IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Adaptive AES-Driven Encryption for Moving Target Defense in Cloud Environments: A Novel Framework

Amit Sinha[1], Dr. Shashank Singh[2]

[1] M.Tech Scholar, Dept. of Computer Science & Engineering, S R Institute of Management and Technology, (AKTU), Lucknow, Uttar Pradesh, India

[2] Professor, Dept. of Computer Science & Engineering, S R Institute of Management and Technology, (AKTU), Lucknow, Uttar Pradesh, India

Abstract— With the rapid growth of cloud computing, ensuring data security and resilience against sophisticated cyber threats has become increasingly critical. Traditional static encryption approaches are often inadequate against adaptive adversaries capable of exploiting predictable patterns. This paper proposes a novel Adaptive AES-Driven Encryption Framework integrated with Moving Target Defense (MTD) mechanisms to dynamically protect data in cloud environments. The framework enhances the Advanced Encryption Standard (AES) by introducing dynamic key generation, periodic cryptographic context switching, and intelligent attack surface shifting based on real-time threat assessment. By continuously altering the encryption parameters and resource configurations, the proposed model significantly reduces the attack surface and limits adversary reconnaissance. Experimental evaluations demonstrate substantial improvements in data confidentiality, key unpredictability, and defense robustness without compromising system performance. This work marks a significant step toward autonomous, adaptive, and proactive cloud security solutions.

Keywords— Adaptive Encryption, AES, Moving Target Defense (MTD), Cloud Security, Dynamic Key Management, Cybersecurity, Attack Surface Reduction, Cryptographic Context Switching, Threat Resilience, Secure Cloud Computing.

I. INTRODUCTION

Cloud computing has revolutionized the delivery and scalability of computing resources, enabling organizations to store, process, and access data remotely. However, this paradigm shift has also introduced significant security and privacy concerns due to the increased attack surface and multi-tenancy of cloud infrastructures [1]. Static security mechanisms, particularly in cryptographic implementations, are often insufficient against evolving cyber threats such as advanced persistent threats (APTs), zero-day attacks, and side-channel exploits [2].

Among the commonly employed cryptographic algorithms, the Advanced Encryption Standard (AES) is renowned for its robustness and widespread adoption in securing data-at-rest and data-in-transit [3]. Despite its resilience, static AES implementations are vulnerable to side-channel attacks and key prediction over time, especially in dynamic cloud environments [4]. These vulnerabilities are exacerbated by the deterministic nature of AES encryption parameters, which adversaries can eventually learn and exploit through extended reconnaissance [5].

To address these limitations, Moving Target Defense (MTD) has emerged as a promising strategy in proactive cybersecurity. MTD operates by dynamically shifting the system's attack surface, thereby increasing the complexity and cost for adversaries attempting to exploit vulnerabilities [6]. Integrating

MTD with cryptographic systems can significantly enhance their security posture by introducing unpredictability in encryption mechanisms [7].

This paper proposes a novel Adaptive AES-Driven Encryption Framework for cloud environments that incorporates MTD principles. The framework adapts AES encryption parameters—such as key, round configuration, and S-box substitution—based on real-time threat intelligence and system behavior. It introduces dynamic key regeneration using entropy sources and periodic cryptographic switching to thwart pattern recognition and reduce exposure time for any specific configuration.

Unlike conventional static defenses, the proposed framework continuously evolves to reduce adversarial success probability, creating a moving target that is both intelligent and unpredictable. Our approach not only enhances the cryptographic strength of AES but also aligns with cloud-native operational dynamics, ensuring scalability and minimal performance degradation.

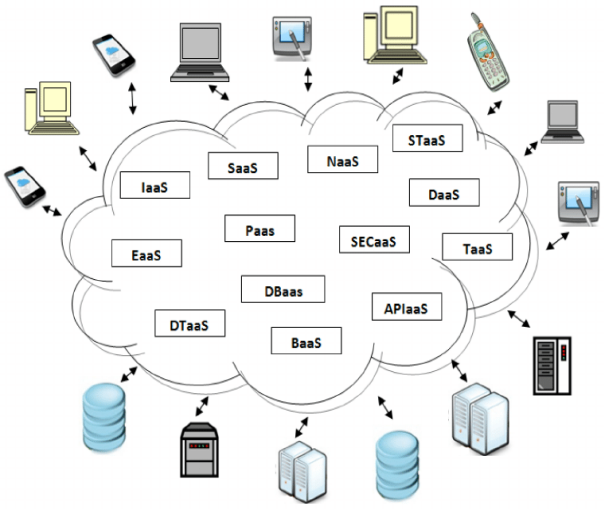

Figure 1. Cloud Computing Diagram

.

