II. SYSTEM ANALYSIS

### A. Existing System Summary

A matter of public concern is how to guarantee the security of data that is outsourced to a remote cloud server and breaks away from the direct control of data owners. Encryption on private data before outsourcing is an effective measure to protect data confidentiality. However, encrypted data make Effective data retrieval a very challenging task. First introduced the concept of searchable encryption and proposed a practical technique that allows users to search over encrypted data through encrypted query keywords. Later, many searchable encryption schemes were proposed based on symmetric key and public-key setting to strengthen security and improve query efficiency with the growing popularity of cloud computing, how to securely and efficiently search over encrypted cloud data becomes a research focus. Some approaches have been proposed based on traditional searchable encryption schemes.

### Disadvantages

- Cloud server may return erroneous or incomplete query results once he behaves dishonestly for illegal profits.
- A latent space with lower-dimensionality while preserving important discriminative features amongst users.
- To learn an effective latent representation, we simultaneously incorporate prior knowledge, such as temporality of wellness features and heterogeneity of users.
- We first present the notations and then formally define the problem of representation learning of longitudinal data.

## III. RELATED WORKS

In the year of 2011, the author "Qian Wang [1]", proposed a paper titled "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing [1]", in that the author described such as: Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design.

In the year of 2015, the authors "Peng Xu, Hai Jin [2]", proposed a paper titled "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack [2]", in that the author described such as: Public-key encryption with keyword search (PEKS) is a versatile tool. It allows a third party knowing the search trapdoor of a keyword to search encrypted documents containing that keyword without decrypting the documents or knowing the keyword. However, it is shown that the keyword will be compromised by a malicious third party under a keyword guess attack (KGA) if the keyword space is in a polynomial size. A malicious searcher can no longer learn the exact keyword to be searched even if the keyword space is small. We propose a universal transformation which converts any anonymous identity-based encryption (IBE) scheme into a secure PEFKS scheme. Following the generic construction, we instantiate the first PEFKS scheme proven to be secure under KGA in the case that the keyword space is in a polynomial size.

In the year of 2013, the authors "Wenhai Sun, Bing Wang [3]", proposed a paper titled "Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking [3]", in that the author described such as: With the growing popularity of cloud computing, huge amount of documents are outsourced to the cloud for reduced management cost and ease of access. Although encryption helps protecting user data confidentiality, it leaves the well-functioning yet practically-efficient secure search functions over encrypted data a challenging

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

problem. we present a verifiable privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, we propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy.

In the year of 2015, the author "Jyotiska Nath Khasnabish, Mohammad Firoj Mithani [4]", proposed a paper titled "Tier-Centric Resource Allocation in Multi-Tier Cloud Systems [4]", in that the author described such as: in IT service delivery and support, the cloud paradigm has introduced the problem of IT resource over-provisioning through rapid automation of manual IT operations. Due to the elastic nature of cloud computing, this shortcoming ends up significantly reducing the real benefit, viz., the cost-effectiveness of cloud adoption for Cloud Service Consumers (CSC). Similarly, detecting and eliminating such over provisioning without affecting the quality of service (QoS) is extremely difficult for Cloud Service Providers (CSPs) since they have no visibility into the actual performance of business service but only into the IT services. we have derived improved analytics to address the issues and to accelerate real cloud adoption for large enterprises within the context of meeting (or exceeding) business service level objectives (SLOs) and minimizing the cloud subscription cost (OpEx) for the business.

In the year of 2015, the author "Beniamino Di Martino, Antonio Esposito and Giuseppina Cretella [5]", proposed a paper titled "Semantic Representation of Cloud Patterns and Services with Automated Reasoning to support Cloud Application Portability [5]", in that the author described such as: During the past years the Cloud Computing offer has exponentially grown, with new Cloud providers, platforms and services being introduced in the IT market. The extreme variety of services, often providing non uniform and incompatible interfaces, makes it hard for customers to decide how to develop, or even worse to migrate, their own application into the Cloud. This situation can only get worse when customers want to exploit services from different providers, because of the portability and interoperability issues that often arise. In this paper we propose a uniform, integrated, machine-readable, semantic representation of cloud services, patterns, appliances and their compositions. Our approach aims at supporting the development of new applications for the Cloud environment, using semantic models and automatic reasoning to enhance portability and interoperability when multiple platforms are involved. In particular, the proposed reasoning procedure allows to: perform automatic discovery of Cloud services and Appliances; map between agnostic and vendor dependent Cloud Patterns and Services; automatically enrich the semantic knowledge base.

