Privacy-Preserving Cloud Computing: Ecosystem, Life Cycle, Layered Architecture and Future Roadmap

Saeed Ahmadi *
*School of Computer Science, University of Guelph, Ontario, Canada
sahmad18@uoguelph.ca

Maliheh Salehfar†
†School of Management and Accounting
Allameh Tabataba’i University, Tehran, Iran
malihehsalehfar@gmail.com

Abstract—Privacy-Preserving Cloud Computing is an emerging technology with many applications in various fields. Cloud computing is important because it allows for scalability, adaptability, and improved security. Likewise, privacy in cloud computing is important because it ensures that the integrity of data stored on the cloud maintains intact. This survey paper on privacy-preserving cloud computing can help pave the way for future research in related areas. This paper helps to identify existing trends by establishing a layered architecture along with a life cycle and an ecosystem for privacy-preserving cloud systems in addition to identifying the existing trends in research on this area.

Index Terms—Cloud Computing, Privacy, Secure Cloud, Privacy-Preserving Cloud, Trend Analysis, Future Roadmap.

1 INTRODUCTION

In recent years, cloud computing has been of great interest to the research community [1] [2]. It is used in a variety of applications ranging from healthcare [3] [4] to geosciences [5] and autonomous vehicles [6], [7]. Cloud computing plays a significant role in modern technology as it is actively interacting with other technological fields such as edge [8] and fog computing [9], Internet of Things (IoT) [10], sensor technology [11] and big data [12], [13]. “Edge Computing has been defined as a distributed computing topology in which the storage and computing has been perfume close to the source of data. Fog Computing has been defined as decentralized computing infrastructure that perfume between the data source and the cloud. Enabling technologies that support cloud computing vary from real-time computing [14] and virtualization [15] to artificial intelligence [16], [17], [18]. Several design objectives including performance [19], reliability [20] and fault tolerance [21] are considered in the design of cloud computing systems. Especially, concerned about different aspects of security including attack resilience [22], [23] [24] and confidentiality [25], [26] have been of concern to cloud computing researchers. However, privacy seems to be the most critical security aspect in cloud computing [27], [28], [29].

In this paper, we first establish an ecosystem for privacy-preserving cloud including applications, vehicular technology, healthcare, social networking, Internet of Things (IoT), smart home, big data, and data centers. Then we developed a life cycle and reviewed it in these stages: design, verification, implementation, and deployment. In the next step, we build a layered architecture containing Privacy-Preserving Infrastructure, Privacy-Preserving Services, and Privacy-Preserving Computing. Lastly, we establish a future roadmap in Quantum-Inspired and Bio-Inspired AI. We present our paper with the hope that we can motivate others to study these topics further as these new technologies develop. It should be noted that although there may be existing survey papers related to the topic at hand, they have shortcomings which motivate our work in this survey. It is our intention to cover the topic of Privacy-Preserving Cloud Computing as comprehensively as possible.

The rest of this paper is organized as follows. Section 2 summarizes existing surveys. Section 3 outlines the applications and technologies that comprise the ecosystem for cloud computing. Section 4 outlines the full 4-stage life cycle of a cloud system . Section 5 describes the layers which make up the architecture of a privacy-preserving cloud system. Finally, Section 6 outlines a future roadmap for cloud computing and how Artificial Intelligence (AI) can be used to create new technologies.

Privacy is important in cloud computing because it ensures that data shared in the cloud can only be accessed by those who have been given permission. Without proper data privacy, the integrity of data stored in the cloud would not be able to be guaranteed. In Figure [1] Artificial Intelligence and Cryptography combine together, resulting in a Privacy-Preserving Cloud system where privacy is built into the foundation using AI and Cryptography concepts.

In Figure [1] the blue cloud represents Artificial Intelligi-
Fig. 1. Privacy Incorporated in the Design of Cloud Computing Environment

2 Existing Surveys

There are many surveys on the security of cloud computing. However, some of them are too outdated for such a dynamic research area. Others do not focus on the privacy of cloud computing[30]. Some existing surveys study cloud computing only in specific applications, and some of them fail to develop a future roadmap. These shortcomings motivate our work in this paper.

2.0.1 Surveys on Challenges, Issues, Concerns and Requirement of Cloud Computing

Storing data deals with many challenges in security and privacy, and Cloud Service Providers should take appropriate steps to overcome these challenges[31]. In this section, previous studies and outputs have been reviewed. Although Mobile Cloud Computing (MCC) provides a way to meet our needs for abundant resources in transportable devices, there is a lack of security and confidentiality. To that end, in [32] security issues and challenges in mobile cloud computing have been analyzed. In [33], Data Integrity (DI), Data Confidentiality (DC), and availability that are very important in cloud storage have been studied. Furthermore, one of the famous and popular technology for organizations and personal users that Cloud Computing has provided is Storage as a Service (StaaS). The security and privacy challenges according to growing concern in StaaS have been presented in [34]. Decreasing security risks in Cloud Computing is the fundamental action that has been analyzed in [35], [36] by authors proposed solutions to overcome. These concerns were further studied in [37] and [38] since that is not obvious where the data is stored and controlled. In [39], the Pixel key pattern and Image Steganography techniques have been proposed to solve insuperable data security problems in Cloud Computing but in [40] potential issues for gathering access to users data and harming their privacy have been studied in order to attract urgent attention. Three threats are data breaches, hijacking of accounts, and multitennancy that brought about security issues that have been analyzed in [41], and predicted that if these issues have been solved, cloud computing will be more widespread. Although The requirements and solutions of cloud computing security were reviewed comprehensively in [42], its publication year is old, and its solution may not be helpful for present technology according to fast development. In [43] and [44], similar algorithms have been proposed to overcome the obstacles in Cloud Computing under three fundamental categories, cryptographic, data storage, and data semantics. Moreover, Information that users should be aware of to estimate risks related to preserving their data was presented in [45], but the privacy of users was not under observed.

2.1 Surveys on the Evolution and Future Foresight

Cloud Computing and Blockchain technology development have been examined in [46], [47], and how these technologies can integrate and improve each other drawbacks were under observation.

2.2 Surveys on the Applications of Cloud

2.2.1 Applications in Healthcare and Medical Systems

In [48], the authors argued the security peril of cloud service platforms in the field of medicine and also provided related solutions. Protecting privacy and security of users and data were presented in [48] and explained a method that can refuse illegal users permission.

2.3 Surveys on Secure Cloud

The existing surveys related to infrastructure and the concept of security in Cloud Computing have been reviewed in this section. Likewise, in the first subsection of this section, we investigate the general security concept in Cloud Computing, and in the subsequent subsections, privacy and security of data, storage, communication [49] have been studied. Moreover, cryptographic and steganography methods, and Secure Data Sharing risks have been reviewed in current surveys subsequently. Following sections, authentication and security auditing, as well as data provenance and challenges and risks, threats and attacks, have been investigated.

2.3.1 The General Concept of Security

In [50] authors came up with a method for solving the problem related to enterprise users, cloud operators, and regulators by analyzing current security and privacy challenges, in addition in [51] authors have analyzed the solution of different categories of risks in cloud systems such as infrastructure threats, host threats, and service providers
threats similar to [52] that authors have introduced a solution to overcome security issues related to confidentiality, integrity, availability, authentication. In comparison to [53], where the authors have viewed the privacy and security of data from the perspective of appropriate training because the consultant is a crucial part of service providers that are dealing with the implementation. The authors in [54] have observed the effect of extended cloud such as Mobile Edge Computing (MEC) and fog on network schematic of cloud computing; also, they analyzed models and architectures of technologies due to the security and flexibility that is required while in [55], the authors have analyzed the algorithms that come from biological In order to deal with security issues of cloud computing. In addition, the authors in [56] have come up with an innovative method which is Cloud Bursting Brokerage and Aggregation (CBBA), and analyzed the secure sharing mechanism to reduce cloud-bursting with denial-of-service (DoS) attacks or distributed denial-of-service (DDoS) attacks that have deleterious effects on cloud computing.

As opposed to [57] that Secure Smart Grids in cloud-based software platforms was observed, the authors in [58] have explained the model, control, and management of the rechargeable batteries such as Li-ion batteries used in IoT. Furthermore, the vulnerabilities and threats in the live migration of Virtual Machine have been presented in [59] and claimed that there is an inadequate solution to provide security. Moreover, Sun and Aida have indicated how they meet the security of user applications with a method for running applications that need huge resources on both local computing resources and Infrastructure-as-a-Service Cloud (IaaS) by making use of machine learning in [60] similar to [61] where the authors have demonstrated how they came over several basic issues and improved CPU frequency in Virtual Machine with Workflow Scheduling. In addition, the security of live migration in virtualization has been analyzed in [62], and authors have introduced three techniques to cover confidentiality and integrity of data, authentication, and authorization of operations.

2.3.2 Privacy-Preserving Cloud
A framework of privacy protection in cloud computing has been demonstrated in [63], and the authors have analyzed the concept of encryption and security and draw future directions, while the authors in [64] reviewed a number of articles related to the privacy and security of electronic health records in cloud architecture and the cryptographic and non-cryptographic of electronic health records protection. In addition, the vulnerabilities and threats in Cloud Computing have been analyzed in terms of confidentiality, integrity, availability, accountability, and privacy-preservability in [65] and they have proposed strategies for protection. Also, for dealing with challenges and improving the level of privacy in Cloud Computing, Privacy Enhancing Technologies was studied by authors in [66] in order to identify a method. The authors have demonstrated a rundown of technologies and patterns in order to protect and encrypt data in [67] and emphasized issues and tackles that can be studied in the future in Vehicular Cloud Computing in [68] by reviewing and examining the structure and concept of cloud storage and adventures and risks of security and privacy of cloud storage. Although, the authors in [69] argued the most advanced method of privacy-preserving that is utilized in e-Health clouds as well as explained categorization of cryptographic and non-cryptographic approaches, in [70] the security and privacy of health data stored in the cloud have been reviewed in order to indicate the advantages and disadvantages of eHealth's security and privacy algorithms. Several implementation techniques that can help developers and a number of privacy issues that should be attended to in the cloud systems environment have been presented by authors in [71]. As opposed to [72] where the number of analyses that carried out in cloud computing has been examined in order to make known threats related to cloud computing architecture, authors in [73] argued security and privacy issues in order to provide appropriate solutions. Moreover, an encryption data method which is the Bloom filter technique has been presented in [74].

