A Vulnerability to Storage Security for Cloud Computing

Md. Afroz, Birendra Goswami

Sai Nath University, Ranchi, Jharkhand, India

Corresponding author: Md. Afroz, Email: afrozhasnain@gmail.com

Utilizing technology and new technologies in the digital world requires a safe and reliable environment as well as a consideration for all the challenges they present, and dealing with them. There is no exception to the rule of cloud computing being one of the new technologies in the IT world. Various studies reveal that one of the major challenges of this technology is the security and safety required for consumers to transfer their data into the cloud. In this paper by reviewing and highlighting security challenges in a cloud computing environment, we aim to highlight the security challenges that cloud computing poses. The article also offers some suggestions on how to enhance the security of data storage in cloud computing systems that using these suggestions can somewhat override the problems.

Keywords: Cloud Computing, Data Security, Security, Information Security, Trust

2023. In Satyasai Jagannath Nanda & Rajendra Prasad Yadav (eds.), *Data Science and Intelligent Computing Techniques*, 893–910. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-2-8-76

1. Introduction

The advent of cloud computing involves a paradigm shift significantly High-Performance Computing (HPC), enterprise, web applications promising an infrastructure that is scalable and cost-effective. Providing rapid scalability and flexible pay-as-you-go pricing models, this transformative technology empowers businesses with a host of third-party cloud-based services and applications without the financial and logistical burdens of in-house infrastructure. No doubt, the repercussion on IT capital costs, labor expenditures, and productivity enhancement is outstanding from cloud computing to say list that can refer to as a key tool of today's modern business operations.

This is further championed by the fact that cloud computing has been intrinsically designed so as to optimize costs while at the same time enhance computing capacity and financial outcome for users. Studies on cloud computing optimization have revealed that this optimization factor is only not important but also crucial to the IT sector as it fostered increased collaboration, speed, and scalability while simultaneously reducing cost. The technology opens doors for life changing opportunities for growth and innovation previously unheard of, to many large enterprises and IT companies especially located in the developed countries.

However, these opportunities come on the backdrop of challenges as well as security concerns. Security in the arena of cloud computing comprises a very critical issue that affects both management of personal data on public networks and storage of user data on servers of the cloud service. The reliability and effectiveness of the security services are essential in that if their provision is not sufficient, it will translate into great risks as well as vulnerabilities.The process of cloud computing is most pegged upon the assurance of tightened security in place. If the above security barriers to cloud technology can be effectively removed or, at least, minimized by the technology provider, then come what may, cloud computing stands a good chance of acting as one of the cornerstones in the field of Information Technology. Hence, the fundamental challenge is to stir up trust in cloud computing -- especially sharing applications, hardware and other resources when there seems to be no clear accountability in the handling of client's data.

This trust can only be built when the issues faced in terms of security in cloud technology, with a particular emphasis on data storage security, are addressed. This paper outlines areas that are challenging when it comes to security in the cloud computing domain, pinpoints major issues and strong weaknesses in current research, and suggests enhancements meant for improving its security.

Creating the trust with the user in transferring and storing the data onto cloud servers are very important for the use and growth of that technology. Moreover, accounting for such key global economic issues as reducing the purchasing power, the identified security challenges and public confidence in cloud computing services can be treated not only as guaranteeing data security but cost-effective solutions for about each person and government.

Resolution of the security challenges will realize strong building up for the development and expansion of cloud computing. Vast economic efficiency and technological advancement in the IT industry is what could be achieved through such a resolution, thus harnessing the huge potential that exists for cloud computing, once a secure trustworthy cloud environment is built.

2. Previous Works

Since the inception of computer networks and the expansion of the Internet, the importance of data transfer and storage security has grown exponentially. This is particularly crucial given the technological advancements and the need for secure channels to transfer high-volume, high-importance data. This paper presents an overview of existing efforts to enhance data security, with a specific focus on cloud computing environments.

Tsai W et al. in [5] proposed a four-layer framework for the development of Web-based security, offering an intriguing perspective. However, this framework only tinkers with one aspect of security. One important facet of strategies for secure data during its processing involves the grouping of processor's cache in virtual machines and separating the virtual cache from the hypervisor cache [6]. This brings to focus the importance of isolation as an element to ensure data integrity.

In Reference [7], different ways of implementing a dynamic security framework were introduced. One factor needing care is that access and storage management for data are being managed and controlled by means of metadata. This strategy involves the related data stored at different locations, controlled by the metadata and may allow the recovery of the same data while it is breached. The concept of "security as a service", is also being elaborated to depict the applications in real life for the security layers or even multiple layers required for the applications [7].

This research highlights the concept of cloud security and the applicability of the security measures in realistic situation, which are subject to individuals' and organizations' practices. While having "security as a service" is an attractive proposition but at the same time it casts doubt over the focus allocated by the service clients. If providers concentrate predominantly on security, it might detract from the development and delivery of other software services [7, 8].

M. Ahmed et al. [9] examined specific security issues related to cloud computing, aiming to establish a secure communication channel with Cloud Service Providers (CSPs) while maintaining data reliability and confidentiality. They also compared the protocols provided by SSL with fair security practices for data protection.

The paper [10] delves into security issues at different levels of cloud computing architecture, encompassing Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It emphasizes the critical need for customer data security across all cloud computing models [10], highlighting the ongoing challenges and solutions in cloud security.

This paper emphasizes the significance of robust security measures in the utilization of cloud services, particularly for applications operating across Internet-connected domains. As cloud computing continues to evolve, so too must the strategies and frameworks for ensuring data security, reflecting the dynamic nature of threats and the need for innovative, effective solutions.

3. Cloud Computing

Cloud computing, with its diverse manifestations and capabilities, offers distinct interpretations and applications, contributing to its broad spectrum of understandings. This diversity is reflected in how some perceive cloud computing primarily as a platform for web-based applications, while others view it as a tool for efficient and parallel computing, particularly suited for complex and large-scale processes [12], [13]. Beyond its various forms, cloud computing also provides a wide range of distinct and diverse services [3].