## A. Proposed System Summary

A secure and fine-grained query results verification scheme by constructing the verification object for encrypted outsourced data files. When a query ends, the query results set along with the corresponding verification object are returned together, by which the query user can accurately verify: 1) the correctness of each encrypted data file in the results set; 2) how many qualified data files are not returned and 3) which qualified data files are not returned. Furthermore, our proposed verification scheme is lightweight and loose-coupling to concrete secure query schemes and can be very easily equipped into any secure query scheme for cloud computing. Just as possibly tampering or deleting query results, the dishonest cloud server may also tamper or forget verification objects themselves to make the data user impossible to perform verification operation. Specially, once the cloud server knows that the query results verification scheme is provided in the secure search system, this information may leak query user's privacy and expose some useful contents about data files. More importantly, this exposed information may become temptations of misbehavior for the cloud server.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

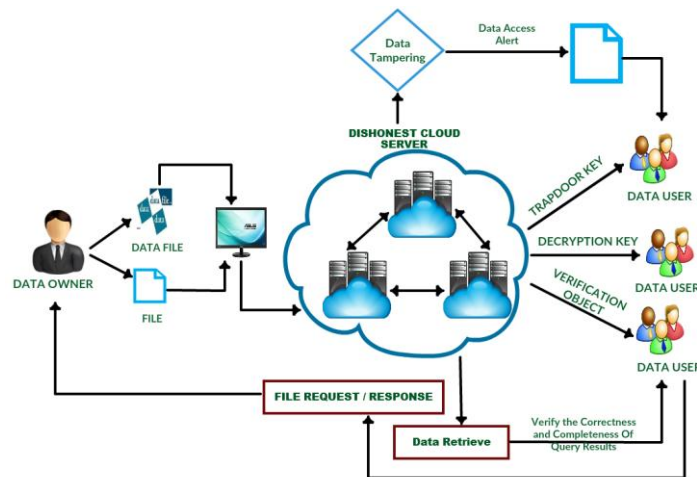


Fig.2 Proposed System Architecture

## Advantages

- We formally propose the verifiable secure search system model and threat model and design a fine-grained query results verification scheme for secure keyword search over encrypted cloud data.
- We propose a short signature technique based on certificate less public-key cryptography to guarantee the authenticity of the verification objects themselves.
- We design a novel verification object request technique based on Parlier Encryption, where the
- Cloud server knows nothing about what the data user is requesting for and which verification objects are returned to the user.
- We provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our proposed scheme.

## IV. SYSTEM IMPLEMENTATION

### A. Query Results Verification

The query result verification mechanism allows the data user to verify the results. In this project, we designed a safe, easy to integrate Fine-grained query results validation mechanism, by giving a given query result set, the query user can not only verify The correctness of each data file in the collection can also be further checked if the collection does not return how many or which qualified data files.

### B. Outsourcing Encrypted File

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. The data owner will outsource the encrypted file to the cloud server; automatically three different keys will be generated for the file.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

## C. Verification Object Construction

To maximize reduce storage and communication cost and achieve privacy guarantee of the verification objects. Trapdoor key, verification object key and decryption key are automatically constructed. The trapdoor key is basically differentiated the data owner and hacker.

## D. Verification Object Signature and Authentication

When a query ends, the query results set and corresponding verification object are together returned to the query user, who verifies the correctness and completeness of query results based on the verification object. Our proposed query results verification scheme not only allows the query user to easily verify the correctness of each encrypted data file in the query results set, but also enables the data user to efficiently perform completeness verification before decrypting query results.

## E. Unauthorized Data Access Alert

When the cloud server or unauthorized person gains the access of the information or data which is stored by the user. The data user will get alert whenever anyone try to access the data or information. We can prevent from accessing the user information or data by verifying the verification object.

## F. File Recovery

Data recovery is a process of salvaging (retrieving) inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a normal way. Even the hacker will access the data or even hacker does the tampering we can still recover the whole document.

## G. AES Algorithm

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

You take the following AES steps of encryption for a 128-bit block:

- (a) Derive the set of round keys from the cipher key.
- (b) Initialize the state array with the block data (plaintext).
- (c) Add the initial round key to the starting state array.
- (d) Perform nine rounds of state manipulation.
- (e) Perform the tenth and final round of state manipulation.
- (f) Copy the final state array out as the encrypted data (ciphertext).