2.3.3 Secure Data
Data Security is vital and important in cloud computing [75]. The encryption algorithms have been analyzed in terms of providing the security of data in storing and transferring in [76] similar to [77] in order to overcome the challenges in the security of information. In [78], the perceptions of audit and data security that is the fundamental obstacle that should pay attention to having been analyzed, while in [79] Multi-Cloud Database (MCDB) has been reviewed, and they explained its drawback, which is the multi-stage cloud that should be considered in order to make it simple in the future. Furthermore, cloud services such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) have been analyzed in terms of cloud computing security issues in [80], and also the authors provided some solutions for security and overcome its drawbacks. In [81], the Mobile Cloud Computing data security frameworks have been under observation to recognize obstacles, issues, and security measures for improvement in future implementation. Moreover, encryption and decryption algorithms have been presented in [82] and authors have proposed new algorithms that improve the security and efficiency of data in cloud computing.

2.3.3.1 Data Security Standards: The existing method of integrity, authentication, and confidentiality of data in cloud computing has been presented in [83] and [84]; also the authors analyzed security techniques, issues, and challenges to improve data security measures in cloud computing.

2.3.4 Secure Storage
There is growing concern about storing data in the cloud [85]. In [86] the authors have demonstrated how the secret key, used in encryption and decryption, has affected the efficiency and security of bandwidth and storage space. The security of data storage related to diabetes disease in cloud computing was under observation in [87], and authors brought up some issues that need to be considered for the framework that collects information similar to [88] where several cloud data storage infrastructure and security algorithms were presented and offered the accountability process, and protection measures that need to be developed in further study. In addition, the effects of data
security in cloud storage on integrity, confidentiality, and availability were analyzed in order to recognize security requirements that have been analyzed in [89]. Also, encryption and decryption algorithms used in cloud storage were analyzed and compared with related techniques to improve their performances in [90]. Authors have claimed sharing operation and searching operation architect needs to develop and design securely in the future. In contrast, in [91] challenges and limitations were observed in terms of data security in these systems and authors have argued how security and usage of information provided in various search systems in cloud storage similar to [92] that authors have analyzed security algorithms and techniques used in the client-side and vendor-side. Moreover, The advantages of using blockchain in cloud computing were presented in [93] as well as authors analyzed how these methods improve the security of data in cloud computing due to its decentralized nature. Likewise, The authors in [94] have analyzed security data and provided solutions to improve third parties infrastructure in terms of safety, privacy, and availability measures.

2.3.5 Secure Communication

For reviewing secure communication subjects in current surveys, Soni and Kumar have analyzed methods and algorithms related to cloud computing security to find the gap between future development and previous research, and they gave prominence to future suggestions.

2.3.6 Cryptographic Security

Cryptographic Security is one of the fundamental methods for providing security and privacy of data in Cloud Computing [95]. Proxy re-encryption, which can encrypt data in cloud computing with user private key, has been under observation in [96] and authors, by comparing it with current algorithms and measures have introduced better security and efficient data solutions similar to [97] where the security schema and design of public-key encryption with equality test (PKE-SF) was discussed and authors have examined its feature efficiency and proposed some helpful directions. In addition, various cryptographic techniques in the public cloud have been reviewed in [98], and demonstrated how these techniques could preserve data from malicious activity in cloud computing and highlighted their issues similar to [99] that several security issues were presented, and authors proposed various solutions for the purpose of getting to know about them for increasing security in cloud conditions. Furthermore, in [100] and [101] the authors compared several cryptographic methods and demonstrated differences in cost and performance, and genetic algorithms and visual cryptography have been proposed for concealing high-priority data similar to [102] that authors have proposed cryptographic techniques that improve the security of cloud storage.

2.3.7 Steganography

In [103] authors have described its related techniques: the Least Significant Bit (LSB) and the Discrete Cosine Transform (DCT).

2.3.8 Secure Data Sharing

The security of data sharing is one of the most critical steps in Cloud Computing [104]. Authors in [105] have introduced several methods that provide data sharing security in the cloud environment but mainly analyzed Ciphertext Policy Attribute-Based Encryption(CP-ABE) that has been used in integrity policies.

2.3.9 Risks, Threats and Attacks

In [106], the authors reviewed several papers and identified several security issues that affected the cloud computing environment. They conclude that the blockchain mitigates security concerns for service providers and users similar to [107] that authors have proposed Advanced Security Measures and Practices to improve the structure of current technology to deal with security risks and challenges. The structure of the blockchain method has been analyzed in [108], and the authors proposed a secure method of blockchain that can overcome security issues and risks as opposed to [109] where the authors have explained the vulnerabilities, attacks, and threats related to cloud services and infrastructures. In addition, the benefits and drawbacks of current security methods have been analyzed in [110], and the authors argued potential capabilities in the security of cloud service in order to overcome disadvantages in comparison to [111] that authors did a thorough investigation in the security of cloud infrastructure and offered a method that can improve issues and risks in that time. However, due to the year when the paper was conducted, this method would not be effective. In addition, In [112], authors conducted a detailed analysis on papers between 2019 and 2020 to help companies be aware of cloud computing vulnerabilities and prioritize due to the widespread use of cloud services as opposed to in [113] that risk management methods that are different from those in IT enterprise have been analyzed in cloud systems and authors have demonstrated its efficiency in cloud security challenges by observing technically. The accuracy of Intrusion Detection Systems (IDS) have been analyzed in cloud base malicious, and attacks in [114] and authors have reported IDS which utilizes multiple method detection to improve its efficiency in the cloud while in [115] the current security framework has been analyzed to accentuate the disadvantages and drawbacks and authors have implemented new Intrusion Detection Systems(IDS) and Prevention System (IPS) that improve security in virtual networks.

2.3.10 Authentication

In [116], the authors have made use of Kerberos as a third-party auditor for authentication, RSA algorithm (Rivest–Shamir–Adleman) for security, and MD5 algorithm to provide integrity and also how the cloud systems provide security when information data is being transferred. In addition, in [117], the duplication process has been presented in detail, and new techniques in a cloud architecture that encrypts duplicate-check tokens of files with private keys have been presented.
2.3.11 Data Provenance

The analysis of current provenance management schemes in the cloud system and their security solution was presented in [118].

2.3.12 Security Auditing

The advantages and drawbacks of several Third Party Auditing (TPA) have been analyzed in [119], and the authors have concluded that nearly all TPA methods need to be developed in terms of the security of public auditing.

2.4 Surveys on Cloud-Based Big Data

Big Data refers to an enormous amount of data that has been produced these days by different sources, such as IoT devices. Since storing a vast amount of data in the cloud computing is becoming a challenge for service providers. Different security methods of eHealth data in the cloud have been presented in [120], also in order to improve security, and the authors came up with a technique that is storing the patient data initially in the cloud, and another in the fog layer. In contrast, in [121], prior research in the security of storage management has been analyzed, and authors have proposed a new technique.

2.5 IoT-Based Cloud and Cloud-Based IoT

Internet of Things (IoT) devices are widespread these days since there is no doubt in the benefits of those devices, but when it comes to private data, the security mechanism has played a vital role [122]. This section studied IoT and cloud computing, two concepts that have become so interwoven and almost inseparable. Several infrastructures of IoT were analyzed effectively from the perspective of security in [123], and authors have observed them by conducting the man-in-the-middle attack between end devices sensor and service providers while in [124] just the security of data in the Internet of Things (IoT) integrated with Cloud Computing has been analyzed, and risks and threats in the Internet of Things have been highlighted. Moreover, the security risks related to storing and collecting data from IoT devices that need urgent action have been presented in [125]. In addition, the authors came up with solutions that may be helpful as opposed to [126] that threats, risks, vulnerabilities of Supervisory Control And Data Acquisition (SCADA) systems have been analyzed, and some crucial issues reported. WebSCADA is an application utilized for innovative medical technologies.

2.6 Surveys on AI-Assisted Secure Cloud

The authors reviewed 60 articles in order to demonstrate challenges and accuracy estimation of using machine learning and the type of machine learning in cloud security [127]. The efficiency of facial recognition techniques in a cloud environment from data security has been analyzed in [128]. Cloud data behavior detection and recognition are the major components that will contribute to developing a secure data surveillance system implemented in a cloud environment that will protect stored data from network intrusions and ensure data security.

In this location, you need a table. Each row of the table is allocated to one of the above surveys. The first column in each row cites the related survey paper. The second row contains the publication year of the survey. The third row indicates whether or not the survey focuses on the privacy of cloud computing (Yes/No). The fourth column indicates whether or not the survey presents a future roadmap (Yes/No). The fifth column indicates whether or not the survey studies cloud computing in a specific application (Yes/No).

The summary of previous studies related to Privacy-Preserving in Cloud Computing has been presented in Table 1 and Table 2. The first column refers to the published year, and the second column shows whether the paper focuses on the privacy of cloud computing or not. The next column indicates whether the paper creates a future road map or not, and the last column specifies if they have been studied in a specific application. In both tables, the papers have been reviewed as 2010. In the Table 1, just 13 papers focus on privacy in cloud computing, while in Table 2, no paper focuses on privacy in cloud computing. Some papers have drawn a future road map and analyzed cloud computing in a specific application.