The definitions of cloud computing are numerous, and several have been discussed in this context. The National Institute of Standards and Technology (NIST) of the United States defines it as [2], [12], [14], [15]: "Cloud computing is a model for enabling 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." Another common and widely accepted definition by Mater et al. [4], [16] describes cloud computing as "A highly scalable tool, with the capability of service generation-enabled, which can be easily used through the internet whenever needed."

To fully comprehend and effectively utilize cloud computing, it is crucial to understand its essential features, deployment models, service usage methodologies, and security measures [15].

The five key characteristics of cloud computing are [2], [17]:

- **On-Demand Self-Service:** Users can independently access computing facilities like servers, storage, and networks as needed, without requiring manual intervention.
- **Ubiquitous Network Access:** Services are accessible over the internet using standard methods, supporting both robust (computers) and more limited (mobile phones) client platforms.
- **Location-Independent Resource Pooling:** Providers dynamically pool computing resources to serve diverse consumer needs in a shared environment. These include resources such as storage, memory, bandwidth and virtual machines.
- **Rapid Elasticity:** The rapid elasticity ensures that there is a guarantee which proves easy to assure that the provision and de-provision of resources are scalable so as to ensure that services are current and scalable with no hitches.
- **Measured Service:** Cloud systems enable the monitoring, management, and reporting of resource usage, providing transparency for both consumers and providers.

As per the National Institute of Standards and Technology says, deployment models for cloud computing encompass [19]:

- **Public Cloud:** Being that this paradigm permits cloud service providers to offer infrastructure and services over the internet, such a cloud is obtainable for access by the general public.
- **Private Cloud:** It is set up for use by a particular organization only, and it offers services and accessibility to data that are limited within the organization such that it is out of reach to outsiders.
- **Community Cloud:** The community cloud is tailored to organizations sharing similar goals and needs, intending to share infrastructure among a few entities often having unique requirements.

Hybrid Cloud: Hybrid cloud combines two or more cloud types (public, private, community) thus enabling the use of mixed external and internal cloud services with a goal of building flexibility and adaptability in the computing environment.

Cloud computing's multifaceted nature, characterized by its key features and deployment models, underscores its versatility and adaptability, making it a vital component of the modern IT landscape. Its capability in catering to a wide portfolio of requirements, starting from individual consumer needs to big-budget enterprise solutions, specifies its significance in the world of digitization today. Usually, services in the cloud computing domain are delivered through three archetypal models that offer a different degree of user control and customization. They are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1], [2], [18]:

Software as a Service (SaaS): This offers users application software and databeses. The main thing that happens here is that the service gets written via the internet, in most cases using a web browser. All infrastructure of the cloud comprising servers, networks, operating systems, and storage is handled by the service provider. While this underlying infrastructure is controlled by the provider and users have no control over it, there can be some customization of application software with the users, albeit within some restricts defined by the service provider [20], [21].

Platform as a Service (PaaS): PaaS offers a level above SaaS, where clients can deploy their own applications using programming languages and tools supported by the provider. Like SaaS, in PaaS, the underlying cloud infrastructure (networks, servers, storage) remains outside the user's control. However, users have more control over the deployed applications and possibly the hosting

environment configurations. PaaS provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the underlying infrastructure typically associated with the process. This model is more useful in software development which offers for different development tools and services [20], [21].

Infrastructure as a Service (IaaS): AaS very basically offers computing resources over the cloud. This model of service provides computing power, storage, network, and other basic computing resources about which the customer runs arbitrary software including operating systems and applications. The end-user does not have any management or control of the underlying cloud infrastructure but remains in control of operating systems, storage, and deployed applications. With its clients having a high degree of control over their IT facilities, IaaS is a highly flexible service often referred to by them for data storage, website hosting, and as a backbone for PaaS and SaaS services [20], [21].

The application of these service models of cloud computing brings an abstraction and control model at different levels to cater for the diverse needs and technical capabilities of the user. SaaS presents ready-to-use applications, PaaS serves up a platform for developing and deploying applications while IaaS offers fundamental computing resources. Understanding these models becomes important to the business or an individual as it will guide them in choosing the appropriate cloud services in regard to their requirement and technical expertise.

4. Security in Cloud Environment

Information security forms one of the paramount aspects within the IT sector, playing a very critical role when it comes to ensuring the success of any given system. This is no exception to cloud computing, which forms one of the greatest facets within the IT industry. The nature of cloud computing, whereby a user may not know with certainty details on how his data are being handled, and the location with which his data are being stored escalates the importance of very robust security measures [2]. That is why the security challenges in cloud computing have numerous facets and, to a greater degree, are defined by service models as well as deployment strategies used. Thus, these factors define the level of trust related services delivered by cloud technologies [11].

This is because internet-based service delivery, normalization protocols, and encryption techniques implemented in the system make the cloud expect stringent security measures. These are protocols that need to be so effective though comprehensive enough that will provide strict data transmission security within the cloud environment [2], [7], [8]. Key security threats to cloud computing especially the data in it include:

Data Location: In a cloud environment, where organizational or business information will be hosted and processed is most important issue. Agreements with the cloud service providers should stipulate data storages and processing places. This consideration is another step in assuring data security but allowing also the legal recourse of maintaining the data integrity and compliances to relevant laws and regulations [22].

Data Isolation: Because the cloud environments are mostly dealing with shared storage spaces, the data belonging to different clients is stored together. Effective measures must be considered by the cloud providers for the isolation of data. This requires putting the correct mechanisms in place to make sure that data from one client cannot be accessed or compromised by another. Ensuring such isolation is critical in securing clients' trust and the security of explicit information [23].

Server Flexibility: One most pronounced advantage of cloud computing is due to the fact that the servers are very flexible and can quickly scale or modify. However, this can be risky when it comes to

matters of security. Problems come in when there is much modification of the servers in regards to configuration and little or no notification given. All these sorts of changes can affect the reliability and security of the data linked with a particular business. These regular updates or modifications if not managed and informed properly may give birth to compromises with data security [23].

These security threats should be addressed as they may compromise the integrity and reliability of cloud computing services. Effective mechanisms have to be implemented to manage the location of data, ensure its isolation, and also the parallelism and flexibility of servers without breaching thesecurity. As cloud computing matures, the service providers and users must be vigilant and proactive in the management of these security concerns so that cloud computing can continue being a trusted as well as reliable element of IT asset.

