Survey on Security and Privacy of Cloud Computing Paradigm: Challenges and Mitigation Methods

Akhtar Hussain
akhtar.hussain@und.edu

Jun Liu
jun.liu@und.edu

Eunjin Kim
eunjin.kim@und.edu

School of Electrical Engineering and Computer Science
College of Engineering and Mines
University of North Dakota
Grand Forks, 58202

Abstract

The success of the Internet has significantly increased the volume of users and data. This has also raised the new requirements for accessing computational resources anywhere and at any time. Traditional computing infrastructure is difficult to meet the new requirements due to inflexible configurations and expensive maintenance and operations. Cloud computing provides a new paradigm of providing a large variety of computing services to large groups of users anywhere and at any time. While cloud computing emerged as a computing model that brought great deals of beneficial services, at the same time, it raised the possibility of risks. The most significant issues that this magnificent phenomenon faces are privacy and security that lead to illegal access of data, data leakage, the disclosure of confidential information, and privacy exposure. In this paper we will systematically assess and review the cloud security and privacy issues and their solution as well as present the systematic model of cloud computing and various types of security threats to this paradigm. Furthermore, this work will also discuss and analyze the data security and privacy protection for cloud storage. Moreover, our paper summarizes several new cryptographic technologies for security protection in cloud-computing paradigm, which include Attribute-Based Encryption (ABE), Homomorphic Encryption (HE), and Searchable Encryption (SE). Our paper also summarizes the open problems and future directions of security protection in cloud computing.

Keyword: Cloud Computing, Cloud actors, Security and Privacy, Encryption, Confidentiality, Security attacks and threats,

1. Overview of the system model of Cloud Computing

In the recent years, advancement in computing architecture and data processing mechanism has totally changed the computing paradigm. Due to this advancement, cloud computing system has turned out to be a necessity for external data storage and resource management. The success of global Internet has drastically increased the volume of users and new requirements for accessing computational resources anywhere and at any time. Traditional computing infrastructure is difficult to meet the new requirements due to inflexible configurations and expensive maintenance and operations. Cloud computing delivers data storage, processing power, databases, networking, and a large variety of software applications over the Internet with flexibility and reliability at much reduced costs. Cloud computing provides numerous advantages to both individuals and companies, particularly in terms of reducing capital expenses and cutting operational costs. By outsourcing on-premises computing resources to cloud service providers which provide quality guarantee on maintaining the operations of computing resources, users can be relieved from paying high procurement and maintenance costs and keeping a team of qualified IT professionals [1][2][26]. The procedure Pay-as-You-Go (PAYG) model gives the ability and flexibility to customize the computing resources, application, data storage, development platform as per the need of client [3]. The main aspects of cloud computing are manageability, scalability, and availability [1]. According to National Institute of Standards and Technology (NIST) [4], cloud computing is defined as a model for facilitating convenient, pervasive, on-demand network access to a shared pool of configurable computing resources (e.g., networks, services, applications, storage, and servers) that can be accessed and released efficiently with least managerial effort and with no interaction of service provider. This model consists of five characteristics, three service models, and four deployment models as summarized in Table 1.

Cloud computing model		
Service Models	Deployment Models	Essential characteristics
1. Software as a Service (SaaS) 2. Platform as a Service (PaaS). 3. Infrastructure as a Service (IaaS)	1. Private cloud 2. Community cloud 3. Public cloud 4. Hybrid cloud	1. On-demand self-service 2. Broad network access. 3. Resource pooling 4. Rapid elasticity 5. Measured service

Table 1 Cloud Computing Model

This paper is to discuss the cloud and security issues in cloud computing paradigm, for better understanding of security issues, it is necessary to understand the cloud computing service models first. Cloud service model is crucial because it lays down the foundation for comprehending the various responsibilities and risks connected to each service model. Different cloud service models give the cloud customer and the cloud provider distinct degrees of control and responsibility. Customers using the cloud can typically operate a variety of operating systems and applications in their virtual machines. Due to their possible size and complexity, the operating systems and applications used by cloud users may have security flaws[31]. Understanding these service models helps in identifying the different security concerns that arise and the corresponding measures that need to be taken. Identifying cloud security without explaining the cloud service model can therefore result in misunderstandings, poor communication, and insufficient security measures.

1.1 Cloud Computing Service Models

As per NIST [4] The basic service delivery models provided by cloud computing are software-as-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS). Depending on the IT requirements and budget of a company, each of the three models have a specific purpose. IaaS is most flexible of the three models. It gives complete control over a company's infrastructure. It is scalable and easily customizable. Computing capabilities, vital storage as standardized services is provided by IaaS. The main example of IaaS are Amazon Web services, Microsoft Azure, and Google Compute Engine (GCE). PaaS provides a layer of environment in which customers can develop their own application without installation underlaying development framework. PaaS also ensures the data protection using encrypting techniques while storing data on third party platform. AWS Elastic Beanstalk, Google App Engine, and Adobe Commerce, LAMP platform (Linux, Apache, MySQL, and PHP) are some examples of PaaS. Policy control management, access to application software and database are provided by SaaS. SaaS provides the ability for single service, that is available on the cloud, to be easily accessed by multiple users. SaaS services are provided by companies like Google, Microsoft Office 365, Dropbox etc.