3 Ecosystem

Privacy-Preserving Cloud can have many uses in different sectors in order to create an ecosystem [132]. In Section 3.1, we explore the various applications of this technology and examine how it can be beneficial in these areas. The technology which allows for these applications to function is explored in Section 3.2. In order to keep these ecosystems secure, there are various technologies and mechanisms which can be used. Section 3.3 covers several of these security measures. Finally, in Section 3.4, this paper will take a look at the security challenges which come along with using a cloud-based ecosystem.

In Figure 2, a base for the ecosystem is formed by Enabling Sciences and Technologies such as Optimization [133], Blockchain [134], PUF, Edge Computing, Fog Computing, and Wireless Sensor Networks [135]. On top of this base stands the pillars consisting of the Enabling Security Mechanism such as Anonymization, Privacy-Preserving Authentication, Privacy-Preserving Access Control, Privacy-Preserving Cryptography, and Privacy-Preserving Watermarking. Finally, Applications rest on top of the structure because they are enabled by the technologies below them. These applications include Data Centers, IoT, Smart Homes, Big Data, Industrial Environments, Vehicular Technology, Healthcare, and Social Networking.

3.1 Applications

3.1.1 Industrial Environments and IIoT

The Industrial Internet of Things is a subset of the Internet of Things which works to optimize industrial production by providing tools with additional connectivity and intelligence, as detailed in [136], [137]. In the healthcare industry, the Internet of Things works to improve services for patients with devices that can more effectively monitor them and collect their health data.
### TABLE 1
Summary of previous studies in Privacy-Preserving Cloud Computing - Part 1

| Published | Year | NN-focuses on the privacy of cloud computing | a future roadmap | cloud computing in a specific application |
|-----------|------|---------------------------------------------|------------------|------------------------------------------|
| [12]      | 2018 | no                                          | no               | no                                        |
| [13]      | 2019 | no                                          | no               | no                                        |
| [14]      | 2019 | no                                          | no               | yes                                       |
| [15]      | 2020 | yes                                         | no               | no                                        |
| [16]      | 2020 | no                                          | no               | no                                        |
| [17]      | 2015 | no                                          | yes              | no                                        |
| [18]      | 2015 | yes                                         | yes              | no                                        |
| [19]      | 2015 | yes                                         | yes              | no                                        |
| [20]      | 2014 | yes                                         | no               | no                                        |
| [21]      | 2016 | no                                          | no               | no                                        |
| [22]      | 2012 | no                                          | yes              | no                                        |
| [23]      | 2017 | no                                          | yes              | yes                                       |
| [24]      | 2020 | no                                          | yes              | no                                        |
| [25]      | 2015 | no                                          | yes              | no                                        |
| [26]      | 2018 | no                                          | no               | yes                                       |
| [27]      | 2013 | no                                          | yes              | no                                        |
| [28]      | 2015 | no                                          | no               | no                                        |
| [29]      | 2015 | no                                          | no               | no                                        |
| [30]      | 2016 | no                                          | no               | no                                        |
| [31]      | 2017 | no                                          | no               | no                                        |
| [32]      | 2017 | no                                          | no               | no                                        |
| [33]      | 2014 | no                                          | yes              | no                                        |
| [34]      | 2015 | no                                          | yes              | no                                        |
| [35]      | 2018 | no                                          | no               | no                                        |
| [36]      | 2018 | no                                          | yes              | no                                        |
| [37]      | 2019 | yes                                         | yes              | no                                        |
| [38]      | 2019 | yes                                         | yes              | no                                        |
| [39]      | 2019 | yes                                         | yes              | no                                        |
| [40]      | 2019 | yes                                         | yes              | no                                        |
| [41]      | 2018 | no                                          | no               | no                                        |
| [42]      | 2017 | no                                          | yes              | no                                        |
| [43]      | 2016 | no                                          | no               | no                                        |
| [44]      | 2019 | yes                                         | yes              | no                                        |
| [45]      | 2019 | yes                                         | yes              | no                                        |
| [46]      | 2019 | yes                                         | yes              | no                                        |
| [47]      | 2019 | yes                                         | yes              | no                                        |
| [48]      | 2020 | no                                          | no               | no                                        |
| [49]      | 2020 | no                                          | no               | no                                        |
| [50]      | 2020 | no                                          | no               | no                                        |
| [51]      | 2020 | no                                          | no               | no                                        |
| [52]      | 2021 | no                                          | yes              | no                                        |

### TABLE 2
Summary of previous studies in Privacy-Preserving Cloud Computing - Part 2

| Published | Year | NN-focuses on the privacy of cloud computing | a future roadmap | cloud computing in a specific application |
|-----------|------|---------------------------------------------|------------------|------------------------------------------|
| [91]      | 2021 | no                                          | no               | no                                        |
| [92]      | 2020 | no                                          | no               | no                                        |
| [93]      | 2020 | no                                          | yes              | no                                        |
| [94]      | 2019 | no                                          | no               | no                                        |
| [95]      | 2017 | no                                          | yes              | no                                        |
| [96]      | 2016 | no                                          | yes              | yes                                       |
| [97]      | 2021 | no                                          | no               | no                                        |
| [98]      | 2016 | no                                          | no               | no                                        |
| [99]      | 2021 | no                                          | no               | no                                        |
| [100]     | 2014 | no                                          | no               | no                                        |
| [101]     | 2017 | no                                          | no               | no                                        |
| [102]     | 2014 | no                                          | yes              | no                                        |
| [103]     | 2019 | no                                          | no               | yes                                       |
| [104]     | 2021 | no                                          | no               | yes                                       |
| [105]     | 2021 | no                                          | no               | no                                        |
| [106]     | 2021 | no                                          | yes              | no                                        |
| [107]     | 2020 | no                                          | no               | no                                        |
| [108]     | 2020 | no                                          | no               | no                                        |
| [109]     | 2020 | no                                          | no               | no                                        |
| [110]     | 2015 | no                                          | no               | no                                        |
| [111]     | 2015 | no                                          | no               | no                                        |
| [112]     | 2015 | no                                          | no               | no                                        |
| [113]     | 2015 | no                                          | no               | no                                        |
| [114]     | 2015 | no                                          | no               | no                                        |
| [115]     | 2015 | no                                          | no               | no                                        |
| [116]     | 2015 | no                                          | no               | no                                        |
| [117]     | 2017 | no                                          | no               | no                                        |
| [118]     | 2015 | no                                          | no               | no                                        |
| [119]     | 2019 | no                                          | yes              | no                                        |
| [120]     | 2019 | no                                          | no               | yes                                       |
| [121]     | 2018 | no                                          | no               | no                                        |
| [122]     | 2021 | no                                          | no               | yes                                       |
| [123]     | 2021 | no                                          | no               | yes                                       |
| [124]     | 2021 | no                                          | no               | yes                                       |
| [125]     | 2020 | no                                          | no               | yes                                       |
| [126]     | 2016 | no                                          | no               | no                                        |
| [127]     | 2015 | no                                          | no               | no                                        |

in or worn by a patient can allow for a doctor to remotely diagnose a patient. [139] outlines a method of protecting the privacy of industrial data to encrypt it before sending it to the cloud, have operations performed on the encrypted data, and returning encrypted results to be decrypted by the user.

#### 3.1.2 Vehicular Technology

The outline of [140] indicates how cloud technology integrated into vehicles allows for road traffic to be improved with devices such as sensors, cameras, and wireless transceivers. The authors of [141] say that it also helps create a network for autonomous vehicles so that data can be stored and processed remotely. In [142], the authors proposed the use of this technology in vehicular advertisement dissemination which allows for vehicles to receive advertisements from a cloud network. Vehicular cloud technology allows for more complex computations, such as calculating traffic and determining optimal routes, to be offloaded to parked cars which do not have to perform computations of higher priority, as said by [143].
Fig. 2. Applications, Enabling Security Mechanisms, and Enabling Sciences and Technologies joining to form an Ecosystem for Privacy-Preserving Cloud.

3.1.3 Healthcare

In [144], authors state that cloud-based data-driven healthcare monitoring services have allowed for a rapid growth of healthcare data which assist with eHealthcare. To protect this medical data, some networks will use a blind cloud framework which replaces patient identities with generated pseudo-identities. The authors of [145] describe how this allows for unidentified data to be stored and analyzed. Searchable encryption schemes can also be used so that health data can be searched for while maintaining privacy as outlined by [146]. Searchable symmetric encryption (SSE) is a method that provides the ability for users to utilize the storage of another party (a server) for privately hosting data that is encrypted. Therefore, the cloud service provider (CSP) does not have access to them, and when a user wants to access the data, CSP provides the encrypted data for them.

3.1.4 Social Networking

In [147], it is described how many social networking platforms store user information on cloud services, so it is very important to keep this data secure. Techniques such as homomorphic encryption, oblivious transfer, and secret sharing can be used to protect user data. "Homomorphic encryption is a method with which users can analyze or manipulate their encrypted data without decryption.

3.1.5 IoT

Cloud technology has improved the Internet of Things’ ability to manage large amounts of data. Flexible privacy-preserving data sharing allows a user to send encrypted data using an identity-based encryption scheme that is outlined in [148]. In addition, a network attestation scheme outlined by [149] can be used to ensure that scalability, forward-security, and privacy.

3.1.6 Smart Home

Privacy-preserving smart homes have the ability to connect a single house to a cloud platform which aggregates the data from all other houses on the network. The outline of [150] indicates that this data can be used to increase home safety and energy efficiency in order to increase a resident’s quality of life.

