# A Comprehensive Review of Secure Dynamic Ownership Techniques for Robust Data Deduplication in Cloud Environments

KM Jyoti Giri[1], Dr. Yusuf Perwej[2]
[1] *M. Tech, Dept. of CSE, Goel Institute of Technology & Management, (AKTU), Lucknow, India*
[2] *Assistant Professors, Dept. of CSE, Goel Institute of Technology & Management, (AKTU), Lucknow, India*

***Abstract*— In the era of cloud computing, ensuring data security and optimizing storage are paramount concerns. This comprehensive review delves into secure dynamic ownership techniques and their role in robust data deduplication within cloud environments. Dynamic ownership, which allows seamless and secure transfer of data ownership between users, is crucial for maintaining data integrity and accountability in collaborative and multi-tenant cloud settings. Concurrently, data deduplication, which eliminates redundant data, enhances storage efficiency and reduces costs. This paper surveys state-of-the-art methods that integrate these two critical aspects, exploring various cryptographic protocols, blockchain-based frameworks, and innovative algorithms designed to secure data during ownership transfer and deduplication processes. We analyze the strengths and limitations of existing solutions, highlight ongoing challenges, and identify future research directions. Our findings underscore the need for advanced, scalable techniques that balance security, efficiency, and performance, thereby advancing the reliability and adoption of cloud storage systems.***

***Index Terms*- Cloud Computing, Dynamic Ownership, Blockchain-Based Frameworks, Cloud Storage**

## I. INTRODUCTION

The proliferation of cloud computing has revolutionized the way data is stored, managed, and accessed, providing unprecedented flexibility, scalability, and cost-efficiency [1]. Organizations and individuals alike are leveraging cloud services to store vast amounts of data, taking advantage of the cloud's ability to handle dynamic workloads and provide ubiquitous access [2]. However, as reliance on cloud storage intensifies, ensuring data security and optimizing storage efficiency have emerged as critical challenges that must be addressed to maintain the integrity and viability of cloud services [3].

Two key concepts that are central to these challenges are secure dynamic ownership and robust data deduplication [4]. Both play a pivotal role in ensuring that cloud environments can meet the high standards of data integrity, confidentiality, and efficiency required by modern applications and users [5].

### 1.1 Secure Dynamic Ownership

Dynamic ownership refers to the capability to transfer data ownership between different users or entities securely and efficiently [6]. This is especially important in collaborative environments where data ownership can change frequently, and in multi-tenant cloud architectures where different users might require access to the same data at different times. Secure dynamic ownership ensures that such transfers are executed without compromising the security and integrity of the data [7].

To achieve secure dynamic ownership, several critical components must be in place:

Authentication and Authorization: Ensuring that only authorized users can initiate ownership transfers.
Cryptographic Techniques: Protecting data during and after the transfer process to prevent unauthorized access and tampering.
Audit Trails: Maintaining detailed records of ownership changes to provide accountability and traceability.

1.2 Robust Data Deduplication

Data deduplication is a technique used to eliminate redundant copies of data, thereby reducing storage requirements and improving storage efficiency [8]. By storing only unique instances of data and referencing duplicates to these instances, cloud storage systems can significantly cut down on the amount of storage space needed, leading to cost savings and enhanced performance.

However, implementing deduplication in a secure manner poses several challenges:

Data Privacy: Ensuring that deduplication does not expose sensitive information.
Integrity: Maintaining the integrity of data while performing deduplication operations.
Efficiency: Achieving high deduplication ratios without introducing significant performance overhead.

1.3 Intersection of Dynamic Ownership and Data Deduplication

The intersection of secure dynamic ownership and robust data deduplication is particularly significant in cloud environments [9]. Effective integration of these mechanisms ensures that data can be securely transferred between users while simultaneously optimizing storage efficiency. This integration is crucial for several reasons:

Scalability: As data volumes grow, the ability to manage storage efficiently and securely becomes more critical.
Security: Protecting data during ownership transfers and deduplication processes is essential to maintaining user trust and compliance with regulatory requirements.
Performance: Balancing the need for security and efficiency without compromising system performance is a key challenge.