## V. RESULTS AND DISCUSSION

The following figure, Fig.3 illustrates the Home Page view of the proposed system, in which this home page allows the user to navigate into the features in the proposed approach.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

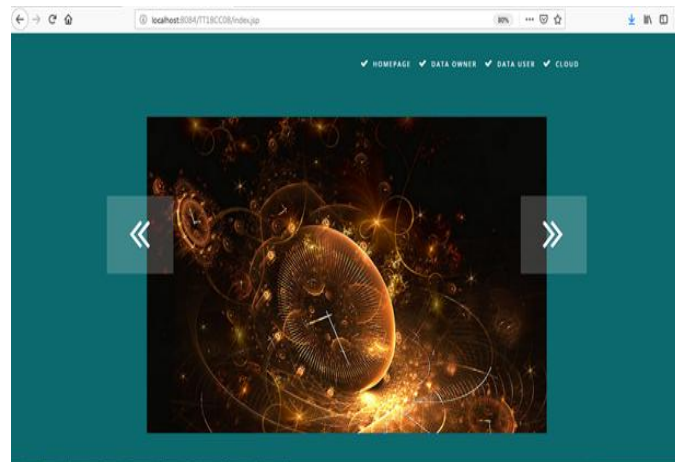


Fig.3 Home Page

The following figure, Fig.4 illustrates the Owner Registration view of the proposed system, in which this registration page allows the owner to register their identity into the system.

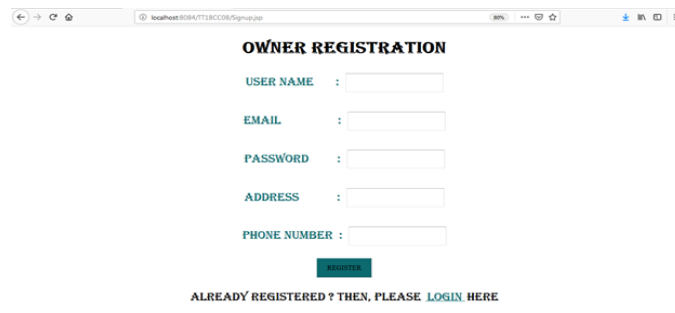


Fig.4 Owner Registration Page

The following figure, Fig.5 illustrates the Owner Authentication Page view of the proposed system, in which it allows the owner to navigate into the main page, if the credentials are valid.

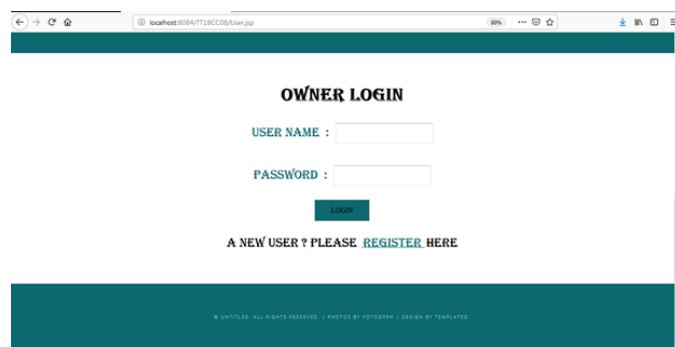


Fig.5 Owner Authentication

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 2, February 2020

The following figure, Fig.6 illustrates the File Upload view of the proposed system.

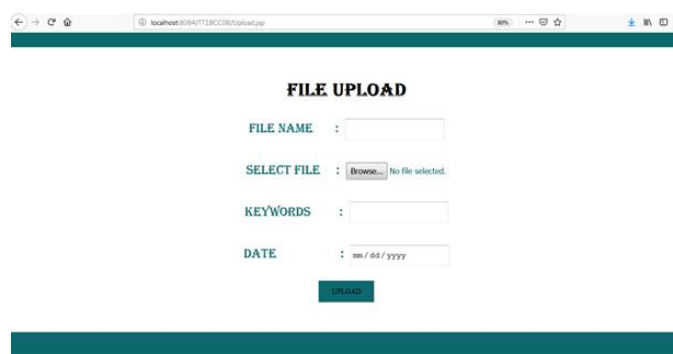
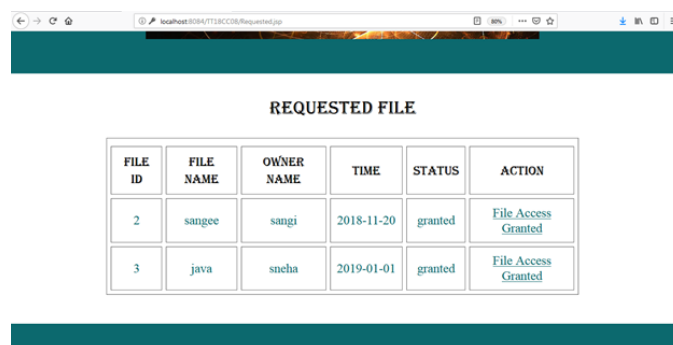


Fig.6 File Upload View

The following figure, Fig.7 illustrates the Requested File Details view of the proposed system. By using this option, users can request for the particular file to the owner and get details accordingly.