3.1.7 Big Data

Because of mobile networks, data is constantly being generated at a rapid pace. In [151], authors state that this data generation is called big data stream. The authors of [152] outline how cloud computing can offer a scalable infrastructure so that this big data stream can be processed and aggregated.

3.1.8 Data Centers

As detailed by the authors of [153], Geo-distributed cloud data centers hold and transfer large amounts of data every day. Due to privacy laws differing based on region, it can make the transfer of data across borders difficult to do. Data centers must ensure that they follow the strict data regulations put in place by countries and organizations, such as General Data Protection Regulation (GDPR).

3.2 Enabling Sciences and Technologies

3.2.1 Optimization

In [154], the authors describe how outsourcing computation-intensive tasks to the cloud allows for systems to be more optimized, but comes at the risk of more privacy and security issues.

3.2.2 Blockchain

In order to protect data stored on the Cloud, blockchain-based technology [155] such as AuthPrivacyChain can be used to prevent hackers from accessing resources as outlined in the framework devised by [156, 157]. In the [158] paper, it describes how blockchain has also been used to implement forward and backward privacy by enforcing searchable public-key encryption, and [159] describes how it can act as a distributed public ledger so that health data can be shared on a cloud-based system.

3.2.3 PUF

In [160], it is said that physical uncloneable functions, or PUFs, provide the ability to have lightweight physical identities for smart devices. Physical Uncloneable Functions (PUFs) introduce an extra player of physical security without bringing any additional overhead to smart devices.
3.2.4 Mobile Computing

Mobile cloud computing allows for users to access cloud services through wireless networks [161]. However, [162] outlines how wireless networks are vulnerable to numerous threats which means more security measures must be taken. Some such measures which can be taken are listed by [163], such as key management for unlinkability, a secure indexing method, and integration of attribute based encryption. In addition, the authors of [164] outline how scalable and privacy preserving friend matching offers a scalable solution for protecting social media user data over mobile networks. Authentication methods such as privacy-aware authentication and MediChain-based privacy-preserving mutual authentication can also help protect data over mobile cloud networks, as described by the authors of [165] and [166].

3.2.5 Edge Computing

In [167], it is described how mobile edge clouds deploy at the network edge in order to allow mobile users to access cloud services. However, mobile social sensing means that users need to report personal information which could result in data theft. In [168], the authors propose that participant grouping can work as one solution by leveraging secure sharing within groups.

3.2.6 Fog Computing

The authors of [169] claim that fog computing can be used to extend cloud computations to the edge of a network and provide storage, geo-distribution, and mobile support. Fog computing can be used to keep data on the cloud safe by using a one-round authenticated key argument protocol as outlined by [170], or by using a homomorphic Paillier cryptosystem as outlined by [171]. Homomorphic encryption is a method of encryption in which users can do mathematical operations on encrypted data without decryption. The Paillier cryptosystem, that Pascal Paillier has proposed in 1999, is a probabilistic asymmetric algorithm for public key cryptography.

3.2.7 Wireless Sensor Networks

Wireless sensor networks are vulnerable to attack if the source node is located. "Wireless sensor network refers to wireless sensors that communicate and collect data, for instance, temperature, humidity, etc., from the environment that have been installed. In [172], authors proposed that one method of protecting the location of the source node is to change packet destinations randomly in each transmission on the network. To compliment this, a source-location privacy protection scheme based on anonymity cloud which can also be used to protect to the location of the source node by constructing an anonymity cloud around the source node has been proposed in [173].

3.3 Enabling Security Mechanisms

3.3.1 Anonymization

In order to check that cloud infrastructure is meeting the intended security standards, the practise of security auditing is often employed [174]. In order to maintain privacy, input data and audit results are anonymized. Anonymization is the process that removes or alters the data that causes a subject to be identified directly, a method called SegGuard uses per-tenant encryption and property-preserving encryption so that the data is able to be audited while still offering sufficient protection has been proposed in [175].

3.3.2 Privacy-Preserving Authentication

Many authentication schemes for tamper-proof devices have been proposed to allow privacy and security in open-access environments. In [176], the authors explain how Vehicular Ad-Hoc Networks require such authentication so that they may improve transportation networks. Because of the cloud, these vehicles need to only register with a trusted authority once in order to authenticate as outlined by the authors of [177]. In [178], the authors suggest that cloud computing has allowed for data from biometric identification to be outsourced to the cloud for computation, offering a more reliable way to authenticate a user. The authors of [179] explain how this biometric data can be protected by using a matrix-transformation-based privacy-preserving biometric identification scheme using the property of the orthogonal matrix and additional randomness. Additionally, the authors of [180] detail how authentication can also be improved for mobile users by using the cloud to support mutual authentication, key exchange, user anonymity, and user untraceability. In [181], the authors suggest that a shared authority based privacy-preserving authentication protocol can be used to address the issue that a challenged privacy request on a shared network can reveal a user’s privacy regardless of whether their request is granted. In a distributed cloud-based system, an authorized accessible privacy model can be used to keep data and identity private simultaneously has been presented in [182]. Anonymous authentication can be achieved by using a registered security token in conjunction with a key exchange which uses preauthentication and postauthentication user anonymity to generate a pseudoidentity [183].

3.3.3 Privacy-Preserving Access Control

In order to facilitate resource sharing, the authors of [184] suggest that cloud applications allow users to delegate their access permissions. Access control policies guard the access to cloud resources and credentials. In the bioinformatic field, large amounts of genomic data are stored and processed over the cloud. The P2GT scheme detailed by [185] uses key-policy attribute-based encryption to manage data access control. Mobile cloud computing can use authentication schemes such as Self-Certified Public Key Cryptography (SCPKC), Chinese Remainder Theorem (CRT), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Scalable Media Access Control and Deduplication and (SMACD) to manage access, as detailed by the authors of [186], [187], and [188]. In order to enforce authorization for fine-grained access control on the cloud, the authors in [189] state that an organization must use encryption.

3.3.4 Privacy-Preserving Cryptography

3.3.4.1 Data Encryption:
According to [190], users can search encrypted documents on the cloud using dynamic symmetric searchable encryption. Dynamic data encryption allows for performance to be improved while working under time constraints [191] and achieves a high level of privacy [192]. The authors in [193] suggest using certificateless encryption keyword search to allow for multirecipient keyword searching, which allows for privacy to be preserved on the Internet of Things. Because the cloud is so open, in [194] the authors claim that identity-based encryption is important to maintain accountability. The authors of [195] state that user identities can even be formed by combining a user’s identity with the identity of their attribute authority. Using asymmetric scalar-product-preserving encryption, in [196] authors indicate that fuzzy multi-keyword search can be achieved.

3.3.5 Privacy-Preserving Watermarking

In [197], authors define Watermarking as when a watermark is embedded into media so that it may be identified. Privacy-Preserving Watermarking allows for a party to entrust the task of watermarking data to a cloud service.

3.3.6 Privacy-Preserving Integrity Checking and Auditing

While cloud storage offers easy maintenance and management of stored data, the authors of [198] say that it does not ensure integrity. Remote data integrity checking can be used to verify that data stored on the cloud is stored honestly [199]. A third party auditor can be used to audit data to ensure integrity, as can dynamic data integrity auditing as stated by the authors of [200] and [201]. A Provable Data Possession proposed by [202] can allow people to audit data efficiently by outsourcing data into small blocks of data and then blinding them so that each block can be individually verified.

3.4 Related Security Challenges

3.4.1 Trust and Reputation

3.4.1.1 Trustable Computing: The authors of [210] state that in Cloud Computing, privacy and trust create an inherent conflict. In order to evaluate the quantification of privacy and trust in a cloud system, in [211], the authors state that both must be weighted accordingly. A Reputation-aware Trust and Privacy scheme proposed by [212] can deal with trust management by leveraging trust scores for cloud services.

3.4.1.2 Computation in Untrusted Environments: Since outsourcing spatial keyword searches to an untrusted cloud can cause privacy concerns, in [213], the authors proposed that top-k spatial keyword searches can be performed instead, where spatial and textual data are encrypted in a unified way. When an untrusted cloud environment is to be used, a privacy-preserving framework using homomorphic cryptography outlined by [214] can be used to conduct the needed computations.

3.4.2 Attack Resilience

Wireless sensor networks are often deployed in open and large areas which makes them vulnerable to attack. To protect the location of the source node, the authors of [215] describe how fake traffic can be created to camouflage the source node in the cloud. If the guest operating system or the virtual machine monitor of a cloud vendor are compromised, an attack can be launched against users. A solution to this problem put forward by [216] is to integrate on-chip memory protection for trusted applications from attacks.

3.4.3 Forensics

The aim of cloud forensics is to process large sets of data from the cloud and recover evidence. A multigranularity privacy leakage forensics method put forward by the authors of [217] allows for analysis of privacy violations which have been caused by malware.

4 Life Cycle

The Life Cycle of a Privacy-Preserving Cloud system can be broken down into four stages. The first subsection covers Design, which outlines what factors must be taken into account when designing a system. Verification is covered in the second subsection and Implementation is covered in the third. The fourth and final subsection looks at how a system of this nature would be deployed and evaluated.

In Figure [3] the formation of a Life Cycle of a Privacy-Preserving Cloud System is illustrated, with each of the four steps in sequence. The arrows connecting each box signifies the order in which the steps occur.
Fig. 3. Design, Verification, Implementation, and Deployment form the Life Cycle of a Privacy-Preserving Cloud System.