1.2 Actors and their Roles in cloud computing

Five major actors with their functions and duties using the newly developed Cloud Computing Taxonomy are explained by NIST Cloud Computing Reference Architecture [5]. These contributing actors are explained below.

a) Cloud Consumer A principal stakeholder or group for cloud computing services that maintains to do business with cloud providers and makes use of their services. Activities and usage scenarios may differ from one another based on the services they require. A few examples of cloud services that a cloud user can choose from are shown in Figure1 [5].

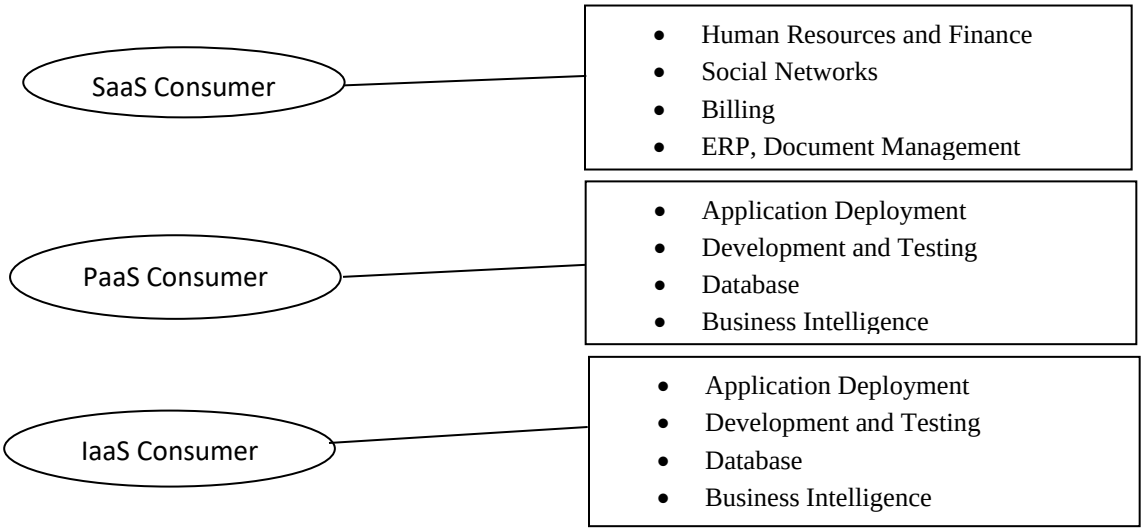

Figure1: Example Services Available to a Cloud Consumer

b) Cloud Provider A cloud provider could be an entity, person, or company that is liable for making services available to interested parties and provides the computing infrastructure necessary for offering the services that run the cloud software. The activities conducted by cloud provider are described in five major areas as shown in Figure 2 [5].

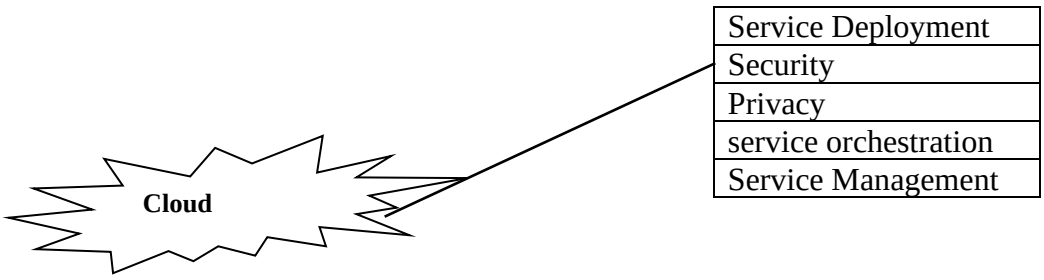

Figure 2: Major Activities of Cloud Provider

c) **Cloud Broker** A cloud broker is an individual that controls the use, execution, and distribution of cloud services and collaborates associations between cloud providers and cloud consumers. Instead of communicating directly to the cloud provider, a cloud consumer requests the services from a cloud broker. The services provided by a cloud broker are separated into three categories below.
   - Service Intermediation: The cloud broker upgrades the service by improving some specific capabilities like performance reporting, enhanced security, identifying management, and offering value-added services to cloud consumers.
   - Service Aggregation: Multiple services are combined and integrated to get new services. A cloud broker combines and integrates multiple services into one or more new services. Some other responsibilities of a cloud broker are to keep data movements secure and offering data integration.
   - Service Arbitrage: Due to this, the cloud broker attains the flexibility to select services from multiple sources.

d) **Cloud Auditor** An independent entity which does evaluation of cloud services, its operation, and security of cloud execution. Interaction between a cloud provider and a cloud consumer may be involved by such assessment. Such audits assure the confidentiality, integrity, and availability of an individual's personal information at every step of creation and operation. This may assist Federal agencies complying with applicable privacy laws and regulations [6].

e) **Cloud Carrier** A cloud carrier behaves as an intermediary that offers connectivity and transfers cloud services between cloud consumers and cloud providers. Cloud providers participate in a way to have two service-level agreements: one with the cloud carrier and one with the cloud consumer. To ensure that the cloud services are used at a consistent level in accordance with the contractual responsibilities of the cloud consumers, a cloud provider negotiates service level agreements (SLAs) with a cloud carrier and may ask for resolved and encrypted connections.