1.4 Objectives of the Review

This comprehensive review aims to explore the current state-of-the-art techniques and methodologies in securing dynamic ownership and implementing robust data deduplication in cloud environments. Specifically, the objectives are:

To provide a detailed overview of the techniques used to secure dynamic ownership and data deduplication.
To analyze the strengths and weaknesses of existing solutions, identifying the trade-offs involved.
To highlight ongoing challenges and gaps in current research.
To propose future research directions that could address these challenges and advance the field.

1.5 Structure of the Review

The review is structured as follows:

Background and Related Work: A discussion on the fundamental concepts and previous work related to dynamic ownership and data deduplication.

Techniques for Secure Dynamic Ownership: An in-depth analysis of various methods and protocols designed to secure ownership transfers in cloud environments.

Methods for Robust Data Deduplication: A comprehensive examination of deduplication techniques and their security implications.

Integration Strategies: Exploration of how dynamic ownership and deduplication can be integrated effectively, including case studies and practical implementations.

Challenges and Future Directions: Identification of current challenges and potential avenues for future research.

By providing a thorough examination of these topics, this review aims to contribute to the development of more secure, efficient, and reliable cloud storage systems, ultimately fostering greater adoption and trust in cloud technologies.

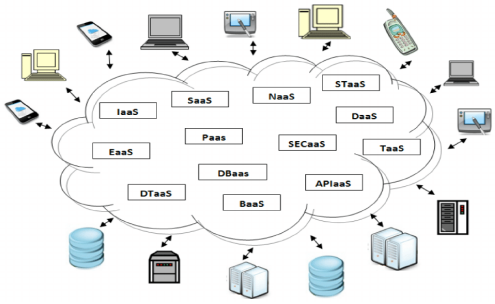


Figure 1. Cloud Computing Diagram

## II. LITERATURE SURVEY

Subhashini et.al[2011][2] have depicted all security related issues present in the distributed computing. The different organizations of the cloud and every one of the issues present in every sending are been characterized in the paper. They have characterized in regard to the administration conveyance where in each kind of SaaS, PaaS, and IaaS. They specifically characterized all the security issues in the product as an administration of distributed computing. In Issues of SaaS, there are classifications dependent on information, arrange, web applications and virtualization vulnerabilities.

Balachandra reddy et.al[2010][4] have talked about administration level understandings that are been issued by client to supplier before getting into cloud. This is the main trust a supplier will see from client, yet it insufficient to give security as it doesn't answers the issues to the misfortunes of the client, there ought to be sure changes as per the sort of administration a client is working and should be institutionalized with favored client get to, information isolation, area of information and so on.

Kresimer Popovic et.al[2010] [7] have talked about various security concerns present in the cloud display which is losing privacy and uprightness of the information while exchange, stockpiling and recovery. They additionally examined on the things that will be think about where the dangers are available in distributed computing like from client to kind of administrations. With the above issues they reasoned that we have to take security and protection in giving cloud administrations.

Patrick Mc. Daniel et.al[2010 [10] portrayed about difficulties of security and upgrades that are to be made over cloud for secure information over cloud. They focused chiefly on security issues over cloud occurrences. The occurrences over cloud will keep running on some base framework which may trade off and causes a security issue. There are additionally outside foes over cloud which may need security of occasions from outsiders. They talked about specific open doors which are to the extraordinary difficulties for analysts. The distributed computing security concerns were examined in detail in [13] the primary issues talked about were protection worries because of outsider clients. As the security because of programmer's increment over web and the distributed computing is absolutely on web, there are diverse issues like assaults are examined on it.

Sameera Abdulrahman Almulla et.al[2010][11]have examined about administration in distributed computing ,the difficulties with respect to the data security worries in regards to classification, integrity and accessibility. They talk about security difficulties of distributed computing in regards to character and access the executives.

Steve Mansfield et.al[2008][12] has talked about with respect to the upsides of having the cloud in the meantime the issues present in cloud. When we use in our edge territory we utilize numerous security sides like firewalls DMZ'z and so on., where as in cloud all are on a remote framework with no security. Creator predominantly indicates out that we require have a lot of trust in the plan of framework with great validation and approval capacities.