4.1 Design

4.1.1 Additional Design Objectives

4.1.1.1 Cost-Effectivity: Because encrypting all intermediate data sets stored on the cloud would not be cost-effective, the authors in [224] suggest that it is more efficient to first identify which data sets require encrypting so that data privacy is maintained while keeping costs low.

4.1.1.2 Efficiency: In [225], it is said that location-based services found in wireless communications present new efficient schemes in outsourced cloud where the users identity is masked for privacy purposes. By designing a data sharing process which provides integrity by design, in [226], authors state that efficiency can be improved by having a third party audit data stored on the cloud.

4.1.1.3 Resource-Constrain Awareness: Vehicular cloud computing consists of many computations that must be performed dynamically [227], but the limited computational capabilities of a single vehicle must be taken into account. To create a functioning system, the authors of [228] insist that a lightweight architecture must be designed. Likewise, in the healthcare system, heavy computations must be performed on limited hardware, necessitating the use of a lightweight resource-aware system, such as the one proposed by [229]. A lightweight Delegatable Proofs of Storage scheme proposed by the authors of [230] can also be used to speed up data integrity checks in cloud storage systems.

4.1.1.4 Time Constraint Awareness: Because cloud storage can contain a large number of images, it is important for security and privacy reasons that data is audited as soon as possible. For this reason, the authors of [231] state that it is important that cloud systems employ auditing schemes that are aware of time constraints.

4.1.1.5 Reliability: Cloud storage services have become a very popular way to store data, but there are risks of data loss and data leaks. The authors of [232] demand that these issues must be addressed in order for a cloud storage service to be reliable.

4.1.1.6 Scalability: Because cloud services are used to support big data applications in sectors such as business and healthcare, it is important that they have a scalable infrastructure. A proximity privacy model proposed by [233] can be used to cluster data so that high scalability can be achieved by performing data-parallel computations.

4.1.1.7 Performance: One way to improve the performance of a cloud system is to exploit geo-distributed clouds to reduce service delay in a method proposed by the authors of [234] Algorithms such as PBtree traversal width minimization and PBtree traversal depth minimization can also be used to increase performance by increasing the efficiency of query processing when used as outlined by [235].

4.2 Verification

In order to address the risk of private data leaking to the public, a Structural Integrity Verification method described by [236] can be applied to cloud systems using three processes: proof organization, proof transformation, and integrity judgement. For large sets of mobile data, the batch verification method proposed by [237] can be used to reduce the computational cost.

4.3 Implementation

4.4 Deployment

When an organization chooses to use a cloud service, they must consider the security and privacy risks which they are willing to take. For this reason, the authors of [238] state that it is important that a cloud service based on an organization’s needs in these areas.

4.4.1 Evaluation

Using advancements in deep learning technology, the authors of [239] state that attacks against cloud systems can be analyzed in order to propose new defense methodologies. In [240], authors emphasize that it is important that quantitative assessment of the privacy practices of cloud services are analyzed so that clients can make an informed decision about which provided they choose to do business with.

5 Layered Architecture

The architecture of a cloud system is layered, with each layer having its own purpose. The first subsection examines the infrastructure of a cloud system which maintains privacy. The second subsection looks at how privacy is maintained with services such as pre-diagnosis computing and location-based services. The third section details how tasks can be managed privately using task allocation and computation offloading.

5.1 Privacy-Preserving Infrastructure

5.1.1 Privacy-Preserving Physical Layer

The authors of [241] state that in order to audit cloud data to check for data integrity, two lightweight auditing protocols can be used based on online and offline signatures. A device needs only to perform a computation when an outsourced file is available.
5.1.2 Privacy-Preserving Data and Data Infrastructure

5.1.2.1 Privacy-Preserving Data: As defined by [242], data deduplication is a technique which eliminates duplicate data stored on the cloud to save space and bandwidth. However, an attacker can abuse a deduplication check to determine if a file is already stored in a cloud system. Restricting deduplication checks to only the agent and the cloud service provider, data privacy can be improved, according to [27].

5.1.2.2 Privacy-Preserving Storage Storage: As outlined in [243], cloud storage systems allow for data to be outsourced flexibly and conveniently. The authors of [244] detail how deduplication allows for cloud storage to only need to keep one copy of a given file to reduce space usage. Because data such as power meter readings require privacy, schemes such as privacy-friendly cloud storage as detailed in [245] are required. Privacy and reliability in cloud storage environments can be achieved using encryption schemes proposed by the authors of [246] such as BP-XOR secret sharing or LDPC secret sharing. Another way to preserve privacy proposed by [247] is to enable cloud users to distribute and search encrypted cloud data across clouds managed by CSPs. To safely share data, the authors in [248] say that sanitizable signatures can be used to hide sensitive information. Its is important that auditing is available in cloud storage systems so that users can have the integrity of their data ensured, as per [249]. In order to properly audit generating-based cloud storage, a proxy that is privileged to regenerate authenticators must be used in a way detailed in [250]. To protect cloud servers from internal attacks, a three-layer storage framework devised by [251] can be used based on fog computing.

5.1.2.3 Privacy-Preserving Databases:

In [28], it is outlined why multi-dimensional range queries on cloud networks should not be fully trusted as many implementations suffer from data leakage. A blockchain enabled query framework can result in high efficiency and scalability [252]. For health data, a query scheme put forth by [253] could be used where medical data is encrypted and stored on the cloud, and then specific diseases are queried on that data. Searchable symmetric encryption, as proposed by [254], can be used to protect the privacy of both the queries and the database. For a secure database, a two-cloud architecture devised by [255] can also be used, where a series of intersection protocols provide privacy for numeric-related range queries.

5.1.3 Privacy-Preserving Data Exchange Infrastructure

5.1.3.1 Privacy-Preserving Data Sharing:

Data sharing is a service that, when supplied by cloud computing, the authors of [256] say can be convenient and economic to a user. In [257], authors emphasize that it is important that the data being shared is not exposed to unauthorized users or to the cloud provider in order to maintain privacy, which generally comes with a computational cost as said in [258]. Secret sharing group key management protocol and public auditing can be used to help tighten security when data sharing in methods detailed by the authors of [259] and [260]. Ring signatures can help to compute verification metadata when performing a data audit when used as described by [261], and a broadcast group key management system detailed by [262] can help with selectively sharing documents.

5.1.3.2 Privacy-Preserving Data Publishing: With cloud computing, because data owners are no longer in possession of physical copies of their own data, this creates the issue of privacy-preserving set-valued data publishing as said in [263]. Using retrievable data perturbation as detailed by the authors of [264], we can create a solution to this issue.

5.1.4 Privacy-Preserving Communications

To deal with the growing amount of network traffic, some traffic is redirected to outsourced middleboxes. To ensure data privacy during redirection, encrypted header-matching schemes proposed by [265] can be used to keep data safe. Network security can also be enhanced by protecting transmitted social messages with integrated security-based mobility prediction algorithms to help resist attacks, as detailed in [266].

5.1.5 Privacy-Preserving Protocols

When ensuring security during data transmission and storage, there should be protocols set in place as described in [267] to protect the identify of communicating units during encryption. To evaluate a protocol, the author in [268] state that a simulation can be performed based on typical circumstances of attacks.

5.2 Privacy-Preserving Services

In the mobile healthcare field, a Diverse Keyword Searchable Encryption scheme proposed by [269] can be used to search and make diagnosis over stored encrypted data. To maintain privacy of genomic data, the authors of [270] state that information should only be access through a fine-grained access control policy with attribute-based encryption. To preserve the privacy of location-based services, data outsourced to the cloud should be encrypted and only be able to be queried by registered authorized users in methods detailed by the authors of [271] and [272]. For data sharing services, the authors of [273] state that data should not be shared with a third-party in order to maintain privacy.

5.3 Privacy-Preserving Computing

5.3.1 Privacy-Preserving Task Management

5.3.1.1 Privacy-Preserving Task allocation: In a mobile network, an auction-based privacy-preserving incentive scheme proposed in [274] can be used for task allocation, where each user can control their privacy budget. Using differential privacy and geocast, we can create task allocation strategies that consider privacy, utility, and overhead in a mobile environment as detailed in [275].

5.3.1.2 Privacy-Preserving computation Offloading: Computation offloading allows for devices to offload tasks to the cloud in order to preserve energy and time. When offloading, usually devices will do so to the nearest edge cloud which can expose the location of the device. This issue can be resolved with a location privacy-guaranteed offloading algorithm proposed in [276].
5.3.2 Privacy-Preserving Task

5.3.2.1 Privacy-Preserving Search:

- **Keyword Search**
  Many approaches towards searching over encrypted data are only able to perform exact searches, as per [277]. A privacy preserving ranked multi-keyword search in a multi-owner model as proposed in [278] allows for a user to search without knowing keyword data. With multi-keyword search, a tree-based structure index can improve efficiency, as outlined in [279] and [280].

- **Content Search**
  A privacy-preserving image search system on cloud as outlined in [281] would help protect users privacy by guarding the sensitive information that is stored in image files such as location and event.

5.3.2.2 Privacy-Preserving Data Analytics: Privacy-preserving data classification techniques such as the ones in [282] can be used where knowledge about client input data is not made available to the cloud server. In order to provide for the needs of elderly people in need of housing, in [283] the authors say that real estate recommendations can be made based on the behaviour of the elderly in the cloud. By analyzing sports records, [284] says that exercise recommendations can be made for individuals who wish to live healthier. Likewise, a clinical cloud system could use data to make diagnoses, as outlined in [285]. Since the client cannot directly access this data, decision tree training and k-nearest neighbor computation can be used as proposed in [286] and [287].