2. Security Concerns in Cloud Computing

Cloud computing is an increasingly popular model for delivering and accessing IT resources over the internet, but at the same time, it also evolves security threats and attacks. Any possible risk to a computer system that could result in significant harm is referred to as a threat in the context of computer security. These threats lead to attacks. All the information and data must transfer through the network and be stored on the cloud, and malicious actors always try to manipulate different liabilities. Hardware and software components of cloud computing face serious threats like viruses, trojans, and inside and outside hackers that can lead to attacks on the whole cloud system [1]. Existing security solutions are not sufficient to secure the cloud infrastructure. In this section, major cloud computing attacks and threats will be explored. Some of the most common security attacks and threats in cloud computing are Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, or STRIDE for short, is a set of criteria

developed in 1999 by Loren Kohnfelder and Praerit Garg to help companies spot potential weaknesses and threats to their products [9]. Each STRIDE class captures individual characteristics of attacks that represent a specific sort of threat [1]. Recent studies describe the current challenges and provide a useful roadmap for current cloud security. This research indicates that threats and related risks are becoming more prevalent. Below is a summary of the threats that this research highlights. While cloud computing emerged as a computing model that brought great deals of beneficial services, at the same time this valuable phenomenon suffers from both inside and outside attacks. Given that cloud computing is becoming more widespread, security attacks are apparent. Based on the Open Web Application Security Project (OWASP), attacks on the cloud [12] are classified in top-down mode.

2.1 Taxonomy of security threats targeting cloud computing

The use of cloud computing has become an imperative part of modern technology due to its advantages, such as its flexibility, scalability, and cost-effectiveness. Nevertheless, the transfer of sensitive data and applications to the cloud by numerous organizations also brings about security concerns. The potential sources of threats to cloud security are diverse and can originate from cybercriminals, insiders, or external causes. Threat taxonomy is essential to complete to deal with these security problems. This procedure involves locating, classifying, and ranking potential threats that might have an impact on the cloud environment. Threat classification allows organizations to prioritize their security efforts and distribute resources in accordance with the need to mitigate and prevent each type of threat. Common categories of cloud computing threats are related to network threats, user related security threats, software application threats and most importantly data related threats [32][1].

2.1.1 Network related Security Threats

Parallel to hardware and software applications, networks play a big role in cloud computing. Due to the difficulty of achieving end-to-end protection, cloud networks present a greater security challenge than conventional IT networks within organizational perimeter limits. The availability of the cloud may be impacted by an assault on the cloud network that reduces or intercepts network bandwidths. Customers who heavily rely on cloud services for their day-to-day company operations may experience widespread disadvantages as a result of the negative effect on cloud availability. For example, in the past GitHub was targeted by a DoS attack, causing widespread service outages. Cloud computing's network infrastructure is vulnerable to various attacks such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), and eavesdropping. DDoS attacks can cripple cloud services by overwhelming the network infrastructure with an enormous volume of traffic Significant threats to connection availability have been observed in network security, including denial of service (DoS), distributed denial of service (DDoS), flooding attacks, and Internet protocol weaknesses. The risk come from external users trying to launch a DoS assault on the network of the cloud service provider with the intention of blocking access to corporate and individual users' computer resources. Network administrators must therefore implement suitable security rules and make use of preventative tools and services to safeguard data and cloud infrastructure. Using firewalls is one of the most popular and efficient ways to stop these threats. There are external and internal network security threats, user related threats that can be performed on physical or virtual networks. Sensitive data is obtained from the businesses, processed by the SaaS application, and then stored at the SaaS vendor end in a SaaS deployment paradigm. To stop the leakage of sensitive data over the network, all data movement must be secured. To ensure

security, this calls for the use of powerful network traffic encryption methods like Secure Socket Layer (SSL) and Transport Layer Security (TLS) [19][20][27][33][43].

- **Abuse of Functionality**
  To congest a network link or make cloud system to fail, attackers perform excessive malicious activities. For example, a denial-of-service attack that locks out genuine users by flooding a login system of web with legitimate usernames and random passwords [13]. The consequences of such attack are consuming resources, unauthorized access control and leakage of confidential information. Similarly, MitM attacks intercept data between the cloud provider and the user, making it possible for the attacker to access sensitive information. Eavesdropping, on the other hand, involves monitoring data traffic on the cloud network. Attackers can use this technique to steal sensitive information and exploit it for malicious purposes.
- **Spoofing attacks**
  A spoofing attack is a compilation of incidents in the field of cloud security, where a person or program efficiently mimics another to obtain an unethical advantage. The example of such attacks is DNS spoofing, IP spoofing, phishing, spoofing metadata by imitating a reliable email sender [18].