5. Data Storage Security in Cloud Computing

Data storage security, therefore, is one of the principal components of cloud computing and therefore incorporates data protection therein based on various media and their integrity while ensuring the fast recoverability of the data in case there is loss [28]. Redundancy and dynamic data handling along with data separation and others are some of the security aspects that software engineers needing a design of the cloud storage system must consider.

Redundancy: One of the main mechanisms in the area of data storage security is redundancy. This entails creating several copies of data in different locations or systems so that when there is failure of the hardware or other reasons arise, the organization does not lose data. This is because user data is dynamic and needs to be updated frequently, so efficient mechanisms are essential to maintain data consistency throughout these redundant copies.

Dynamic Data Handling: Dynamic Data Handling can be referred to as the ability to handle efficiently the data that keeps on changing. This indicates that any changes made at a particular end by any user should reflect instantaneously in every point of storage so that the data at all times remains up to date and, in a state of accuracy.

Data Separation: Data Separation refers to the ensuring that the user's data remain in segregation and not accessed by another user. That is, the segmentation that ensures that one user's data do not get mixed up with second user's, hence keeping the confidentiality and integrity of the data for each separate user and avoiding instances like unauthorized access or modifications of another user's set of data.

Cloud storage is distributed virtualized servers accessible over the internet in which data can be stored instead of local systems [23]. Users, therefore, can have their data on these cloud servers and can make it readily available rather than maintaining physical space for the same. The elasticity of cloud storage allows a user to scale their storage needs theoretically and only pay for storage which is actually used [25]. However, as any distributed storage system, the cloud storage has its further security challenges [26].

Key considerations for security of data in cloud storage are achieved by providing the client (user device), the server (where the data is stored) and the communication channel between them with security [23].

Client Security: It is security of user's device from unauthorized access.

Server Security: The data on the server at all times need to be secure, reliable, and accessible.

Communication Security: o avoid intercept or tamper with the transmission data between the server and the client, it is imperative that the data be transmitted through a secure channel. Protocols, such as SSL (Secure Sockets Layer), have been extensively used to make these sorts of communications secure [24].

Amazon, Google, or Dropbox - all prominent cloud storage providers - assure data protection from cybercriminals and employ encryption to increase this effect. At the same time, data security details can be different in terms of every available system on offer and specific user needs. For instance, digital libraries may focus on the consistency of data more than value in secrecy thus requiring a strong mechanism for necessarily not focusing on the encryption of the data but ensuring accuracy of data.

Through methodologies as Proof of Retrievability (POR) and Provable Date Possession (PDP), the cloud storage providers promise their clients on data recoverability as well as integrity. One of the most effective approaches towards achieving this is by use of POR that promises to confirm data recoverability without necessarily having a complete download of file [20].

Access Control Cryptography is a user-centric approach where the data encryption is done locally on the device of the user before uploading it to the cloud. Here, the data security in this way gets improved and increases its level of confidentiality as well. For example, Amazon does provide a library "AmazonS3 Encryption Client" for local encryption but it requires technical expertise from the user to implement the whole mechanism which most of the users may not be easy with [25].
securing data storage in cloud computing entails an approach that layers the security of the data stored, devices that access the data, and even channels that are used to deliver the services. As cloud computing expands, these vulnerabilities can be addressed through the introduction of robust and user-friendly security solutions that will be the driving force in ensuring the trust and confidence in the continued adoption of cloud services [35].

6. Vulnerabilities in Cloud Computing

As organizations gear up in opting to migrate their critical applications and data to cloud computing environments, it becomes imperative taking cognizance of a variety of threats that could result in the violations of the integrity, security, and reliability of its systems. The following are some of these vulnerabilities encompassed within the cloud computing nature:

6.1 Session Riding and Hijacking

It is a situation whereby one uses a valid session key usually helped by theft of cookie used for user authentication to gain unapproved access to data or services. This vulnerability, very characteristic for technologies used in web applications, allows infiltrators to exploit deficiencies of a structural origin for nefarious purposes. Session riding is another concept that pushes web applications users against their will to carry out undesired actions on the same. These could be deletion to user data, unauthorized transactions and even comprise of system configurations [35]. The escalating web technologies are constantly emerging with new attacks and threats to the security of the data and the activities of the online businesses.

6.2 Virtual Machine Escape

The only difference is that the virtual machines (VMs) in cloud computing share common operating systems and applications for their physical counterparts. Remote attackers basically exploit the vulnerability that is available in the virtualized cloud environment. The co-location of multiple VMs expands the attack surface, increasing the risk of inter-VM compromises. One major vulnerability is the

'VM escape' whereby an attacker can run code that escapes the VM and interacts directly with the hypervisor, allowing potential control of the host system.

6.3 Service Availability and Reliability

As much as it is superior, cloud computing is not faultless when it comes to reliability and accessibility. Instances such as the December 2021 outage for Amazon Web Services (AWS) show that even the cloud infrastructures can suffer from disruptions. Outages can cascade through and affect a myriad of internet-dependent services and applications. This will raise questions on the responsibility of cloud service providers and the mechanisms in place to avert such failures.

6.4 Insecure Cryptography

Challenges constantly face cryptography as attackers find different ways of cracking cryptic algorithms. However, in most occurrences, the algorithms are often implemented with flaws that weaken the strength of the desired encryption. A major issue in cloud environments is getting to random numbers which are fundamental to strong encryption especially in virtual machines of less sources of entropy against physical servers.

6.5 Data's Portability and Protection

The relationship between a cloud service provider and its clients is contractual, but all issues pour when a client choses to terminate business. Issues include provider misuse or retention of client data and what becomes of the client data and services if the provider folds. These all add up for continued challenges to trying to ensure security as well portability of data in cloud computing.

6.6 Vendor Lock-in

The cloud computing market identifies emerging service providers and business models and the risk of vendor lock-in. As a result, for the clients, there is a dependency on one provider that hampers them from switching to another provider easily because of its heavy switching cost for changing the provider easily. In addition, as the protocols in this domain are not standardized at all, so it hardly leaves any flexibility for the clients.