## III. OVERVIEW OF CLOUD COMPUTING

In Cloud Computing, we talk about a disseminated design that brings together server assets on a versatile stage, so that accommodate cloud administrations and on-request figuring assets. Cloud specialist co-ops (CSP‟s) propose cloud stages for their customer's fulfillment by using and making their web administrations. Web access suppliers (ISP‟s) offer customers to enhance the fast broadband to get to the web. CSPs and ISPs (Internet Service Providers) together offer administrations. Distributed computing is an imperative model that permits increasingly advantageous to access, on-request organize access to a mutual pool of configurable figuring assets like systems, servers, stockpiling, applications that can be immediately provisioned and discharged with administration provider's communication or negligible administration exertion. By and large, cloud providers offer three sorts of administrations, i.e. programming as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are a few explanations behind associations to move towards IT arrangements that incorporate distributed computing as they are basically required to

pay for the assets on utilization premise. Mists are the development of the dispersed frameworks in the creative pattern, the ancestor of cloud being the matrix. The client does not ready to require skill or colleague to control the framework of mists; it gives just deliberation idea. It tends to be produced as an administration of an Internet with increment adaptability, higher throughput, enhances nature of administration and registering power. Distributed computing suppliers convey visit online business applications, which are gotten to through an internet browser from servers [1].

a. Characteristics of Cloud Computing

- Ultra large-scale: In ultra vast scale processing, the size of cloud is extensive union. The billow of Google has possessed more than one million servers get to. For instance, IBM, Microsoft, Yahoo, Rediff, Amazon they have more than several thousand servers. There are many servers in a venture control get to.
- Virtualization: Distributed computing makes client to get to benefit all over, through a terminal. All that you can finish the procedure through a web access by utilizing a note pad PC or an advanced cell or a Tablet or a Laptop. Clients can accomplish or share it safely through a straightforward way, whenever, anyplace. Clients can finish an assignment that can't be finished in a solitary PC.
- High reliability: Cloud applies information multi transcript blame tolerant, the calculation hub isomorphism interchangeable thus as to enhance and guarantee the high unwavering quality of the cloud benefit. By utilizing distributed computing is profoundly dependable than neighborhood PC process connection.
- Versatility: Distributed computing can create a few sorts of uses upheld by cloud administration, and single cloud can keep up various applications running in the meantime.
- High extendibility: The size of cloud can exceptionally stretch out or progressively want to meet the expanding necessity of cloud administrations.
- On demand service: Cloud is a huge asset pool, which will you can pay as per your prerequisite; cloud is much the same as that running water, electric, and gas that can be charged by the sum that you utilized.
- Extremely inexpensive: The focused on the board of cloud makes the endeavor needn't embrace the administration cost of the server farm that expansion speed of the administration. The flexibility can enhance the usage rate of the available assets contrasted and conventional frameworks, accordingly clients can thoroughly appreciate the cloud administration and minimal effort as favorable position or to a great degree modest.

## IV. DEPLOYMENT MODELS OF CLOUD

The cloud can be deployed in three models. They are described in different ways. In generalized it is described as below:

A. Public Cloud: Open cloud depicts distributed computing in the customary standard sense, whereby assets are progressively provisioned on a fine-grained, self-benefit premise over the Internet, through web applications/web administrations, from an off-website outsider supplier who charges on a fine-grained utility registering premise. This is a general cloud accessible to open over Internet.

B. Private Cloud: A private cloud is one in which the administrations and foundation are kept up on a private system. These mists offer the best dimension of security and control, however they require the organization to at present buy and keep up all the product and framework, which lessens the cost funds.

C. Hybrid Cloud: A half and half cloud condition comprising of different inward as well as outer suppliers "will be normal for generally ventures". By incorporating numerous cloud administrations clients might have the capacity to facilitate the change to open cloud administrations while staying away from issues, for example, PCI consistence.

## V. SERVICES PROVIDED BY CLOUD

The different types of services provided by cloud are IaaS, PaaS and SaaS, shows in figure 2.

A. Infrastructure as a Service (IaaS): IP's deal with a bigger arrangement of figuring assets, for example,

putting away and preparing limit. Through virtualization, they can part, allot and progressively resize the assets to manufacture impromptu frameworks as requested by the clients, the Service suppliers. They send the product stacks that run their administrations. This is framework as an administration.

B. Platform as a Service (PaaS): Cloud frameworks can offer an extra reflection levels as opposed to providing a virtualized foundation. They can give the product stage where frameworks keep running on. The measuring of equipment assets is made in a straightforward way.

C. Software as a Service (SaaS): There are administrations of potential enthusiasm to a wide assortment of clients facilitated in a cloud framework. This is a substitute to locally running application. A case of this is online option of run of the mill office applications, for example, word processor.