2.1.2 User related Security Threats

Security measures that cloud providers takes to safeguard the data of their consumers is stated as user centric security. That involves implementing security measures that are developed according to requirements and predilections of users, access control and encryption techniques. This includes implementing access controls, encryption, and other security measures that are tailored to the needs and preferences of individual users. Cloud computing providers can increase consumer confidence and guarantee the secure processing and storage of their clients' sensitive data by giving priority to user security. Malicious Insider, identity theft and unauthorized activities could be user related security threats and they accomplished by account hijacking and it is normally done by the stolen credentials by which the confidentiality, integrity, and availability of critical part of cloud services are compromised. Muti-factor authentication and data security platform such as end-to-end encryption can be used to avoid such hijacking threat. Authorization, authentication, and Identity and access management issues are main attributes of user-oriented security. These three attributes are explained below [34-38].

- **Authorization** The process by which a system decides what degree of access a specific authenticated user should have to secured resources under its control is known as authorization. To ensure that only authorized parties can interact with data in a cloud setting due to the increased number of entities and access points, authorization is essential to get access to databases, resources, and information systems and it is based on the responsibilities and permissions of the user. Various authorization control mechanisms are provided. These control models are DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role based access control), and ABAC (Attribute Based Access Control). These controls have advantages as well disadvantages.
- **Authentication** Determining a person's endorsement to conduct an action on data, such as reading or writing, is the act of doing so. Before engaging in the action, they are authorized to, users must authenticate. The cloud service provider presents and implements access control policies through the cloud environment, such as the services and resources should only be accessed by the authorized users . Authentication has two methods; they are physical security

mechanism and digital security mechanisms. Physical security mechanism includes retina recognition, face recognition and fingerprint recognition. Whereas digital security mechanism is simple credential like (username, passwords), Multifactor authentication and single sign-on (SSO).

- **Identification and Access Management** According to an IBM security framework for a typical company, identity and access management is one of the key security controls that should guide the organization's security policy. It should ensure that only legitimate users should be permitted entry to the corporate data that may be present across applications. Administrative, discovery, maintenance, policy enforcement, management, information sharing, and authentication tasks can all be handled by Identity and access Management. Identity and Access Management (IAM) validates the use of a single identity that is managed across all apps while also ensuring security. It is used to give or restrict access to data and other system resources as well as to authenticate users, devices, or services.

2.1.3 Software Application related Security

Software application is one the most vital component of cloud computing. Its significant importance makes application security as one of the most vulnerable areas of information security [1]. Software security is a major and crucial issue when creating a cloud system. It has numerous security flaws, such as implementation errors, buffer overflows, flaws in the way it was built, broken error handling promises, and more [7]. Many application developers today use programming languages with built-in classes and methods that have a variety of security flaws. like HTML/CSS/PHP/JS to mitigate injection masked code. Similarly, backend application's weaknesses are abused by SQL injection. To prevent such concerns and tackle application related security challenges there is need to train and make it to necessary for developers to concentrate on some areas like encryption identity management services, authentication services, and identity and access management services [21].

- **Hacked interface and application program interfaces** other threat which compromised security of cloud is called Hacked interface and application program interfaces. As the API is main entrance point for cloud customer and it help to hack the interface. Regular software patch update could only prevent from such attack [1].
- **Elevation of Privilege** In such threat a user exploits a buffer overflow to take control of the cloud system at the core level. An attacker who can breach all system defenses and enter the trusted system itself. The attackers get the elevated access privileges to secured resources. This is done by manipulating configuration fault in any application, design defect, bug, or system trickle [11][7]. With proper quality assurance check on implanted security techniques before deployment of cloud system could avoid such threat.
- **Buffer Overflow attack** Buffer overflows are a frequent occurrence in today's cloud systems, and vulnerability is created when memory close to a buffer is overwritten, which shouldn't be done either on purpose or carelessly in a program. Such attacks usually target to eliminate memory, which includes elements like the stack that hold local variables like those used as arguments and parameters inside of methods. Buffer overflow attacks should be avoided by risk managers by eliminating and distinguishing them before the software system is employed in cloud computing system [14].
- **Embed malicious code attack** One type of web-based assault is called a malware injection attack, in which attackers take lead of shortcomings in a cloud-based web application

by embedding malicious code that modifies the way the application typically runs. The malicious code may visibly undermine the application's security. It is always feasible for a developer to add malicious code with the goal of compromising an application's security, either now or in the future. Target cloud service models SaaS, PaaS, and IaaS are each infected with a malicious application, program, and virtual computer by hackers [15].

- **Malware injection attacks** SQL injection and cross-site scripting (XXS) attacks are the two main categories of malware injection attacks that are most repeatedly used to manipulate online application exposures in cloud computing. The most frequent assault for obtaining data from user cookies is cross-site scripting, which can result in a security issue. The primary target of SQL injection attacks is SQL servers hosting weak database apps. Generally, this attack launched with the help of multiple bots that are equipped with a SQL injection kit to fire a SQL injection attack and if the attacker launches it successfully then attacker can remotely retrieve sensitive data, manipulate the content of the database, and by executing the system commands take the control of the web server [16].