6.7 Dependency on the Internet

The fact that service delivery of cloud computing depends on the internet exposes an organization to huge risks, especially in cases where its accessibility is either unreliable or totally not possible at any given time. This characteristic dependency on the internet therefore raises questions as to whether it is actually best for an adoption of the platform for critical systems, which are housed in parts of the world with unreliable access to the internet.

Although cloud computing offers new and flexible innovative solutions for business operations, there are also various risks and vulnerabilities surrounding it. Therefore, implementing proper measures to resolve these problems is extremely important in the context of adjusting cloud technologies securely and effectively. In the following sections, some of the modern algorithms and methods will be discussed in respect of their improvement or enhancement of the data storage security on the cloud computing environment or platform within which they are implemented.

7. Existing Algorithms for Data Storage Security

7.1 RSA Algorithm

The RSA algorithm, one of the important public key cryptosystems, is used by the vendors to encrypt and decrypt data. As a first-generation algorithm, RSA has established its place in the realm of data security providing a robust mechanism for secure communications without any need for exchange of any unique secret key between the parties.

The RSA is a very versatile digital signature and public key encryption algorithm. The strong security underlying the process rests on the computational difficulty associated with factoring large integers, hence its power against decryption without authority. The process includes here two parties: A1 and B1. Here Party A1 sends an encrypted message to Party B1 with no exchange of secret keys prior. The encryption is really done by using the public key of A1, and B1 then decrypts it with his private key which not accessible to nobody else. In a digital signatures usage, A1 can sign a message with his private key and B1 is able to verify the signature from A1's public key. These dual function capabilities of the RSA algorithm posses increased utility for a wide variety of cryptographic applications.The method of RSA algorithm occurs in the following three core steps: key generation, encryption, and decryption.The RSA algorithm operates through three fundamental steps: key generation, encryption, and decryption.

Key Generation: During this step of the method, two prime numbers called as p and q are taken. Using random numbers but they are mandatory in terms of key generation. The product of p and q is calculated to obtain n (n = pq), which is used in both the public and private keys. The choice of large prime numbers for p and q is very important to assure that the encryption is strong because the product of two large primes cannot be factored easily such as in RSA.

Encryption: This is the stage where the message was encrypted with the sender's private key. The keys contain an exponent as well as a number whose combination produced n (formed from p and q). The message was converted into a ciphertext only unlockable using the public key.

Decryption: The recipient uses now his private key to decrypt the message. Again it is derived from same values of p and q but a different or uniqueness exponent. The private key is kept secret now and is used for enabling the recipient to actually decrypt messages that are encrypted using his public key.

The strength of the RSA algorithm comes from a simplicity to operate with the encryption not easily broken due to large prime factorization to promote secure communication and verification without sharing private keys between entities. This has made RSA an important tool in modern day cryptography since it is universally used for securing the transactions of data through varied platforms and applications.

Then a function (n) calculation is made: $\varphi(n) = (p - 1)(q - 1)$.

Additionally, an integer e is selected so that $1 < e < \varphi(n)$.

Then, the value for d comes out to be: $d = e\text{-}1 \bmod n$, since $de \bmod n = 1$ and e and n are co-prime. This way, the private key becomes (n, d), and the public key is (n, e).

The encryption text formula is $c = m^e \bmod n$, and the decryption text formula is $m = c^d \bmod n$ [28].

7.1.1 RSA algorithm's Security

This very strong algorithm RSA in its early years of development was subjected to various attacks despite its robustness. Nevertheless, continuous developments and rework on the attacks have

diminished the efficacy of such attacks. One of those developments drastically improves RSA security by suggesting unique modulus (n = pq) mechanism for each user as a remedial measure against a prevailing vulnerability.

In systems where a common modulus is used for all users, a significant security risk emerges.

In such a situation, if the central authority generates both public and private keys by using a prearranged common value for n, it would be possible that some user has (A1) opportunity to factor the modulus n with their own exponent (e and d). This would mean that A1 can deduce another user's (B1's) private key using B1's public key itself. The fix for this vulnerability is rather simple, just don't use the same common n over all users. In those systems in which each user independently generates his key pairs in their devices, it is unfeasible for this attack to be executed due to the simple fact that every one of the users will have a unique value of n as a product of two unique prime numbers chosen independently. Another distinguished attack on the RSA algorithm is a timing attack. Such kind of attack uses the time that is necessary to perform such cryptographic operations like a digital signature or some other encryption/decryption process.

Therefore, an attacker listens to the time of such operations with the purpose of guessing the private key. Timing attacks are of special interest for network-connected systems or systems using smart cards. Although a smart card ensures the contents stored within it, an attacker can analyze immediate response times of the card's cryptographic operations in order to infer the private key. It must be noted that, unlike other cryptographic threats, timing attacks do not require direct access either to the cryptographic device (like a smart card) or the system. These attacks can be remotely done, hence positing a major concern for those systems whose response times can be monitored from a network.

Most cryptographic implementations use constant-time operations to make sure that processing time subtly communicates no information about either the data being processed or, more importantly, about the key. Thus, minimizing the risk of timing attacks.

Although the RSA algorithm has faced various threats throughout its lifetime, continuous changes have greatly strengthened it. From the use of unique moduli per user to the implementation of constant-time cryptographic operations are key improvements towards these attacks. Like any other modern cryptographic system, alertness and adaptation have to be continuously exerted against the arising threats keeping intact the integrity and security of RSA algorithm.

7.2 Elliptic Curve Cryptography (ECC) Algorithms

Eliptic Curve Cryptography (ECC) is the most recent and the significant improvement in the process of developing public key cryptographic algorithms offering increased security measures and greater efficiency than other contemporary methodologies including the RSA. One of the most notable features that makes ECC stand out is its ability from the field to provide security equivalent to other asymmetric systems with much shorter key sizes. A 256-bit key for ECC, for example, provides an equivalent level of security as a 3072-bit key of RSA [27]. ECC is thus particularly advantageous when the environment has limited capacity to bandwidth or storage as this efficiency in key size translation becomes an advantage that stands out.