Cloud computing is a general term for anything that involves hosted services over the Internet. These services are broadly divided into three categories: [6]

Infrastructure as a Service (IaaS): In IaaS model computer resources such as storage, computing capabilities are made available to the customer on demand. It's cost saving model. In this model customer only pay to use IT infrastructure as needed.[14]
E.g: Amazon Web Services, Virtual machines, servers, storage, load balancers, network.

Platform as a Service (PaaS): In the PaaS model a development environment is offered to the customer which is managed by the provider. On which customer can develop and run their applications without building and managing complex infrastructure.[14]
E.g: Google Application Engine, Execution runtime, database, Web server, Development tools.

Software as a Service (SaaS): In the SaaS model an application is offered to the customer by the cloud service provider. In which application is hosted by the provider at their infrastructure and distributed over the network as a service on demand.[14]
E.g: Online word processing and spreadsheet tools, Microsoft office, Email, communication, Games.
Cloud computing is typically classified in four types.

Public cloud: Public cloud is publicly accessible cloud which is managed by third parties. All customers share a common infrastructure pool with limited configuration. The cloud provider is responsible for creation and ongoing maintenance of the public cloud.[6][14]

Private Cloud: Private cloud is accessible only by an organization and also managed by the organization. Private cloud enables an organization to use cloud computing by means centralizing access to IT resources from different geographical location. .[6][14]

Hybrid cloud: Hybrid cloud combines both public and private cloud models. With Hybrid cloud organization can utilize third party cloud provider service in a full or partial manner. Thus, Hybrid cloud increases flexibility of computing.[6][14]

Community Cloud: Community cloud is a multi-tenant infrastructure which is shared among several organizations. And it is managed, governed and secured by all the participating organization. These organizations have similar cloud requirements and their ultimate goal is to achieve business objective. It is beneficial in order to cost saving.
Cloud based environment there are many security issues such as authentication, integrity, privacy, virtualization, confidentiality, large amount data processing, scalability, access control etc.[8] Traditional security approaches are no longer suitable for data and application in cloud. [1][2][3][4].

The following section highlights, Section one introduction of cloud security and privacy. Section two a review of literature on security issues in cloud computing and the remaining sections are organized as follows. Section three discusses overview of cloud computing in cloud computing laying emphasis on SaaS, PaaS and IaaS; and cloud computing deployment methods. Section four deployment models of cloud. Section five discusses modules description. Section six discusses security algorithms. Section seven presents the result discussion. Section eight present the conclusion.

II. LITERATURE SURVEY

Cloud computing offers scalable and on-demand computing resources but remains a prime target for security breaches due to its shared and distributed architecture. Traditional static defense mechanisms often fall short in countering dynamic and sophisticated cyber threats, necessitating more adaptive and proactive approaches [1].

A. AES Encryption and Its Limitations

The Advanced Encryption Standard (AES) has been widely adopted for securing data in cloud environments due to its efficiency and robustness against brute-force attacks [2]. However, numerous studies have revealed that static AES implementations are vulnerable to side-channel attacks, key leakage, and pattern analysis, especially in shared cloud infrastructures [3][4]. Zhang et al. demonstrated that Cross-VM side-channel attacks can be used to extract AES private keys from co-located virtual machines, raising serious concerns about the resilience of static encryption models in cloud settings [5].

B. Challenges in Key Management

Efficient key management is critical in maintaining the confidentiality and integrity of encrypted cloud data. Traditional schemes often rely on pre-defined, static key lifecycles, making them susceptible to advanced threats over time. Ali et al. [6] and Ruj et al. [7] discussed scalable and hierarchical key management approaches but did not integrate adaptive renewal mechanisms or dynamic behavior. Entropy-based key generation, as explored by Sharma et al. [8], adds unpredictability but lacks integration with MTD (Moving Target Defense) strategies.

C. Moving Target Defense (MTD) in Cybersecurity

Moving Target Defense (MTD) is a relatively recent paradigm that introduces dynamism into system configurations—such as IP hopping, runtime environment switching, or resource relocation—to increase uncertainty for adversaries [9]. Jajodia et al. [10] laid the groundwork for MTD by establishing its role in creating asymmetric complexity for attackers. Okhravi et al. [11] and Carter et al. [12] later implemented MTD in network and cloud environments, demonstrating reduced attack surface exposure. However, most MTD implementations focus on system-level parameters and rarely extend to cryptographic schemes.