5.3.2.3 Privacy-Preserving Content Processing:

- **Image**
  
  - **Image Retrieval**
    Cloud computing has allowed for large amounts of images to be stored easily as outlined in [288], but this has led to a number of privacy concerns, as per [289]. In [290], it is described how content-based image retrieval applications have generally been limited by computation and storage requirements. A polyalphabetic cipher can be used to improve security with no retrieval accuracy degradation, according to [291], and k-ranked multi-keyword search defend against keyword guessing attacks when used as outlined in [292]. In [293], the authors outline how watermark protocols can also be used to prevent from unauthorized image copying.
  
  - **Image Reconstruction**
    In [294], it is outlined how an outsourced image recovery service allows for users to only need to outsource compressed images to the cloud in order to reduce the amount of storage that they use. The cloud can then reconstruct the compressed images safely.

- **Video**
  
  - **Video Surveillance**
    During video surveillance, it is important that privacy is protected without interfering with the regular tasks of the surveillance, say the authors of [296]. The authors of [297] describe how Privacy Region Protecting protects privacy regions without effecting the non-privacy regions so that they are visually intact.
  
  - **Video Reporting**
    In [298] it is described how in vehicular networks, real-time video reporting can instantly report traffic accidents for safety reasons. Using a 5G network, it can be ensured that the system is reliable and secure.

5.3.2.4 Privacy-Preserving Cloud Auditing: Problems such as privacy disclosure, authority abuse, and collusion attacks can be solved by cloud auditing as detailed in [299], [300]. One such scheme proposed in [301] allows for user anonymity without group signatures so that tags are compact. As a real world example, unmanned aerial vehicles require an audit scheme to accommodate their limited storage and computing performance. They can use an audit scheme such as the one in [302] using a distributed string equality check and Merkle-hash tree multi-level index structure.

5.3.2.5 Other Kinds of Privacy-Preserving Computing:

Cloud computing has been used in other such ways, as detailed in [303], such as Pockit, a calculation toolkit which outsources data to perform common arithmetic securely. In [304], authors claim that a secure and efficient privacy preserving provable data possession scheme can be used to allow auditors to verify data possession. Vehicular ad hoc networks allow vehicles to make real time computations and receive updates on things such as road conditions and accidents as outlined in [305]. Finally, as described in [306], cloud systems have allowed for medical prediagnosis services to develop so that users can privately receive remote healthcare.

![Fig. 4. The Layered Architecture of Privacy-Preserving Cloud](image-url)
these layers are the sublayers represented by the orange parallelograms. Withing the sublayers are the subsublayers represented by the green parallelograms. On the left of the image is a legend which labels the symbols and what they represent.

6 Future Roadmap: the Promise of AI

We anticipate that research on privacy-preserving cloud will move towards quantum-inspired and bio-inspired AI-assisted privacy-preserving cloud in the near future. Our reason for such an anticipation is the existence of trends towards AI-assisted cloud, AI-assisted secure cloud and AI-assisted privacy-preserving cloud as well as quantum-inspired AI and bio-inspired AI, which are discussed in Subsections 6.1, 6.2, 6.3, 6.4 and 6.5, respectively.

6.1 AI in Cloud

AI models have been used in the vast amount of data the needs to be analyzed, these models can learn from the data that we have provided for training thus works with a meager error rate [307]. Machine Learning and Probabilistic Analysis based Model (MLPAM) is a novel model created with machine learning to preserve data in the Cloud environment. A comprehensive analysis indicates its security and efficiency in [308], the authors have argued that MLPAM could provide safety and efficiency of data sharing and control in the future for multiple environments such as IoT while in [309]. An Automatic Cloud Detection neural network (ACD net) has been presented that contains two features which can overcome the overestimation problems in Cloud Computing. However, the authors have not created a future road map and explain that their solution cannot overcome the thin cloud detection issue because of an inadequate training dataset. In addition, the Asynchronous-Advantage-Actor-Critic (A3C) presented in [310] for decentralized learning to analyze the parameters of tasks and hosts to make a scheduling decision to perform better, as well as they introduced scalable reinforcement learning models that can be explored more in the future. Furthermore, for developing and managing Deep Neural Network (DNN) in the Cloud-to-Things Continuum, the authors in [311] have used Kafka-ML framework, an open-source framework used in Machine Learning and Artificial Intelligence management. Their analysis has indicated that response time has improved noticeably in comparison with Cloud-only deployment. Moreover, since the mobile web has not had adequate resources to support Deep Neural Network (DNN) in cloud computing, the authors in [312] a Lightweight Collaborative Deep Neural Network called LcDNN has been presented in order to make use of Deep Neural Network (DNN) possible in the cloud for mobile. However, a new deep model named Multiscale Attention Convolutional Neural Network (MACNN) has been presented in In [313], that used asymmetric encoder-decoder structure for ground-based cloud detection. In contrast, in [314], a utility-based mechanism has been offered to equilibrium cost and availability in spot instances. Likewise, a Long Short Term Memory for Neural network framework has been used to examine price tendency. On the other hand, a method in neural network architecture named CloudU-Net for Ground-based Daytime and Nighttime Cloud Images (GDNCI) used has been presented in [315], that is used in the weather forecast; as observed in the paper, its performances have been improved for daytime and nighttime cloud images. As opposed to [316] that An innovative Multilevel Attention-based U-shape Graph Neural Network (MAUGNN) has been introduced, and the authors’ purpose was using (MAUGNN) is to learn point cloud effectively due to 3-D sensors in the IoT industry. In addition, in [317] a multiscale convolutional neural network with color vegetation indices (MCCNN) has been presented. The purpose of this model is labeling in point cloud for the 3-D model; also, the authors have analyzed its efficiency in Terrestrial Laser Scanning (TLS) data (Semantic3D) and ALS data which is Vaihingen3D data point cloud. Similar to [318] that a Pipelined point cloud based Neural Network processor (PNN) has been presented in order to low latency PNN-based 3-D intelligent systems in mobile devices. The authors in [319] have claimed the speed of algorithms has increased because of the 3-D points from the depth image sample and group directly. Furthermore, a novel spatiotemporal neural network with four modules has been introduced in order to remove cloud cover from satellite images in [320] not to mention its impact on the quality of remote sensing mapping and geoinformation has gotten better. As opposed to [321] that Neural Ordinary Differential Equations (NODEs) with Recurrent Neural Networks (RNNs) has been studied in order to assimilate image observations that are to say, with this method classifying missing data in cloud cover is possible. In [322] similarly, a new model was presented for detecting cloud, the method has been developed in Deep Neural Network (DNN) [322] technique with the cross-track infrared sounder, and authors have used the cloud information measured from the image to train their model. Moreover, a number of methods in the neural network, which can be in time-series dataset of cloud server power modeling, have been analyzed in [323]. Also, the authors have studied the advantages and drawbacks of models and their effects. In contrast, deep neural networks have been presented in [324] to obtain deep-hidden fault information in cloud data centers by analyzing massive alarm data collected in their interconnections. In addition, due to storing and analyzing an illimitable amount of data is just possible in cloud computing, in [325], a method for predicting the amount of data requisite cloud services has been presented that is a hierarchical Pythagorean fuzzy deep neural network. Furthermore, in order to improve the accuracy of occupancy map videos, the authors in [326] implement a Convolutional Neural Network (CNN). They claimed that this is the first learning-based work to improve the performance of Video-based point Cloud Compression (V-PCC).

6.2 AI in Secure Cloud

A federated-learning-enabled IoT scheme that provides security and efficiency has been presented in [327], this framework has been produced in order to provide communication-efficient and privacy-preserving users’ data in smart grids with Cloud collaborations similar to [328] that
a secure, verifiable, and fair technique has been presented which protect the privacy of sensitive information, and it operates in an untrustworthy cloud-server. Furthermore, in order to preserve medical diagnosis from Data Islands(DI)-level poisoning attacks, a secure federated learning mechanism that guarantees the confidentiality of DI-related information named SPDDL that make use of multiple keys possible has been presented in [329]. In contrast with [330] that authors have analyzed several neural network prediction services from the perspective of privacy-preserving, the privacy of the model, and the query are considered as well as examined several proposals and introduced an optimized neural network prediction scheme that brings about high accuracy, model privacy, and low overheads in the outsourcing setting. Moreover, In [331], different features have been created to symbolize each disability, then by these features, the image of people with a disability such as wheelchairs, blind people, and people with Down syndrome have been classified. The authors’ result in [331] has demonstrated that the level of securing image mobility in Cloud systems has been improved. In addition, the authors have introduced a framework that provides training and testing data privacy in [332], this framework is a secure cloud-intelligent network that is supported by privacy-preserving machine learning similar to [333] that authors have introduced a framework called SDPDDL (Secure and Privacy-preserving distributed deep learning) for secure and privacy-preserving Distributed Deep Learning (DDL) that makes better security, efficiency, and functionality and preserves users’ identities from external adversaries. Likewise, a framework that is secure and provides authentication for E-Education (online and virtual education) in cloud systems has been presented in [334] to overcome cost, time processing, and security challenges. As opposed to [335] that authors have indicated how to make use of several software-as-a-service (SaaS) on a platform-as-a-service (PaaS) by analyzing data security also the integration between machine learning algorithms and secure data protection algorithms has been studied in [335] similar to [336] that the authors produced and introduced a Phishing Detection (PD) framework that has a three-step feature and developed in machine learning and a Secure Storage Distribution (SSD) in order to provide security and privacy Cloud-IoT data. In addition, a novel firewall method called Enhanced Intrusion Detection and Classification (EIDC) has been introduced in [337]. This firewall detects and ranks by a technique named most frequent decision that increases the performance of learning as opposed to [338] that a model of Quality of Services (QoS) has been introduced that is new and intelligent. The critical feature in that model is deciding the files to be decrypted without decrypting the whole file list in the secure Storage. One of the most crucial concerns is balancing security and performance, which affect each other in the cloud user community. In deep learning networks on a bare metal cloud-based, a system called License Plate Recognition System (LPRS) has been constructed and introduced in [339], the purposes of this system are plate localization, character detection, and segmentation as opposed to [340] that authors have tried to improve the speed and accuracy of facial recognition without losing the privacy of robots in the encrypted domain. Similar to [341] that a model of cloud data repository has been introduced that has trained with mobile data dataset through Training dataset Filtration Key Nearest Neighbor (TsF-KNN) and public-key cryptographic algorithms. The algorithms decline the time of the process and provide privacy and integrity of data. Furthermore, the authors in [342] have argued the advantages of M-Learning by utilizing Mobile cloud computing and analyzed issues and security. Also, they have provided an introduction of Mobile cloud computing structures. Likewise, the authors in [343] have developed a face recognition that is secure in cloud computing in order to protect privacy by random unitary transform encryption algorithms and for dealing with noise and modeling error by making use of multi-device diversity.