First presented at IBM in 1985 by Victor Miller and at the University of Washington by Neal Koblitz, ECC affects a revolutionary approach toward public-key cryptography. In reality, it is the mathematics of elliptic curves that provides a very strong foundation to the cryptographic systems, and this is the primary appeal of ECC. ECC is based on the mathematical principle of discrete logarithm that presents with equivalent key lengths a more difficult problem to an attacker than the factoring problem in RSA [27].

In the public key cryptography, to which RSA along with ECC belong, every participant preserves a pair of keys: the public key as well as the private one. Such keys play unique yet essential roles in the processes of encryption and decryptions:

Public Key: This is openly given to its participants in the communication process. It enables recipients of messages in open communication to verify or decrypt a digital signature. In ECC, the public key is generated by using elliptic curve mathematics from the private key that makes it infeasible for anyone to be able to deduce the private key from knowledge of the public key.

Private Key: The private key is a secret key and known only to the owner of the key. It is used for message decryption or suitable signing off of digital documents. Within ECC structure, the most apparent concern is expressed by the private key since encryption and decryption are possible without six good digits of the private key.

ECC provides a very high level of security with smaller key sizes and thus can be realized with not only less computational and storage requirements but also much improved speed, as compared to other contemporary symmetric and asymmetric algorithms, which make it very attractive for modern day cryptographic applications. Its adoption is more particularly beneficial in contexts, when the prime concern moves towards the availability of resources such as mobile devices or IoT applications, where efficiency and security both are critically required.

Elliptic Curve Cryptography is an efficient and provably safe way to apply public-key cryptography. Based on the esoteric branch of mathematics that deals with elliptic curves as well as discrete logarithms, it places a formidable obstacle in front of cryptographic attacks and hence has remained a favored option in a large number of modern applications that require security.

7.3 Data Encryption Standard (DES)

The block cypher Data Encryption Standard (DES) blocks size is 64 bits. It was invented by IBM in the 1970s and announced as a standard of data encryption in the United States of America in 1976. It had originally been used within the borders of only the United States of America, and as time went by it was raced internationally and became popular all over the globe. In 16 cycles DES employs substitutions and transpositions one after the other in a fairly convoluted manner [24]. This approach has the fixed key length of 56 bits which seems insufficient taking into account the steady improvement in computing power that had already been demonstrated. However, worth noting is the fact that 3DES also known as triple DES is an attempt used to make DES harder to crack. In 3DES, each block of data is encrypted thrice using DES that extends the key in this course. In reality, it uses a "bunch of keys" consisting of three DES keys K1, K2, and K3, each 56 bits long [24].

This realization prompted a further advancement of DES to create a better version, called Triple DES or 3DES, which was meant to fortify cipher resistance against breaking.

3DES improves the security to the vulnerability of the original DES algorithm through applying the process of DES three times on each block of data during encryption. The triple encryption makes it cipher more secure against attacks that may be mounted against it due to the effective increase in the length of the key and complication of the method of decryption. The 3DES method utilizes a series of three DES keys - K1, K2, and K3 - each 56 bits in length.

In practice, such keys can be used in various configurations: three distinct keys for maximal security, two keys where the first and third keys are the same which is more secure but requires the user only two keys, a mode that is possibly an acceptable compromise between the two considerations.

It should be pointed out that the effective key length of 3DES that can be effectively used will depend on the way the keys are being arranged

3-key 3DES: The configuration will involve use of three keys but in different arrangements. This gives the highest security level, and therefore its effective key length is equal to 168 bits (56 bits × 3).

2-key 3DES: It compiles the use of two keys with the first and third keys which are same (K1 = K3). Its format is stronger than DES with lower resource requirement as for 3-key 3DES. Basically, it provides an effective key length of 112 bits. While 3DES is often regarded as stronger, it has fallen out of favor to more advanced encryption standards such as AES (Advanced Encryption Standard) due to its slower processing time and the fact that it is weak against some cryptanalytic attacks. It has, however, made significant contributions to the field of cryptography by bridging the gap between the original DES and the more modern encryption algorithms.

DES and its successor 3DES are probably the most significant milestones in cryptographic history showing simultaneously people's struggle to create encryption techniques in line with phenomenal growth of computational power, and at the same time constant need for even more secure data protection techniques.

7.4 Triple Data Encryption Standard (Triple DES)

Therefore, Triple DES (3DES) was born as a powerful successor to the original Data Encryption Standard (DES) algorithm filling in on those weaknesses of DES that were being exploited by smart hackers. 3DES, being a symmetric encryption method, at one time turned out to be the most used symmetric algorithm across industry segments world wide. However, with strong and fast strides in cryptographic technologies, 3DES has been slowly losing its strong foothold [29].

At the core of 3DES is the essential principle that the DES algorithm is performed three times on each data block. With this triple layer encryption, it makes 3DES three times as efficient in providing security than its vintage counterpart. The process involves using the first key to encrypt the data block, using the second to decrypt it (which essentially adds another bit of ordering information) and then the third to re-encrypt it. This does not only complicate the method of encryption but also increases the level of difficulty from the attacker's end by a great extent to breach the cipher. 3DES has found use in one important domain, that is, financial security. It is widely used to encrypt UNIX passwords as well as ATM PINs, sectors in which security for such sensitive details holds a special priority.

The choice of 3DES in these applications only emphasizes the belief put on its reliability by industries that handle critical and confidential data.

Though it is more secure, the move from 3DES to more advanced encryption like the Advanced Encryption Standard (AES) being essentially driven by its slower processing shots and operational imbalances while process in bulk. AES offers improved security with more efficient processing, making it the first preference in the contemporary cryptographic applications [33].

While Triple DES represented a huge leap in security compared to the original DES, its own phase-out operation is under process due to developments in cryptographic technologies that are rapidly growing. Yet, the legacy of 3DES remains untouchable due to its role in data protection, which was crucial at the time when conclusive development of digital security technologies occurred.