FILE ID	FILE NAME	OWNER NAME	TIME	STATUS	ACTION
2	sangee	sangi	2018-11-20	granted	<a href="#">File Access Granted</a>
3	java	sneha	2019-01-01	granted	<a href="#">File Access Granted</a>

Fig.7 File Requisition

## VI. CONCLUSION AND FUTURE SCOPE

We propose a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server. A short signature technique is designed to guarantee the authenticity of verification object itself. Moreover, we design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually returned by the cloud server. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed scheme.

In future of outsource data -Search method is not efficient since the cloud needs to search through the whole database, which is very inefficient. In future we have some work in this line that will be enhancements for efficient verification for large-scale outsourced data. This system works on semi trusted cloud but in future it will be extended up to all types of cloud environment and can provide better security. Furthermore in future we can extend our search scheme to use external storage more carefully while maintaining privacy.



# International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Visit: [www.ijirset.com](http://www.ijirset.com)

**Vol. 9, Issue 2, February 2020**

## REFERENCES

- [1] Qian Wang, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, May, 2011.
- [2] Peng Xu, Hai Jin, Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack, 2015.
- [3] Wenhai Sun, Bing Wang., Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking, 2013.
- [4] Jyotiska Nath Khasnabish, Mohammad Firoj Mithani, Tier-Centric Resource Allocation in Multi-Tier Cloud Systems, 2015.
- [5] Beniamino Di Martino, Antonio Esposito and Giuseppina Cretella, Semantic Representation of Cloud Patterns and Services with Automated Reasoning to support Cloud Application Portability, 2015.
- [6] N. Park and D. J. Lilja, "Characterizing datasets for data deduplication in backup applications," in Proc. IEEE Int. Symp. Workload Characterization (IISWC), 2010, pp. 1–10.
- [7] A. ODriscoll, J. Daugelaite, and R. D. Sleator, "Big data, hadoop and cloud computing in genomics," J. Biomed. Inform., vol. 46, no. 5, pp. 774–781, 2013.
- [8] P. C. Zikopoulos, C. Eaton, D. DeRoos, T. Deutsch, and G. Lapis, Understanding Big Data. New York, NY, USA: McGraw-Hill, 2012.
- [9] M. Dong, H. Li, K. Ota, and H. Zhu, "HVSTO: Efficient privacy preserving hybrid storage in cloud data center," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), 2014, pp. 529–534.
- [10] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 1206–1216, May 2015.
- [11] M. Dutch. (2008, Jun.). SNIA: Understanding Data De-Duplication Ratios [Online]. Available: [http://www.snia.org/sites/default/files/Understanding\\_Data\\_De-duplication\\_Ratios-20080718.pdf](http://www.snia.org/sites/default/files/Understanding_Data_De-duplication_Ratios-20080718.pdf)
- [7] M. Dong, H. Li, K. Ota, L. T. Yang, and H. Zhu, "Multicloud-based evacuation services for emergency management," IEEE Cloud Comput., vol. 1, no. 4, pp. 50–59, Nov. 2014.
- [12] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sink-location privacy enhanced scheme for WSNS through ring based routing," J. Parallel Distrib. Comput., vol. 81, pp. 47–65, 2015.
- [13] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid," IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, pp. 178–191, Jun. 2013.
- [14] J. Jose, T. T. Tomy, V. Karunakaran, A. K. V. A. Varkey, and N. C. A., "Securing passwords from dictionary attack with character-tree," in Proceedings of 2016 International Conference on Wireless Communications, Signal Processing and Networking, Mar. 2016, pp. 2301–2307.
- [15] A. Arora, A. Nandkumar, and R. Telang, "Does information security attack frequency increase with vulnerability disclosure? an empirical analysis," Information Systems Frontiers, vol. 8, no. 5, pp. 350–362, Dec. 2006.
- [16] R. Song, "Advanced smart card based password authentication protocol," Computer Standards & Interfaces, vol. 32, no. 5, pp. 321–325, 2010.
- [17] M. C. Ah Kioon, Z. S. Wang, and S. Deb Das, "Security analysis of MD5 algorithm in password storage," in Proceedings of Instruments, Measurement, Electronics and Information Engineering. Trans Tech Publications, Oct. 2013, pp. 2706–2711.
- [18] P. Oechslin, "Making a faster cryptanalytic time-memory trade-off," in Proceedings of Advances in Cryptology - CRYPTO 2003. Springer Berlin Heidelberg, 2003, pp. 617–630.