6.3 AI in Privacy-Preserving Cloud

Although federated learning has been designed to provide data privacy, the data uploaded from federated learning has been threatened by attackers [344]. In [346], authors have introduced an innovative mechanism to preserve data privacy on cloud-edge learning systems similar to [347] that the authors have introduced an encryption technique called BGV that encrypts data and makes use of cloud servers algorithms to train for the deep computation model. Furthermore, the secure-centralized-computation-privacy-preserving reinforcement learning algorithm has been presented in [348] in order to protect the privacy of users’ data by using a fully homomorphic encryption scheme in a cloud computing infrastructure. In order to provide better complexities and security, a deep neural network architecture has been introduced in [349], called MSCryptoNet that works based on a fully homomorphic cryptosystem in the privacy-preservation setting. Nevertheless, there is a growing concern about the privacy and security of data when it comes to machine learning. In [350], the authors have introduced a secure cloud-intelligent network framework that preserves the privacy of data as opposed to [351] that authors have produced a framework that organizes sparse coding in edge and cloud networks. In this framework for recognizing noise and error of data, they have utilized classification. Moreover, one of the most popular applications in the fog-cloud computing environment is distributed deep learning (DDL) because of its efficiency and scalability. However, there are challenges when using DDL in fog-cloud computing, such as protecting users’ privacy in the training process and confirming users’ identities forged by external adversaries. According to those problems, the authors in [352] have presented a secure and privacy-preserving DDL (SPDDL) for fog-cloud computing. In addition, one of the challenges in the internet of things (IoT) is big data that have been generated. A double-projection deep computation model (DPDCM) for feature learning in big data has been introduced in [353], which has two layers. In addition, For training the DPDCM, the authors have designed a learning algorithm. However, our result in neural network learning depends on how much data we use in the training step. If we want to use another party’s data set, we need a solution because no party wants to disclose people’s private data to others. In [354], authors have described their practical multiparty Back-Propagation neural network
learning scheme over arbitrarily partitioned data. In this model, the Cloud runs most operations on encrypted data from ciphertext uploaded. Whereas In [355], the authors have argued the privacy of users’ data which is used to train. They introduced a model that encrypts users’ data with their public key called the privacy-preserving deep learning model. Furthermore, in smart cities where urban facilities use technology such as smart health, parking, transport, We are dealing with the date which its privacy and security are vital. In [356], the authors introduced a privacy-preserving autoencoder-based deep learning classifier in the Cloud for solving this problem in smart cities. In addition, Homomorphic Secure Multi-party Computation (SMC) or Homomorphic Encryption (HE) schemes have been used for the security of the cloud process with considering the privacy of data. The authors in [357] have argued supervised and unsupervised machine learning capability through neural networks on encrypted data similar to [358] that for privacy-preserving deep neural networks, authors have introduced a framework for transformation network training in coordination. By using the framework, users can train a transformation network with a model from a cloud provider in a secure environment. Moreover, for analyzing big data, at first, organizations should remove Personally Identifiable Information (PII) because it breaks users’ privacy. A Mondrian-based k-anonymity and Deep Neural Network (DNN) based framework has been presented in [359] to preserve data privacy; their analysis shows that it was suitable similar to [360] that in DNN training/classification a new algorithm was presented that filtered images in order to preserve cloud base privacy. In addition, the authors have presented a cloud-based federated approach that makes use of multiple clouds with different distorted data sets and demonstrated appropriate accuracy of DNN with the original dataset can be provided. In contrast, a technique that analyzes images on the client devices and is independent of local Convolutional Neural Network (CNN) has been presented in [361]. Also, the most important effect of CNN-based applications in the mobile Cloud that works on raw image data is serious privacy concerns. Furthermore, In [362] the challenges in time latency, energy consumption, and privacy level have been analyzed in an Edge-Cloud Collaboration (ECC) scenario including several users. The authors presented a Markov Decision Process (MDP) for balancing cost and the privacy level and the Deep Q-Network (DQN), which decreases delay, energy cost, and improves privacy. However, in the cloud environment, data protection is a vital step. In [363], a Machine Learning and Probabilistic Analysis based Model (MLPAM) has been introduced in order to provide security and data protection in the cloud environment. In addition, For reducing data leakage, MLPAM has a powerful sharing protocol. To that end, a growing number of organizations have utilized machine learning applications for many purposes, such as attack detection. We can make sure of its accuracy and efficiency with a privacy-aware deployment method (PDM) that has been presented in [364]. With this method, we can provide privacy which is a challenge in cyber-physical cloud systems (CPCs).

### 6.4 Quantum-Inspired AI

Processing a vast amount of dataset that is complex requires evolving algorithms to provide a way for better training and learning. Since The trajectory planning problem is one of the challenges in a wireless uplink transmission scenario, the authors in [365] have presented a solution that is optimizing via the quantum-inspired reinforcement learning (QIRL) method that improves the performance of an uncrewed aerial vehicle from when it starts flying to its destination. Moreover, New training algorithms have been presented for deep reinforcement learning (DRL) to equilibrium exploration and exploitation in [366]. As opposed to the traditional mechanism, this algorithm is inspired by quantum computation. Also, in [367] quantum-inspired multidirectional association model called QMAM and a one-shot learning and self-convergent iterative learning called IQMAM. Their analysis has indicated the ability to maintain a stable memory capacity and reliable recall in the model. In contrast, in [368], autonomous mobile robots have been controlled navigationally by A new Quantum-inspired Reinforcement Learning (QIRL) method. According to Markovian tests, the QIRL method is better than traditional reinforcement learning in learning and initial states. Likewise, In [369], authors have been presented Quantum-inspired Fuzzy Based Neural Network (Q-FNN) model that is new in learning for challenging two-class classification. This model is much better for accuracy, sensitivity, and specificity.

### 6.5 Bio-inspired AI

In [370], bio-inspired representation learning is said to combine low-level contrast and high-level semantic features in order to generate a visual attention map. As outlined in [371], a neural network can be used to train Bio-inspired features. Some such examples can be seen in [372] where bio-inspired technologies are used to simulate animal movements in aerial vehicles, and in [373] where it is used for autonomous navigation. In [374], bio-inspired metaheuristic algorithms are used for the detection of spam emails and a bio-inspired algorithm in [375] is used for optimizing the Internet of Things. Another optimization algorithm can be found in [376] where it is used for UAV planning.

In Figure 5, the left side of the figure represents the current state of Privacy-Preserving Cloud technology, whereas the right side shows the future for this technology. The arrows from Privacy-Preserving Cloud point towards other technologies with which it can join to create new technologies. The DNA symbol represents Bio Science. Privacy-Preserving Cloud joins with Bio Science to create Bio-Inspired Privacy-Preserving Cloud. The Atom symbol represents Quantum Science, which joins with Privacy-Preserving Cloud to create Quantum-Inspired Privacy-Preserving Cloud.

### 7 Conclusion

Over the course of this survey paper, we have highlighted the Ecosystem, Applications, Architecture, and Lifecycle of Privacy-Preserving Cloud Computing. By creating this survey paper, future researchers who would like to learn more about Privacy-Preserving Cloud can now use this
paper as a resource to strengthen their knowledge of the subject. Because of the benefits that Cloud Computing has provided, it is used in many fields. However, because of the high level of usage of Cloud Computing across so many industries and technologies, there is a large amount of sensitive data that is potentially exposed. Paying attention to this subject, there is a growing concern about privacy in Cloud Computing. Having looked at this issue, Privacy-Preserving Cloud Computing technologies and methods have emerged in order to provide security and privacy. To recap the main points, current surveys from 2010 have been reviewed, and the summary of them has been provided in the tables that can be found at the end of Section Two. Those tables indicate whether the survey focuses on privacy or draws a future roadmap or the cloud computing has been reviewed in a specific application. Furthermore, Design, Verification, Implementation, and Evaluation that are categorized as the four stages of the Life Cycle of the Privacy-Preserving Cloud system have been reviewed. The layered of a cloud computing system is also detailed in order to explain the systems that work together in order to make sure that a cloud system can stay private. Moreover, the benefits of Privacy-Preserving Cloud Computing have been observed in the ecosystem. The future road map that consists Quantum-Inspired AI and Bio-Inspired AI have been presented in this paper. We would encourage researchers wishing to continue our work to study these areas further as the technology develops in the future. Using these new fields, the ways in which cloud computing can be used as a tool can increase in even greater numbers.

References

[1] S. Tang, C. Yu, and Y. Li, “Fairness-efficiency scheduling for cloud computing with soft fairness guarantees,” IEEE Transactions on Cloud Computing (Early Access Article), 2020.