7.5 Blowfish

This is an algorithm that was developed by Bruce Schneier back in 1993, and thereby can easily be referred to as the stepping stone towards the development of symmetric encryption codes. Blowfish comes to notice because of its performance and flexibility features since it is a symmetric block cipher. Blowfish, with a block size of 64 bits and key length being variable, has been recognized for performance and security. Its standout feature for Blowfish is speed that largely illustrates trial as well as research analytical experiments. The algorithm is very efficient, from both the software and hardware implementation aspects as it aids quick encryption and decryption operations. Mainly, its simplicity of structure as well as the use of pre-computed substitution boxes (S-boxes) after setting the key facilitates such efficiency. In terms of key length, this allows for a highly flexible level of security from 32-bit to 448-bit keys. The flexibility provided by Blowfish makes it an effective choice for applications required to make use of adjustable levels of security without hindering the processing speed.

The architecture of Blowfish involves 16 rounds of encryption that provide a satisfied powerful and complicated transformation of every block of the input data. Every round applies key-dependent permutations and substitutions, which characterize Blowfish as quite immune to such known simple cryptographic attacks like brute-force, differential, linear cryptanalysis.

Blowfish presents considerable benefits in both energy consumption as well as throughput. The fact that this algorithm has low computational overhead makes the executions of the algorithm energy oriented particularly in powerful mobile devices and embedded systems where power conservation is a major concern. However, with the advancements of cryptographic research and advent of newer algorithms, Blowfish experienced a decline in its usage like other earlier interventions. Today, new applications are moving away from old algorithms to the new ones such as AES due to their larger block size and thorough security analysis. Nonetheless, Blowfish was significant within the historical context since it provided a design for quick and efficient symmetric ciphers.

The Blowfish algorithm adapts as the perfect proof of Bruce Schneier's cryptography skills when it comes to giving the right mixture between the speed and efficiency but with the necessary security. Its creation has left an inheritance that until today still establishes recursively at some point the way in which the cryptographic algorithms get at present designed and evaluated today, in the permanent search for the ideal method of data encryption with high levels in both security and efficiency.

7.6 Advanced Encryption Standard (AES)

The introduction and use of the Advanced Encryption Standard (AES) marked a significant step in the cryptographic practices, more so after the acknowledged weaknesses of Data Encryption Standard (DES). In January 1997, the National Institute of Standards and Technology (NIST) initiated a process to decide who would be the successor of DES, which invoked open competition among the worldwide cryptographic community. This ultimately led to fifteen diverse cryptographic techniques proposed by as many countries being considered for evaluation over a period of nine months.

Among them, the "Rijndael" algorithm designed by Dutch cryptographers Vincent Rijmen and Joan Daemen, stood out for its effectiveness and efficiency. The Rijndael algorithm was selected by NIST in 1999, and in two years, it was formally approved as the official AES encryption standard by NIST in 2001. AES acts as a block cipher to provide a block size of 128 bits. One of the distinct characteristics for AES is that the key length is flexible hence can allow a 128, 192 and 256 bits key. This flexibility thus offers a window for various secu-rity levels for several requirements and applications.

The structure of AES has two main cryptographic techniques: substitutions and transpositions. Unlike in DES, where 16 cycles were used; in this algorithm the amount of cycles that are called rounds is 10,

12, or 14 depending on the length of the key. Each AES round consists of four different steps, which offer a high level of security due to the way confusion and diffusion of the plaintext are effectively achieve. These steps include:

SubBytes (Substitution of Bytes): This is the simple step that consists in the non-linear byte substitution from pre-defined substitution table (S-box) to each byte. The transformation will be made within the state array.

ShiftRows (Row Shifting): The shift rows consist of scanning through the array and shifting the rows by different amounts which is done in a bid to achieve inter-block diffusion.

MixColumns (Mixing of Columns): It is the linear mixing operation that transforms the column of the state, further dispersing the byte values inside the column.

AddRoundKey (Addition of the Round Key): The state is now XORed with a round key. The round key is derived from the main AES key using a key schedule. This step puts the key into the state.

By combining these steps in each round, the security provided by AES against known cryptographic attacks is very high. AES's efficiency combined with the strong security profile made AES his preferred choice for encryption no matter whether this is used in government communications, financial transactions, or secure storing of data.

The transition that had occurred from DES to AES is a momentous occasion in history regarding cryptography. AES well designed and strong on security has today emerged as reigning default cryptography for contemporary encryption acting as a yardstick against which cryptographic algorithms should measure up during the digital era.

7.6.1 Modes of Operation for AES

In this Advanced Encryption Standard (AES) implementation, the data blocks are broken down into some distinct blocks in which each particular block is encrypted separately. In this approach, there is the compulsion to use various modes of operation defining distinct procedures for the process of both encryption and decryption of every block of data [24]. These modes are of overridding together in importance in securing the overall effectiveness of the involved encryption.

A common factor existing in most of these modes of operation in AES, apart from the differences therein, is an Initialization Vector (IV). An IV exists as a block of bits and adds uniqueness and non-repetition to the process of encryption. The IV is mainly used to introduce randomness within the encryption process. Introducing randomness enhances security by ensuring that any similar data block encrypted on multiple occasions will not reveal the same cipher text, hence practically impossible to lead to a pattern being formed for third-party analysis purposes.

The National Institute of Standards and Technology (NIST) has defined the six special modes of operations that are authorized for provision of data confidentiality in the operation of AES. Each individual mode possesses different characteristics considered to be suitable based on different federations of cryptographic applications:

ECB (Electronic Codebook): In this mode, each block of plaintext is independently encrypted. While it is very simple to encrypt in the ECB mode, it can reveal patterns in the plaintext and thus may be less secure in some applications.

CBC (Cipher Block Chaining): Here, the ciphertext blocks are chained with each next block by adding the previous ciphertext block to the current plaintext block before encryption. Identical

plaintext blocks will produce different ciphertexts, and that's why it is more secure compared to the ECB mode.

CFB (Cipher Feedback): CFB mode is a self-synchronizing stream cipher. It consists of smaller units of plaintext being processed and implemented in applications where block alignment is unsuitable.

OFB (Output Feedback): In addition to converting the block cipher into a stream cipher, it also introduces keystream blocks which are further XORed with plaintext blocks to get the ciphertext. The savings with this mode is that encryption errors do not propagate.