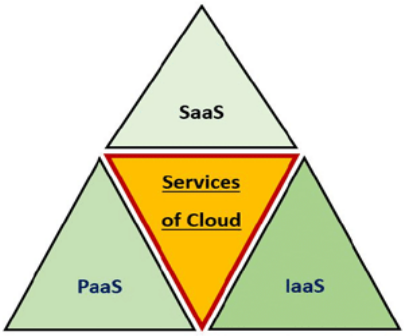


Figure 2. Services Provided by Cloud

## VI. SECURITY ALGORITHMS

In Cloud Storage, any person's or association's information is depicting about open and keep up from various associated and conveyed assets that give to a cloud. Encryption calculation [25] assumes a critical job to give secure correspondence over associated and appropriated assets by utilizing the key device for ensuring the information. Encryption calculation has fundamentally changed over the information into mixed kind to ensure by utilizing "the key" and transmitter client just have the way to unscramble the information. There are two kinds of key encryption systems utilized in security calculations; they are symmetric key encryption and awry key encryption. In symmetric key encryption, single key is utilized to scramble and decode the information. Two keys are principally utilized in uneven key encryption. They are private key and open key. In Public key process, it is utilized for encryption. Another private key is utilized for unscrambling [26]. There are various existing procedures used to acknowledge security in distributed storage. The principle center is about cryptography to make information secure while transmitted over the system. Cryptography idea is that the reconsider and practice of procedures for anchoring correspondence and information inside the nearness of foes. In cryptography idea, encryption and unscrambling strategies are utilized. An encryption procedure changes over message or plaintext into figure content and decoding strategy separates the first message or plaintext into similar figure content. At first, the data must be encoded and transmitted by utilizing the encryption calculation in cryptography. Besides, the data ought to be unscrambled by utilizing the decoding strategy the collector side can peruse the first data. To give security to cloud a few calculations are planned and depict beneath, show in table 1.

- RSA Algorithm: RSA calculation has utilized open key encryption strategy. This calculation is conveyed to life by Ron Rivest, Adi Shamir and Len Adelman in 1977. It is latest uneven key cryptography calculation. It might conceivably very much used to give mystery assurance. In this calculation uses the best number to concoct open key and private key contingent upon numerical precision and duplicating extensive numbers together. It uses the square size of information amid transmission; that its plain-content and figure content numbers among 0 and n for a lot of n esteems. Size of information n (i.e.values) is known as 1024 bits. The genuine test inside the instance of RSA calculation would be the age and choice of people in general key and private key. At interims these two diverse keys can be performed encryption and unscrambling systems. As the sender knows about in regards to the encryption key and recipient perceives about the unscrambling key, these systems we can create encryption and decoding get into RSA.

- Blowfish Algorithm: Blowfish calculation is a symmetric key calculation that was created in 1993 by Bruce Schneier. Its working is about relatively

like DES, anyway in DES enter is little in size and can be decoded in basic way, anyway in Blowfish calculation the measure of the key is monstrous [27] and it can contrast from 32 to 448 bits. Blowfish additionally comprises of 16 rounds like DES [28]. Blowfish calculation can encode information having various size of eight and if the span of the message isn't different of eight than bits are secured. In Blowfish calculation additionally 64 bits of plain content are isolated into two sections of message as size 32 bits length. One section procures as the left piece of message and another is correct piece of the message. The left piece of the message is XOR with the components of the P - exhibit which makes some esteem, after that esteem is transmitted through change work F. The esteem started from the change work is again handled XOR with the other portion of the message i.e. with right bits, after that F| work is called which supplant the left 50% of the message and P| supplant the correct side of the message.

- Data Encryption Standard (DES) Algorithm: The Data cryptography standard (DES) [29] is a symmetric-key square figure found as FIPS-46 inside the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). In encryption site, DES takes a 64-bit plaintext and makes a 64-bit figure content, after that the unscrambling site, it takes a 64-bit figure message and makes a 64-bit plaintext. Every encryption and unscrambling methods are utilized for same 56 bit figure key. The encryption procedure is made of two changes (P-boxes), that we tend to call introductory and last stage, and sixteen Feistel rounds [30]. Each round transmits an alternate 48-bit round key produced from the figure key encryption.