2.1.4 Data related Security threats

Cloud computing has transformed the way businesses store, process, and access data. However, it has also brought along new security challenges. One of the biggest concerns is the risk of data-related security threats. Malicious actors may try to exploit susceptibilities in the cloud infrastructure or steal login credentials to gain illegal access to data. In addition, cloud providers may face insider threats from employees who have access to confidential information. To mitigate these risks, businesses need to implement strong security measures such as encryption, access control, and regular monitoring and auditing of their cloud environments. It is also crucial to choose a trustworthy and dependable cloud service provider that follows best procedures for data security. Since cloud computing requires the storage and processing of sensitive information in remote servers, it can be susceptible to attacks such as data breaches, theft, loss, and reputational loss and disclosure of customer data.

- **Data Breaches** First important threat which is one of the critical for cloud customer is data breaches. In that threat personal critical information like credit card number, social security number etc. could be sneaked, viewed, or released to unauthorized users. A data spill or data leak is another name for a data breach. From a security perspective, data leakage has emerged as one of the biggest organizational dangers. Data breaches can be avoided by apply basic security measures like administering susceptibility, penetration testing and by applying strong protection against malwares in addition to strong password implementation. Sometime encryption technique could also prevent the data from thread actors [1][28].
- **Data Manipulation** Another issue that can occur when moving data to and from the cloud is data manipulation. This requires data insertion, alteration, and data removal. This compromises the availability, integrity, auditability of security. This type of threat can be managed by the simple methodology is to encrypt and/or sign all data that is being transferred backward and forward [7][10]. A provider may keep extra copies of the data fraudulently to sell them to interested third parties. The data leakage impacts the web application and attacker take off benefit of configured permission in cloud operations [7]. Man-In-The-Middle Cryptographic Attacks, Brute Force Attacks, Dictionary Attack imply to as probabilistic-based attacks which consider the possibility that attack would be successful. The attackers used different statistical and analytical tools to exploit the weak cryptographic cloud system [17].

- **Reputational loss and disclosure of customer data** Reputational loss and disclosure of customer data are Significant risks to customer and provider that are caused by a threat called Distributed denial-of-service attacks (DDoS). Source such threats are large number of internet bots which attach the cloud platform altogether and make the denial-of-service situation. Such threats could be avoided by deploying proper denial of-service response plan and proper management plan. The major cause of such threat happens when proper log mechanism for user's action on application or system is not implemented properly. So, it creates a chance that a person will commit a crime in a system that cannot track them. These threat compromises the Auditability, Trust Privacy, Cryptography [1][7]. Proper log tracking system can avoid this threat.

3. Overview of data security and privacy issues in cloud storage system

This study seeks to address the issues covering the security and privacy of cloud storage after reviewing the basic framework of cloud computing and the typical security risks associated with it in earlier sections. Cloud storage systems pose a number of data security and privacy concerns that must be resolved in order to maintain the protection of confidential data. Organization and users of cloud storage take the data security as important concern. Data access through a storage application for cloud computing must be highly available, while high speed and maximum scalability must also be maintained. Users moved to cloud data storage due to huge pool of shared resources provided by it. Due to the nature of cloud storage, problems with data security and privacy are unavoidably created during this process. Data storage provided by cloud storage providers offer this service with a guarantee of security Confidentiality, integrity, and Availability [8][25]. Cloud storage systems highlight a number of data security and privacy concerns that must be resolved in order to maintain the protection of private data. Data storage and its security becomes a most prominent issue after the active migration of government's departments, enterprises, and individual users. The protection of data from unauthorized modification, addition, or deletion in information system is critical [1]. The assurance integrity, confidentiality and availability of data can be achieved by ACID property. Atomicity, consistency, isolation, and durability are all abbreviated as ACID. The primarily challenges to maintaining data security and anonymity in cloud storage systems are as follows [22]:

- **Security Provider** Many customers are afraid about how effortlessly hackers and criminals can get into distant data. Cloud service providers pay special consideration to this challenge and devote a lot of resources to confront it.
- **Privacy Preserving** Virtual computing is utilized in cloud computing an data is spread over multiple virtual centers, due to that various legal systems will have differences over data privacy protection
- **Rights of Ownership** After data is transported to the cloud, some people are worried that they will lose their rights or won't be able to sustain the rights of their clients. Such issue could be resolved by well-experienced user-sided contracts.
- **Data Mobility** Data transportability is very high with cloud computing. Customers may not always be informed of where their data is situated.
- **Multiplatform Support** How the cloud-based service incorporates across numerous platforms and operating systems, such as Linux, Windows, OS X, and thin clients, is more of a problem for IT teams using managed services. The need for multiplatform assistance will decrease as more user interfaces move around to the web.

- **Recovery of Data** Cloud storage systems rely on complex infrastructure and may suffer from hardware or software failures, leading to data loss. Data should be backed up so it can be retrieved in the future to prevent this. Users of the cloud can maintain an offline backup of crucial data.
- **Data Portability and Transition** Some cloud users be concerned that if they shift service providers, their data may be difficult to transfer. Data conversion and porting rely heavily on the type of data retrieval format used by the cloud provider, especially when that format is incomprehensible.