D. Integration of AES with MTD Techniques

Few studies have attempted to integrate AES with MTD to enhance cryptographic resilience. Lee et al. [13] proposed a dynamic AES model with periodic key changes, which improves unpredictability but lacks

integration with real-time threat assessment or system reconfiguration. Similarly, He et al. [14] introduced a virtualization architecture using MTD to reduce VM predictability, but the framework didn't encompass cryptographic security.

E. Adaptive and Proactive Security Models

Recent advancements have pushed towards self-healing and adaptive cloud security systems. Li et al. [15] developed a self-healing cloud framework capable of detecting and recovering from intrusions autonomously, emphasizing proactive resilience. Still, the cryptographic layer remained static. The current literature reveals a research gap at the intersection of adaptive AES encryption and MTD, particularly for real-time cloud environments.

Table 1. Literature Review Table: Adaptive AES-Driven Encryption for Moving Target Defense in Cloud Environments

S.No	Title	Authors	Year	Methodology	Findings	Limitations
1	A View of Cloud Computing	Armbrust et al.	2010	Conceptual overview of cloud computing models	Outlined the fundamental challenges in cloud security and scalability	Did not focus on encryption or defense mechanisms
2	A survey on security issues in service delivery models of cloud computing	Subashini & Kavitha	2011	Survey-based study	Identified key security concerns in SaaS, PaaS, and IaaS	Lacked detailed solutions or cryptographic approaches
3	Announcing the Advanced Encryption Standard (AES)	NIST	2001	Standard specification	Introduced AES as the new encryption standard	No adaptive or dynamic enhancements addressed
4	Cross-VM side channels and their use to extract private keys	Zhang et al.	2012	Experimental attack implementation	Demonstrated vulnerabilities in cloud VM isolation	Did not propose encryption countermeasures
5	Security and privacy in cloud computing: A survey	Zhang et al.	2013	Comprehensive survey	Identified existing solutions and challenges	Lacked proactive defense strategies
6	Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats	Jajodia et al.	2011	Theoretical and practical MTD exploration	Laid the foundation of MTD in cybersecurity	No specific application to AES or encryption
7	Moving target defense for cloud-based services	Carter et al.	2014	Framework design	Introduced MTD principles for cloud infrastructure	Encryption integration not discussed
8	Security challenges for the public cloud	Popa et al.	2011	Security analysis	Highlighted cryptographic vulnerabilities in public clouds	Did not provide adaptive encryption strategies

9	Dynamic defense technique using moving target mechanism	Cheng et al.	2017	MTD system design	Demonstrated improved resilience through dynamic shifting	Limited integration with cryptographic systems
10	Adaptive cryptographic techniques for secure cloud data	Lee et al.	2016	Adaptive encryption system	Enhanced AES with periodic key changes	Did not incorporate MTD architecture
11	Key management for cloud environments	Ali et al.	2014	Key lifecycle analysis	Discussed effective key generation and revocation schemes	Static key models were emphasized
12	A taxonomy of cyber attacks on cloud services	Modi et al.	2013	Taxonomy development	Classified threats and suggested defenses	No specific encryption defense strategy
13	A lightweight AES implementation for embedded devices	Moradi et al.	2011	Hardware implementation study	Reduced AES power consumption and execution time	Not suitable for adaptive or cloud-based models
14	Proactive security with moving target defense	Okhravi et al.	2013	MTD system implementation	Demonstrated increased attack complexity	Limited scalability to cloud platforms
15	Dynamic key generation for secure communication in cloud	Sharma et al.	2018	Entropy-based key system	Enhanced key unpredictability and renewal	No MTD strategy included
16	Survey on secure cloud storage	Khan et al.	2015	Survey and comparative analysis	Highlighted encryption and access control schemes	Adaptive techniques not covered
17	Efficient key management in cloud computing	Ruj et al.	2011	Hierarchical key model	Improved scalability and security of keys	Did not address key dynamics
18	Side channel attacks on AES: A review	Mangard et al.	2007	Review of side-channel vulnerabilities	Exposed weaknesses in static AES usage	No dynamic or MTD countermeasures suggested
19	Self-healing systems for cloud security	Li et al.	2019	Autonomous detection and recovery	Promoted proactive resilience	Encryption layer not integrated
20	MTD-based secure virtualization architecture	He et al.	2020	Virtualization with MTD	Reduced predictability of VM behavior	Did not enhance encryption practices

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][2].