- EI Gamel: The ElGamal encryption framework is an uneven key encryption calculation for performing open key cryptography, which depends on the Diffie– Hellman key trade process by utilizing cryptography. It was represented by Taher Elgamal in 1984. ElGamal encryption is ensured in the free GNU Privacy Guard programming, most recent forms of PGP, and different cryptosystems. The Digital Signature Algorithm is nitty gritty about a variation of the ElGamal signature conspire, which ought not be mistaken for ElGamal encryption. ElGamal encryption can be portrayed over any cyclic gathering G. Its security dependent on the trouble of a specific issue in G identified with processing discrete logarithms.

- Advance Encryption Algorithm (AES): (Advanced Encryption Standard), is the new encryption standard recommended by NIST to supplant DES. The Brute power assault, in this aggressor endeavors to test all the character mixes to open the encryption, it is the main viable assault known against assurance. Together AES and DES are square figures. It has an uneven key length of 128, 192, or 256 bits; default 256 bits. It scrambles information squares of 128 bits in 10, 12 and 14 round relies on the key length. AES Encryption is fast and adaptable; it very well may be executed on various stages especially in little gadgets. What's more, AES has been painstakingly tried for various security applications. [31][32].

- DSA: DSA is the full type of Digital Signature Algorithm. DSA is a Federal Information Processing Standard for handling advanced marks. It was anticipated by the National Institute of Standards and Technology (NIST) in August 1991 to be utilized in their Digital Signature Standard (DSS) and endorsed as FIPS 186 in 1993.Four audits to the underlying detail has been discharged: FIPS 186-1 in 1996,FIPS 186-2 in2000,FIPS 186-3 in 2009and FIPS 186-4 of every 2013. In DSA, key age has depicted around two stages. In essential stage is to settle on calculation parameters that can be shared between various clients of the framework. Second stage is to register open and private keys for giving to a solitary client. The irregular mark esteems k are increasingly vital for performing entropy, mystery, and uniqueness. These three necessities can unveil the entire private key to an assaulter.

Table 1. Security Algorithms

| Algorithm | DES | AES | BLOWFISH | RSA | DSA |
|---|---|---|---|---|---|
| Developed | IBM in1975 | Joan Daeman Vincet Rijman in1978 | Bruce Schneir in1998 | Ron Rivest, Adi sharmir ,L Adleman in 1977 | NIST in 1991 |
| Key Size | 56 | 128<br>192<br>256 | 32 -448 | 1024-4096 | - |
| Security | adequate | Secure | Secure | secure | secure |
| Memory Usage | High | Medium | Very Low | - | - |
| Confidentiality | Low | High | Very High | High | - |
| Power consumption | Low | Low | Very High | High | - |
| Encryption | Medium | High | Very High | High | - |

- 3DES: This was produced as an enhancement of DES in 1998. In this run of the mill the encryption strategy is identified with unique DES however connected multiple times to enhance the encryption level. Be that as it may, 3DES is slower than other square figure systems. This is an improvement of DES and 64 bit square length with 192 bits key size. 3DES has lessened execution as far as throughput level and power utilization when contrasted and DES. It in every case needs additional time than DES because of its triple stage encryption attributes [33] [24].
- MD5- (Message-Digest calculation 5): Generally, the cryptographic hash work calculation is utilized with a 128-piece hash esteem and procedures a variable length message into a settled size yield of 128 bits. At first, the information message is separated into lumps of 512-piece squares a short time later the message is secured so its aggregate length is distinct by 512. In this procedure, the transmitter of the information uses the general population key to encode the message and the collector utilizes its private key to decode the message.

## CONCLUSION

The rapid advancement and widespread adoption of cloud computing have underscored the critical need for effective data security and storage optimization mechanisms. This comprehensive review has explored the vital areas of secure dynamic ownership and robust data deduplication within cloud environments, providing a detailed examination of the current state-of-the-art techniques, methodologies, and their integration.

Dynamic ownership ensures that data can be securely and efficiently transferred between different users or entities, maintaining the integrity and accountability of data in multi-tenant and collaborative cloud settings. Various approaches, including advanced cryptographic protocols, blockchain-based frameworks, and secure authentication mechanisms, have been analyzed for their effectiveness in protecting data during ownership transfers.