3.1 Data encryption technologies and data protection method

Massive data generation and outsourcing of data to the cloud make the data insecure. An effective technique is used to protect the data is called encryption. That encode the data into other form by using some cipher algorithms. Three main aspects of cloud storage challenges are confidentiality, integrity, and availability. Data confidentiality refers to preventing active attacks on users' data by unauthorized parties. The data receiver complies exactly with the information transmitted by the sender. The reliability of the data is known as data integrity i.e., the data cannot be altered at choice. The term "data availability" highlights the ease with which users can access, download, or modify data at any time as soon as they require it, the cloud. Other than these other requirements of data security are Fine- Grained Access Control, Secure Data Sharing in Dynamic Group, Leaking Resistant, Completely Data Deletion.

At this point, encryption is still the primary remedy for cloud computing's problems with data security. The part that follows introduces some encryption technologies that are frequently used in cloud storage systems [23][29][30].

3.1.1 Identity-Based Encryption

Identity-Based Encryption (IBE) public-key cryptographic method that empowers users to encrypt and decrypt data using an identifier as the public key, such as an email address or a username. In traditional public-key cryptography, users must obtain a public key certificate from a trusted third party or certificate authority (CA) before they can use public-key encryption. However, with IBE, a user's identity can act as their public key, eradicating the need for a CA and making easier the key management process. In an IBE system, a trusted entity called the Private Key Generator (PKG) generates a master secret key and public parameters. The PKG uses the master secret key to generate private keys for each user in the system based on their identity. To encrypt a message for a user, the sender obtains the user's public parameters, which are typically available in a public directory, and uses them to encrypt the message. The recipient can then use their private key, which is derived from their identity and the public parameters, to decrypt the message. It also enables more flexible access control and allows for fine-grained encryption based on the identity of the user. However, IBE also has some security risks, such as the possibility of a PKG compromising the system by generating private keys for unauthorized users. Therefore, careful consideration of the security risks and appropriate safeguards should be taken when implementing an IBE system.

In conventional Public Key Infrastructure (PKI) process there is weakness that enhanced the workload of sender when it shares its data with multiple receivers. To resolve this shortcoming the concept of IBE was introduced. The concept is to link the user's identity. The basic idea of IBE is illustrated in scenario, When Alice sends an email to Bob at b@ho.com, she simply encrypts her communication using the public key string "b@ho.com". Alice does not need to obtain Bob's public key certificate. After receiving the encrypted message, Bob contacts a third-party Private Key Generator (PKG) and authenticates himself to it in the same way as he would to a Certificate

Authority (CA). The PKG generates Bob's private key, allowing him to decrypt and read the email. Notably, Alice can transmit encrypted email to Bob even if he has not yet configured his public key certificate, unlike the current secure email infrastructure. [24][2][39].

3.1.2 Attribute-Based Encryption

Attribute-Based Encryption (ABE) is enhanced version that replaces the identity of IBE with the set of attributes. ABE is based on user attributes; it is a form of public key encryption that enables users to encrypt and decrypt messages or data. ABE is a type of encryption method that grants access to encrypted data based on certain attributes or criteria rather than using traditional cryptographic keys. In ABE, data is encrypted by means of a set of attributes or policies that are defined by the owner of the data, rather than using a single key. ABE is a valuable tool for securing data in circumstances where traditional encryption methods may not be practical. For example, in a cloud computing environment, users may need access to data from multiple locations, and traditional encryption keys may not be sufficient for granting access to the data. With ABE, access to the data can be granted based on specific policies or attributes, making it easier to manage access control in complex environments. ABE works in four steps namely setup, key Generation, Encryption, Decryption phase. Firstly, relevant security parameters are entered, and the associated master key (MK) and public parameters (PK) are generated. The second step involves the data owner providing the system with their own attributes to acquire the private key related to those attributes. In the third stage, the data owner encrypts the data using his or her public key to produce the ciphertext (CT), which is then sent to the recipient or to a public cloud. Users of decryption finally receive ciphertext and can decrypt it using their own secret key. The data owner can designate who can access the encrypted data due to ABE's claim to offer fine-grained access control over encrypted files in data-sharing tools. Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are the two major classes [2][38][40].

- **Key-Policy ABE (KP-ABE)**
  In KP-ABE, data is encrypted using a set of attributes or policies, and access to the data is conferred to a user who has a private key that matches the specified attributes or policies. This type of ABE is typically used for securing data in cloud environments or for data sharing applications.
- Ciphertext-Policy **Attribute-Based Encryption (CP-ABE)**
- In CP-ABE, data is encrypted using a set of attributes, and access to the data is granted to a user who has a set of attributes that match the attributes used to encrypt the data. This type of ABE is typically used for securing data in IoT applications or for securing communications between devices.