CTR (Counter): A counter value is given to each block of plaintext in CTR mode. The counter itself is encrypted and result is XORed with the plaintext. It's a quite basic method and can be simply parallelized.

XTS-AES (XEX-Based Tweaked Code Book Mode with Ciphertext Stealing): TS-AES is developed for the purpose of encryption of data over block-oriented storage devices. It provides the required critical security on the aspect of data-at-rest effectively [30].

Each of these modes fulfills some security considerations like the pattern hiding, error propogation and ability to parallelize. The choice of a particular mode is guided by the demands of the encryption scenario like the necessity of data integrity, confidentiality and the specific nature of the data being encrypted.

Making the proper choice of AES mode operation decision is a critical one, in any cryptographic design. It therefore strikes finely a balance between the need for the highest level of security possible while taking into account considerations such as computational efficiency and application-driven requirements, ensuring that AES can be used to encrypt data in a wide range of ways flexibly and securely.

7.6.2 Security of AES

The Advanced Encryption Standard (AES) is an epitome of cryptographic security technologies, with none of the weaknesses reducing its reliability having been legitimately disclosed. This robustness speaks of the serious scrutiny and analysis it passed before its use in the United States. AES was thoroughly studied and tested two years, reaching its credibility and being reliable as a premiere cryptographic algorithm. Primary of the important features in AES is its very good key security. The length of the key in AES is significantly much larger than its predecessor, DES, with a minimum of nearly double the security against brute-force attacks. The key length increased, coupled with the choice of further extension and the number of encryption rounds, makes AES stronger against attempts to make it vulnerable using large-scale computational resources. The flexibility to scale key length and rounds gives AES a defense mechanism that is malleable to be adapted following any increase in computational power in the future.

AES, with respect to the latest threats and the advancements of computational capability, is under constant analysis and research within the cryptography community. A dedicated website [31] catalogs these studies and developments giving insights on the current state of AES security. In particular, a 2009 paper [24, 32] detailed how to use a technique known as the "Related Key Boomerang" attack on AES with 192 and 256 bits. However, this study claims that while it gives the theoretical threat, in practice the attack is impractical. The volume of data and computational complexity required to perform the same are so huge, in fact, difficult to handle with current technology capabilities.

Its complexity, long key lengths, along with flexibility against computational challenges, make AES

secure by design. Continuous researches and reviews in the academic world have kept AES secure as a reliable technique for encryption. In conclusion, the resilience of AES against practical attacks guarantees its dominance and resilience as a cornerstone in the field of cryptography for the protection of data even against the most sophisticated threats that define the digital age.

Table 1. Comparison of Cloud computing's current security methodology

S.No	Characteristics / Algorithms	Developed	Blocksize (Bits)	Keylength (Bits)	Security	Speed
1.	RSA	1977	128	1024-4096	Considered secure	Very Slow
2.	ECC	1985	256	224	Considered secure	Fast
3.	DES	1997	64	56	Proven Inadequate	Very Slow
4.	Blowfish	1993	64	32-448	Considered Secure	Fast
5.	AES	2000	128, 192 or 256	128, 192 or 256	High secure	Very fast

The table above shows a comparison between various cryptographic algorithms set for use in the cloud computing platform. It gives account of algorithms such as RSA, ECC, DES, Blowfish, and AES alongside the year of development, b size, key length, security level assured as well as the processing speed. The 1977-developed RSA is secure although slow. The ECC from the year 1985 is faster with smaller key and block sizes. The DES is considered inadequate mostly because of its small key size, not to add that it is very slow. Blowfish, characterized by its design for speed and flexible key length, and AES, very safe and rapid, mark a step ahead in cryptographic techniques. The characteristics of the two algorithms are distinct, appropriate to the diverse security needs presented in cloud computing environments.

8. Conclusions

In the system of cloud data storage, users are released from the necessity to store the data locally – a task is being left to the cloud. This shift stands out underlining the paramount importance to make sure that the files in what is called data are safe, reliable, accessed when they are stored at distributed servers of the cloud. For this, the structure and securities implementation on those components of cloud data storage are necessarily to be assessed.

Client-Side Encryption: For client component, it is required to have a strong encryption mechanism using, for example, AES (advanced encryption standard). This has been proven through numerous tests and real projects deploying AES. In the United States alone, AES is widely used for encryption of sensitive information in a wide range of applications supported by US government investigations and endorsements by National Institute of Standards and Technology (NIST). Furthermore, cutting-edge encryption algorithms with genetic algorithms or other dynamic encryption techniques can even further increase the security of the system. Such advanced algorithms support innovative changes in the encryption process itself, increasing its adaptability and resistance to new forms of attacks.

Server-Side Security: The server-side component offering a huge storage and hosting our data creates unique demands in regard to security. The server-side infrastructure has to offer solid security measures securing the integrity and availability of the data. A good number of such providers use information encryption control mechanisms like symmetric encryption to ensure information confidentiality. Comparing security policies of renowned data storage service providers discern best practices and effective security strategies used by the providers. The third important factor of

consideration for cloud service providers is enhancing server security. High security of the server and assurance of accountability will easily affect user's decision for preferred cloud service provider. Thus the providers who ensure secure environment at the server will leave proper marked in the user's minds and become very competitive.

Security of the Communication Channel: The communication over a communication channel from cloud service providers to cloud users depicts an important link in data storage and transmission. This is one of the utmost insecure sections in the entire process through which third parties may easily obtain unauthorized access to user data and information. This channel can only be safeguarded if advanced techniques are put in place that aims at curbing unauthorized intrusions and vulnerabilities. This, therefore, means that the upgrade of internet protocols is a new initiative that must incorporate the contemporary computer science techniques and technologies. It's also important to note that more secure channels of communication will be established as well as data recovery protocols. This may involve the use of encrypted communication protocols, secure socket layers (SSL) and periodic updates to make it compliant with the latest security norms.

Cloud data storage systems rest on the security and integrity multiple aspects that comprise client-side encryption, server-side security as well as firm communication channels. Through the application of advanced encryption systems, strengthening server security protocols, as well as communication channels, cloud service providers can maintain a secure and reliable environment for data storage. This comprehensive security framework is important in causing the trust amongst the users build and to be maintained not by hampering the growth of cloud computing services.