Data deduplication, aimed at eliminating redundant data, plays a crucial role in optimizing storage utilization and reducing operational costs. Techniques such as convergent encryption and secure hashing have been discussed for their ability to ensure data privacy and integrity while achieving high deduplication ratios. The integration of these methods with dynamic ownership mechanisms is essential to prevent security breaches and maintain efficient storage systems.

Despite significant progress in both fields, challenges remain that necessitate further research and innovation. These include the need for seamless integration of dynamic ownership and deduplication processes, minimizing performance overhead, and developing scalable solutions that can handle the increasing volume and complexity of cloud data. Additionally, addressing issues related to data privacy, compliance with regulatory standards, and user trust are crucial for the continued advancement of cloud technologies.

Future research should focus on creating holistic frameworks that combine secure dynamic ownership and robust deduplication, leveraging emerging technologies such as artificial intelligence, machine learning, and blockchain. These integrated solutions will be pivotal in addressing the evolving security threats and ensuring the trustworthiness of cloud storage systems.

In conclusion, secure dynamic ownership and robust data deduplication are foundational to the security and efficiency of cloud storage systems. By advancing these technologies, we can pave the way for more secure, reliable, and efficient cloud environments, ultimately fostering greater adoption and trust in cloud services across various sectors. This review highlights the importance of continued research and development in these areas to meet the growing demands and challenges of cloud computing.

REFERENCES


[1] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.

[2] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.

[3] Sudha.M, Bandaru Rama Krishna rao, M.Monica, "A Comprehensive approach to ensure secure data communication in cloud environment" International Jornal Of computer Applications, vol. 12. Issue 8, pp. 19-23.

[4] Balachander R.K, Ramakrishna P, A. Rakshit, "Cloud Security Issues, IEEE International Conference on Services Computing (2010)," pp. 517-520.

[5] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing" proceeding of International workshop on Quality of service 2009", pp.1-9.

[6] Gary Anthes, "Security in the cloud," In ACM Communications (2010), vol.53, Issue11, pp. 16-18.

[7] Kresimir Popovic, Željko Hocenski, "Cloud computing security issues and challenges," MIPRO 2010, pp. 344-349.

[8] Kikuko Kamiasaka, Saneyasu Yamaguchi, Masato Oguchi, "Implementation and Evaluation of secure and optimized IP-SAN Mechanism," Proceedings of the IEEE International Conference on Telecommunications, May 2007, pp. 272-277.

[9] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, "A Break in Clouds: Towards a cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009, pp. 50-55.

[10] Patrick McDaniel, Sean W. Smith, "Outlook: Cloudy with a chance of security challenges and improvements," IEEE Computer and reliability societies (2010), pp. 77-80.

[11] Sameera Abdulrahman Almulla, Chan Yeob Yeun, "Cloud Computing Security Management," Engineering systems management and its applications (2010), pp. 1-7.

[12] Steve Mansfield-Devine, "Danger in Clouds", Network Security (2008), 12, pp. 9-11.

[13] Anthony T. Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, Tata Mc GrawHill 2010.

[14] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[15] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[16] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN "10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[17] H. KAMAL IDRISSI, A. KARTIT, M. EL MARRAKI FOREMOST SECURITY APPREHENSIONS IN CLOUD COMPUTINGJournal of Theoretical and Applied Information Technology 31 st January 2014. Vol. 59 No.3

[18] Kuyoro S. O, Ibikunle F. & Awodele O Cloud Computing Security Issues and ChallengesInternational Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[19] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gongng The Characteristics of Cloud Computing2010 39th International Conference on Parallel Processing Workshopse Brazilian Computer Society 2010

[20] SO, Kuyoro. Cloud computing security issues andchallenges. International Journal of Computer Networks, 2011, vol. 3, no 5.

[21] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal

of Computer Applications, no. 5, pp. 11-14, 2012.

[22] J. Krumm, "A survey of computational location privacy," Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.

[23] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695- 3929 -4.

[24] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[25] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[26] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[27] Pratap Chandra Mandal, „Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X Vol. 2, Issue 7.

[28] G. Devi and M. Pramod Kumar, „Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm", International Journal of Computer Trends and Technology. (2012) Vol. 3 Issue 4, ISSN: 2231-2803, pp.592-596.

[29] Neha Jain and Gurpreet Kaur „Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[30] G. Devi , M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.

[31] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[32] Gurpreet Singh, Supriya Kinger "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[33] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[34] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.