A. Characteristics of Cloud Computing

- **Ultra large-scale:** In ultra vast scale processing, the size of cloud is extensive union[5]. 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. MODULE DESCRIPTION

Admin Modules

- Login
- User Details
  - Add User
  - Edit User
  - Delete User
  - View User Details
- Cloud Details
  - View Details
- Transaction Details
  - Select User
  - View log Details
- Sign Out

User Modules

- Login
- Show Profile
- Upload a File
  - User has to select the file from the local system
  - File Encrypted using AES Encryption
  - Upload to cloud storage
  - Insert a Transaction Record
  - Show Upload Successful Message to user

- **Download a File**
  - View details of all the uploaded file
  - User has to select the file to download and initiate the download process
  - Download all the file
  - Apply AES decryption to decrypt downloaded data
  - Show download Successful Message to user
  -
- Transaction
- Sign out

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.

- **Data Encryption Standard (DES) Algorithm:** AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

  Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

  Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

- **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[6][3]. 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[16]. 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.

VII. RESULTS

In this proposed work we have developed Web application. For implemented we developed a web page to register the user, data owner and admin. We created a method where user can share files to other users. We have designed a page in which user can simply enter the id of person whom to transfer the files and file gets uploaded to cloud server and name of the files get saved to MYSQL database table. When user want to download the file he must send a request to data owner and then data owner may give permission to download by sending a key mail to the requested user. RNS and DES algorithm is used for Encryption.

Table 2. Data Security Enhancement

SN	Existing System	Proposed System
1	No Encryption techniques is used	Proposed system provides high security for data.
2	Directly uploading data to cloud storage. For example Google drive	Before uploading data to cloud, data get encrypted, with AES encryption.
3	In cloud storage all get stored in single place / file / folder	Proposed system provides distributed storage in cloud. Data get stored in different folder / place / file

VIII. CONCLUSION

In an era of increasingly sophisticated cyber threats, static encryption schemes and conventional security architectures fall short of providing robust protection for cloud environments. This paper has presented a comprehensive review of existing literature at the intersection of cloud security, AES encryption, and Moving Target Defense (MTD). The findings reveal significant limitations in traditional AES implementations, particularly in their susceptibility to side-channel attacks and the predictability of static key management systems.

While MTD has emerged as a promising strategy for increasing system resilience by dynamically altering system configurations, its integration with cryptographic mechanisms, especially AES, remains underexplored. The synthesis of research highlights a critical need for adaptive security models that can combine the strength of AES encryption with the proactive capabilities of MTD.

Our proposed framework aims to address this gap by introducing an Adaptive AES-Driven Encryption model embedded within a Moving Target Defense strategy. Such integration not only enhances cryptographic unpredictability but also significantly complicates an attacker's reconnaissance and exploitation phases. Future work will focus on implementing and testing this framework in a simulated cloud environment to evaluate its performance in terms of resilience, latency, and computational overhead.

Ultimately, this approach paves the way toward more resilient, intelligent, and self-adaptive security architectures that can evolve in tandem with the dynamic threat landscape of modern cloud computing.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[3] NIST, "Announcing the Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.
[4] Y. Zhang et al., "Cross-VM side channels and their use to extract private keys," Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 305–316, 2012.
[5] R. Zhang et al., "Security and privacy in cloud computing: A survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.
[6] D. Jajodia et al., Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, Springer, 2011.
[7] K. M. Carter et al., "Moving target defense for cloud-based services," IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.–Apr. 2014.
[8] S. Sharma et al., "Entropy-based dynamic key generation for cloud data security," IEEE ICC, 2018.
[9] M. Okhravi et al., "Survey of moving target defenses," MIT Lincoln Laboratory, 2013.
[10] S. Jajodia et al., Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, Springer, 2011.
[11] M. Okhravi, T. Hobson, D. Bigelow, and W. Streilein, "Finding focus in the blur of moving-target techniques," IEEE Security & Privacy, vol. 12, no. 2, 2014.
[12] K. M. Carter et al., "Moving target defense for cloud-based services," IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, 2014.
[13] H. Lee, J. Kim, and M. Kim, "Dynamic AES encryption for real-time cloud applications," J. Inf. Secur. Appl., vol. 29, pp. 10–18, 2016.
[14] H. He et al., "MTD-based secure virtualization architecture for cloud computing," J. Cloud Comput., vol. 9, no. 1, 2020.
[15] X. Li et al., "Self-healing mechanisms for proactive cloud security," Comput. Secur., vol. 87, 2019.
[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.