3.1.3 Homomorphic Encryption

Homomorphic Encryption was designed to overcome the concerns raised by IBE and ABE. Homomorphic encryption is a type of encryption that enables particular computations on ciphertexts to generate an encrypted result that, when decrypted, is indistinguishable to the outcome of operations carried out on the plaintexts. It effectively protects the security of data that is sent. The file is homomorphically encrypted by the data owner and sent to the cloud server. With the appropriate private keys, the authorized users can decrypt the ciphertext. Receiver simply needs to submit the functions that correspond to the operations to the cloud server if he wishes to perform certain operations on the ciphertext. This means that the data remains encrypted while computations are being performed, providing a high level of privacy and security. The security of

data that is outsourced is adequately protected by homomorphic encryption. Homomorphic encryption could be enormously beneficial in circumstances where data confidentiality is crucial, for instance, in domains such as finance, healthcare, or government. On the other hand, the adoption of homomorphic encryption is confined by its high computational complexity and limited capabilities when compared to conventional encryption methods. However, ongoing research aims to enhance the efficiency and functionality of homomorphic encryption methods. There are three main types of homomorphic encryption [2][41].

- **Fully Homomorphic Encryption (FHE)**
  FHE is the most effective form of homomorphic encryption, which grants arbitrary calculations to be performed on ciphertext, including addition and multiplication.
- **Partially Homomorphic Encryption (PHE)**
  PHE grants only one type of computation to be performed on the ciphertext, either addition or multiplication.
- **Somewhat Homomorphic Encryption (SHE)**
  SHE is a settlement between FHE and PHE, allowing a limited number of calculations to be performed on the ciphertext.

3.1.4 Searchable Encryption

Normally data is uploaded on the cloud in encrypted form. To search the encrypted data over the cloud searchable encryption technique is used. SE (Searchable Encryption) is a good method for protecting users' confidential details while retaining server-side search functionality. The server can scan encrypted data using SE without disclosing any plaintext data. SE requires the encryption of the data and the formation of a searchable index over the encrypted data. There are several types of SE techniques, such as Symmetric Searchable Encryption (SSE), Public-key Searchable Encryption (PEKS), and Homomorphic Encryption (HE). SSE and PEKS agree to users to operate precise matching and range queries over encrypted data, whereas HE permits for more complex procedures, such as addition and multiplication over encrypted data. In contrast to PEKS, which allows multiple users who have access to the public key to produce ciphertexts, SSE only permits private key holders to produce ciphertexts and to construct trapdoors for search [2][42].

4. Direction of Future Research on Cloud Security

The popularity of cloud computing is anticipated to increase in the coming years as it has established itself as a crucial part of contemporary computing infrastructure. Research on cloud security is required as cloud computing develops further to guarantee the privacy, accuracy, and accessibility of data and services therein. A privacy protection system should be deployed to protect the private information that is embedded in shared data, particularly data containing highly private information like government and medical records. Recent years have also seen a significant increase in the popularity of modern machine learning and deep learning, particularly for image processing, DNA sequencing, and medical diagnosis. These algorithms require the creation and development of effective and secure outsourced data protection techniques. Future studies should focus on the problem of how to handle various data types using the concepts underlying various encryption techniques. How to find structured social network data that contains encrypted media data, such as an image or video data, for instance.

To protect against insider threats, cloud computing also requires a security solution. Numerous options still work with the cloud. But the insider danger cannot be resolved with the current solutions. Future studies could concentrate on creating mechanisms to guarantee the dependability

and accountability of cloud-based services to boost trust in cloud computing. This might entail creating methods for auditing cloud-based services as well as building tools for service-level agreement enforcement. (SLAs). As cloud-based data analytics gain popularity, it is necessary to create methods for performing data analysis while protecting people's privacy. The development of data analytics algorithms that safeguard sensitive data while protecting privacy could be the main topic of future research.

There is a need for efficient intrusion detection methods in the cloud as cyber threats continue to change. Future studies might concentrate on creating real-time assault detection and response cloud-based intrusion detection systems. Deep learning methods gained popularity recently, and deep learning algorithms have made enormous advances in the fields of finance, defense, medical diagnosis, and academia. There is a need to develop techniques that can use these modern techniques while preserving the privacy of individuals, Future research could focus on developing privacy-persevering deep learning algorithms that protect sensitive data and help to identify threats and attacks in cloud computing. In addition, another important technology Blockchain could be ideal mitigation for many cloud security concerns due to its features such as immutability, accountability, efficiency, and privacy preservation. There are some research studies required that can address concerns related to malfunctioning machines, trust, accountability, compliance, integrity, and malicious insider behaviors [1][2][43].

5. Conclusion

Cloud computing provides a new paradigm of providing a large variety of computing services to large groups of users anywhere and at any time. While cloud computing emerged as computing model that brought great deals of beneficial services, however at the same time, this raises the possibility of risks. The most critical issues that this magnificent phenomenon faces are privacy and security that leads to illegal access of data, data leakage, the disclosure of confidential information, and privacy exposure. In this paper we reviewed the cloud security and privacy issues and their possible solution as well as present the systematic model of cloud computing and various types of security threats and attacks to this paradigm. Furthermore, we also discussed the data security and privacy protection for cloud storage. Moreover, and summarized several new cryptographic technologies for security protection in cloud-computing paradigm, which include Attribute-Based Encryption, Homomorphic Encryption, and Searchable Encryption. We also summarized open problems and future directions of security protection in cloud computing.