References

[1] Md. Afroz, Birendra Goswami., "Energy-Efficient Green Technology Cloud Computing", Proceedings of 2nd International E-Conference in Emerging Trends in Computer Science, Govt. Vijay BhushanSinghDeo Girls PG College Jashpur Nagar, Jashpur Chhattisgarh, India: pp. 225–228, 2022.

[2] F. Soleimanian, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,Vol. 1, ISSUE 6, pp. 49-54, 2012.

[3] M.Monsef, N.Gidado, "Trust and privacy concern in the Cloud", 2011 European Cup, IT Security forthe Next Generation, pp. 1-15, 2011.

[4] D Zissis, D Lekkas, "Addressing cloud computing security issues, Future Generation ComputerSystems", Elsevier B.V, Vol.28, pp.583-592, 2010.

[5] Tsai W, Jin Z, Bai X.,"Internetware computing: issues and perspective." Proceedings of the first Asia-Pacific symposium on Internetware. Beijing,China: ACM, pp. 1–10, 2009.

[6] Raj H, Nathuji R, Singh A, England P. "Resource management for isolation enhanced cloudservices.", Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois,USA, pp. 77–84, 2009.

[7] S Subashini, V Kavitha, "A survey on security issues in service delivery models of cloud computing",Network and Computer Applications, Elsevier, Vol. 34, pp. 1-11, 2010.

[8] KapilSachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis,University of Texas, Austin, 2011.

[9] Mahbub Ahmed, Yang Xiang, Shawkat Ali, "Above the Trust and Security in Cloud Computing: ANotion towards Innovation", 2010 IEEE/IFIP International Conference on Embedded and UbiquitousComputing, pp.723-730, 2010.

[10] V.KRISHNA REDDY, Dr. L.S.S.REDDY, "Security Architecture of Cloud Computing",International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9, pp.7149-7155,2011.

[11] Siani Pearson, "Privacy, Security and Trust in Cloud Computing", HP Laboratories, appeared as abook chapter by Springer, UK, 2012.

[12] Fariborzfarahmand, "Risk Perception and Trust in Cloud", ISACA JOURNAL VOLUME 4, pp.1-8,2010.

[13] Weiss, A.; "Computing in the Clouds," netWorker, vol. 11, issue 4, p.16-25, 2007.
[14] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of The Cloud Computing SecurityProblem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.
[15] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Manage-ment in Cloud Computing – ASurvey, Inter Networks Research Group, University Utara Malaysia, Technical ReportUUM/CAS/InterNetWorks/TR2011-01, 2011.
[16] T. Mather, S. kumaraswamy, S. Latif, Cloud Security and privacy: an Enterprise perspective onRisk and Compliance, Governance An International Journal Of Policy And Administration,O'Reilly Media, Inc., p. 312, 2009.
[17] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journalof Engineering Science and Technology, Vol. 3, No. 4, p. 2672-2676, 2011.
[18] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal ofComputer Science & Emerging Technologies, Vol-2 No 5 October, 2011.
[19] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures,Interdisciplinary journal of con-temporary research in business, Vol.3, No 9, p. 1323-1329, 2012.
[20] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, TechnicalEditorBillMeine, Elsevier Publishing, 2011.
[21] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis,University of Texas, Austin, 2011.
[22] J. Hurwitz, R. Bloor, M. Kaufman, F. Halper, Cloud computing for dummies, Wiley, 2009.[23] Z. A.Khalifehlou, F. S. Gharehchopogh, "Security Directions in cloud Computing Environments", 5thInternational Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara,Turkey, pp. 327-330, 17-19, 2012.
[23] B. Shwetha Bindu, B. Yadaiah, "Secure Data Storage In Cloud Computing", International Journal ofResearch in Computer Science, Vol 1 Issue 1, pp. 63-73, 2011.
[24] Abbas Amini, Secure Storage in Cloud Computing, Master Thesis, Technical University of Denmark,Kongens Lyngby, Denmark, 2012.International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013
[25] D. Kanchana, Dr. S. Dhandapani, "A Novel Method for Storage Security in Cloud Computing",International Journal of Engineering Science and Innovative Technology (IJESIT), Vo 2, Issue 2, pp.243-249, 2013.
[26] Nikos Virvilis, Stelios Dritsas, Dimitris Gritzalis, "Secure Cloud Storage: Available Infrastructuresand Architectures Review and Evaluation", TrustBus'11 Proceedings of the8th internationalconference on Trust, privacy and security in digital business, Springer-Verlag Berlin, Heidelberg©2011, 2011.
[27] Ravi Gharshi, Suresha, "Enhancing Security in Cloud Storage using ECC Algorithm", InternationalJournal of Science and Research (IJSR), Vol 2, Issue 7, 2013.
[28] Dan Boneh, Twenty Years of Attacks on the RSA Cryptosystem, Notices of the AmericanMathematical Society (AMS), Vol. 46, No. 2, pp. 203-213, 1999.
[29] Charles P. Pfleeger, Security in Computing, Fourth Edition, Pfleeger Consulting Group, ShariLawrence Pfleeger - RAND Corporation, Prentice Hall, 2006.
[30] NIST.gov - Computer Security Division - Computer Security Resource Center, Block Cipher Modes,http://csrc.nist.gov/groups/ST/toolkit/BCM/index.html [accessed: July 2013].
[31] IAIK - TU Graz : AES Lounge, http://www.iaik.tugraz.at/content/research/krypto/aes/#security [accessed: 9 August 2013].
[32] Alex Biryukov and Dmitry Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, University of Luxembourg, ePrint Archive: Report 2009/317
[33] Satoh, A., Morioka, S. (2003). Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES. In: Boyd, C., Mao, W. (eds) Information Security. ISC 2003. Lecture Notes in Computer Science, vol 2851. Springer, Berlin, Heidelberg. https://doi.org/10.1007/10958513_20
[34] T. Schreiber, "Session Riding a Widespread Vulnerability in Today's Web Applications" [Online], Available: http://www.securenet.de/papers/Session_Riding.pdf, white paper, 2004.
[35] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, no. 2, pp. 50-57, 2011. [11] A., Greenberg,