References

[1] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.
[2] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.
[3] Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.
[4] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing
[5] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500(2011), 1-28.
[6] Chief Information Officers Council, “Privacy Recommendations for Cloud Computing”, http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx

[7] Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200-222.
[8] Prajapati, P., & Shah, P. (2022). A review on secure data deduplication: Cloud storage security issue. Journal of King Saud University-Computer and Information Sciences, 34(7), 3996-4007.
[9] Shevchenko, N. (2018, December 3). Threat Modeling: 12 Available Methods. Retrieved March 1, 2023, from https://doi.org/None.
[10] Lagesse, B. (2011, March). Challenges in securing the interface between the cloud and pervasive systems. In 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops) (pp. 106-110). IEEE.
[11] Yan, G., Wen, D., Olariu, S., & Weigle, M. C. (2012). Security challenges in vehicular cloud computing. IEEE Transactions on Intelligent Transportation Systems, 14(1), 284-294.
[12] Huang, Y. W., Huang, S. K., Lin, T. P., & Tsai, C. H. (2003, May). Web application security assessment by fault injection and behavior monitoring. In Proceedings of the 12th international conference on World Wide Web (pp. 148-159).
[13] Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. Telecommunication Systems,70,447-
[14] Alzahrani, S. M. (2021). Buffer Overflow Attack and Defense Techniques. Int. J. Comput. Sci. Netw. Secur, 21, 207-212.
[15] Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3), 79.
[16] Sharma, N., Alam, M., & Singh, M. (2015). Web based XSS and SQL attacks on cloud and mitigation. Journal of Computer Science Engineering and Software Testing, 1(2), 1-10.
[17] Murugan K, Suresh P (2018) Efcient anomaly intrusion detection using hybrid probabilistic techniques in wireless ad hoc network. Int J Netw Secur 20(4):730–737
[18] Gumaei A, Sammouda R, Al-Salman AMS, Alsanad A (2019) Anti-spoofng cloud-based multispectral biometric identifcation system for enterprise security and privacy-preservation. J Parallel Distrib Comput 124:27–40
[19] Somani G, Gaur MS, Sanghi D, Conti M, Buyya R (2017) DDoS attacks in cloud computing: issues, taxonomy, and future directions. Comput Commun 107:30–48
[20] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
[21] Prokhorenko V, Choo K-KR, Ashman H (2016) Web application protection techniques: a taxonomy. J Netw Comput Appl 60:95–112
[22] Dinadayalan, P., Jegadeeswari, S., & Gnanambigai, D. (2014, February). Data security issues in cloud environment and solutions. In 2014 World Congress on Computing and Communication Technologies (pp. 88-91). IEEE.
[23] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.
[24] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings (pp. 213-229). Berlin, Heidelberg: Springer Berlin Heidelberg.
[25] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4, 1-13.
[26] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[27] Agarwal, A., & Agarwal, A. (2011). The security risks associated with cloud computing. International Journal of Computer Applications in Engineering Sciences, 1(Special Issue on), 257-259.
[28] Barona, R., & Anita, E. M. (2017, April). A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International conference on circuit, power and computing technologies (ICCPCT) (pp. 1-8). IEEE.
[29] Liu, Y., Sun, Y. L., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: solutions and future directions. Journal of Computing Science and Engineering, 9(3), 119-133.
[30] Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.
[31] Varadharajan, V., & Tupakula, U. (2014). Security as a service model for cloud environment. IEEE Transactions on network and Service management, 11(1), 60-75.
[32] Swathy Akshaya, M., & Padmavathi, G. (2019). Taxonomy of security attacks and risk assessment of cloud computing. In Advances in Big Data and Cloud Computing: Proceedings of ICBDCC18 (pp. 37-59). Springer Singapore.
[33] Xia, H., & Brustoloni, J. C. (2005, May). Hardening web browsers against man-in-the-middle and eavesdropping attacks. In Proceedings of the 14th international conference on World Wide Web (pp. 489-498).
[34] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.
[35] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.
[36] Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.
[37]https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-policygovernance-risk-compliance/
[38] Dubey, S., & Rai, P. K. (2021). A Review of Cloud Service Security with Various Access Control Methods.
[39] Anand, D., Khemchandani, V., & Sharma, R. K. (2013, September). Identity-based cryptography techniques and applications (a review). In 2013 5th international conference and computational intelligence and communication networks (pp. 343-348). IEEE.
[40] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98).
[41] Yi, X., Paulet, R., Bertino, E., Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption (pp. 27-46). Springer International Publishing.
[42] Wang, Y., Wang, J., & Chen, X. (2016). Secure searchable encryption: a survey. Journal of communications and information networks, 1, 52-65.
[43] Akello, P., Beebe, N. L., & Choo, K. K. R. (2022). A literature survey of security issues in Cloud, Fog, and Edge IT infrastructure. Electronic Commerce Research, 1-35.