[2] J. Lai, F. Guo, W. Susilo, X. Huang, P. Jiang, and F. Zhang, “Data access control in cloud computing: Flexible and receiver extendable,” IEEE Transactions on Services Computing (Early Access Article), 2021.

[3] Z. Yang, B. Liang, and W. Ji, “An intelligent end-edge-cloud architecture for visual iot assisted healthcare systems,” IEEE Internet of Things Journal (Early Access Article), pp. 1–1, 2021.

[4] Y. Zhang, Y. Sun, Y. Sun, R. Jin, K. Lin, K. Lin, W. Liu, and W. Liu, “High-performance isolation computing technology for smart iot healthcare in cloud environments,” IEEE Internet of Things Journal (Early Access Article), pp. 1–1, 2021.

[5] M. Papa, V. Mattioli, M. Montopoli, D. Casella, B. Rydberg, and F. S. Marzano, “Investigating spaceborne millimeter-wave ice cloud imager geolocation using landmark targets and frequency-scaling approach,” IEEE Transactions on Geoscience and Remote Sensing (Early Access Article), pp. 1–1, 2021.

[6] M. Pan, Y. Li, Z.-L. Zhang, and J. Luo, “Scs: Smart cloud computing system with shared autonomous vehicles,” IEEE Transactions on Big Data (Early Access Article), pp. 1–1, 2020.

[7] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, “Enabling drones in the internet of things with decentralized blockchain-based security,” IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6406–6415, 2020.

[8] Y. Zhang and H.-Y. Wei, “Risk-aware cloud-edge computing framework for delay-sensitive industrial iots,” IEEE Transactions on Network and Service Management (Early Access Article), pp. 1–1, 2021.

[9] I. M. Ali, K. M. Sallam, N. Moustafa, R. Chakraborty, M. J. Ryan, and K.-K. R. Choo, “An automated task scheduling model using non-dominated sorting genetic algorithm ii for fog-cloud systems,” IEEE Transactions on Cloud Computing (Early Access Article), pp. 1–1, 2021.

[10] M. Aazam, S. U. Islam, S. T. Lone, and A. Abbas, “Cloud of things (cot): Cloud-fog-iot task offloading for sustainable internet of things,” IEEE Transactions on Sustainable Computing (Early Access Article), pp. 1–1, 2020.

[11] R. M. A. H. ur rehman, M. Liaqat, A. H. M. Aman, S. H. A. Hamid, R. L. Ali, J. Shuja, and M. K. Khan, “Sensor cloud frameworks: State-of-the-art, taxonomy, and research issues,” IEEE Sensors Journal (Early Access Article), pp. 1–1, 2021.

[12] X. Jiang, J. Ni, J. Wu, and X. Yang, “A cloud big-data-driven dynamics control approach for unmanned ground vehicles for safety improving,” IEEE Intelligent Transportation Systems Magazine (Early Access Article), pp. 1–1, 2021.

[13] X. Wang, C. Xu, K. Wang, F. Yan, and D. Zhao, “Memory scaling of cloud-based big data systems: A hybrid approach,” IEEE Transactions on Big Data (Early Access Article), pp. 1–1, 2020.

[14] T. S. Chang and T.-H. Chen, “Rangeseq: Range-aware real time segmentation of 3d lidar point clouds,” IEEE Transactions on Intelligent Vehicles (Early Access Article), pp. 1–1, 2021.

[15] P. Zhao and G. Dan, “Joint resource dimensioning and placement for dependable virtualized services in mobile edge clouds,” IEEE Transactions on Mobile Computing (Early Access Article), pp. 1–1, 2021.

[16] T. Sun, G. Liu, R. Li, S. Liu, S. Zhu, and B. Zeng, “Quadratic terascale based point-to-surface 3d representation for deep learning of point cloud,” IEEE Transactions on Circuits and Systems for Video Technology (Early Access Article), pp. 1–1, 2021.

[17] Z. Su, Y. Wang, T. Luan, N. Zhang, F. Li, T. Chen, and H. Cao, “Secure and efficient federated learning for smart grid with edge-cloud collaboration,” IEEE Transactions on Industrial Informatics (Early Access Article), pp. 1–1, 2021.

[18] G. J. Portella, G. N. Rodrigues, E. Y. Nakano, A. Boukerche, and A. C. M. Melo, “A novel statistical and neural network combined approach for the cloud spot market,” IEEE Transactions on Cloud Computing (Early Access Article), pp. 1–1, 2021.

[19] M. S. Al-Abiad, A. Douik, S. Sorour, and J. Hossain, “Throughput and energy efficient coordinated multi-access in multi-clouds,” IEEE Transactions on Mobile Computing (Early Access Article), pp. 1–1, 2020.

[20] X. Tang, “Reliability-aware cost-efficient scientific workflows scheduling strategy on multi-cloud systems,” IEEE Transactions on Cloud Computing (Early Access Article), pp. 1–1, 2021.

[21] B. Ray, A. Saha, S. Khatau, and S. Roy, “Proactive fault-tolerance technique to enhance reliability of cloud service in cloud federation environment,” IEEE Transactions on Cloud Computing (Early Access Article), pp. 1–1, 2020.

[22] C. Zhao, J. S. Gill, P. Pisu, and G. Comer, “Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing,” IEEE Transactions on Intelligent Transportation Systems (Early Access Article), pp. 1–1, 2021.

[23] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoud, H. Karimipour, and G. Srivastava, “Block hunter: Federated...
learning for cyber threat hunting in blockchain-based iot networks,” IEEE Transactions on Industrial Informatics, pp. 1–1, 2022.

[24] D. Cotorome, L. D. Simone, P. Liguori, and R. Natella, “Fault injection analytics: A novel approach to discover failure modes in cloud-computing systems,” IEEE Transactions on Dependable and Secure Computing (Early Access Article), pp. 1–1, 2021.

[25] Y. Zhang, C. Xu, N. Cheng, and X. S. Shen, “Secure password-protected encryption key for deduplicated cloud storage systems,” IEEE Transactions on Dependable and Secure Computing (Early Access Article), pp. 1–1, 2021.

[26] H. Xiong, X. Huang, M. Yang, L. Wang, and S. Yu, “Unbounded and efficient revocable attribute-based encryption with adaptive secret key for cloud environment,” IEEE Internet of Things Journal (Early Access Article), pp. 1–1, 2021.

[27] A. Sultangazin and P. Tabuada, “Symmetries and isomorphisms for privacy in control over the cloud,” IEEE Transactions on Automatic Control, vol. 66, no. 2, pp. 538–549, 2021.

[28] A. Alabdulatif, I. Khalil, A. Y. Zomaya, Z. Tari, and X. Yi, “Fully homomorphic based privacy-preserving distributed expectation maximization on cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 11, pp. 2660–2681, 2020.

[29] S. Nakhodchi, B. Zolfaghari, A. Yazdinejad, and A. Dehghan, “Steeleeye: An application-layer attack detection and attribution model in industrial control systems using semi-deep learning,” in 2021 18th International Conference on Privacy, Security and Trust (PST). IEEE, 2021, pp. 1–8.

[30] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication and attestation of distributed patients in hospital networks using blockchain," IEEE journal of biomedical and health informatics, vol. 24, no. 8, pp. 2146–2156, 2020.

[31] A. Yazdinejad, R. M. Parizi, A. Bohlooli, A. Dehghantanha, and K.-K. R. Choo, “A high-performance framework for a network programmable packet processor using p4 and fpga,” Journal of Systems and Computer Applications, vol. 136, p. 102564, 2020.

[32] A. A. - M. A. S. Elameer, “A review in security issues and challenges on mobile cloud computing (mcc),” in Proceedings of 1st Annual International Conference on Information and Sciences (AIICS), Fallujah, Iraq, November 2018.

[33] A. K. B. S. M., “A review on challenges of security for secure data storage in cloud,” in Proceedings of International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, Tamilnadu, India, November 1, 2019.

[34] A. B. S. A-Z. R. A.-S. A. Rodan, “Storage as a service (staaS) security challenges and solutions in cloud computing environment: An evaluation review,” in Proceedings of Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, November 2019.

[35] A. M. S. P. R. G. S. Nath, “Cloud computing security issues & challenges: A review,” in Proceedings of International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, January 2020.

[36] S. S. P. Sudhish, “Security in cloud computing systems: A review of challenges and solutions for security in distributed computing environments,” in Proceedings of 9th National Systems Conference (NSC), Greater Noida, India, December 2015.

[37] A. N. D. Gupta, “A review on different security issues and challenges in cloud computing,” in Proceedings of International Conference on Computing, Power and Communication Technologies (ICUCCT), Greater Noida, India, September 2018.

[38] C. K. G. S. G. S. R. S. Bhat, “Security issues and challenges in cloud computing: A mirror review,” in Proceedings of International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, December 2019.

[39] R. K. J. Kaur, “Cloud computing security issues and its solution: A review,” in Proceedings of 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, March 2015.

[40] J. G. S. M. Sharma, “Cloud computing and its security issues — a review,” in Proceedings of Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hele, China, July 2014.

[41] N. C. Paxton, “Cloud security: A review of current issues and proposed solutions,” in Proceedings of IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), Pittsburgh, PA, USA, November 2016.

[42] I. I. M. Daneva, “Cloud computing security requirements: A systematic review,” in Proceedings of Sixth International Conference on Research Challenges in Information Science (RCIS), Valencia, Spain, 2012.

[43] T. A. P. S. P. A. T. Bhole, “A review on contemporary security issues of cloud computing,” in Proceedings of 1st International Conference on Intelligent Systems and Information Management (ICSIM), Aurangabad, India, October 2017.

[44] R. D. V. Kute, “A review paper on security concerns in cloud computing and proposed security models,” in Proceedings of International Conference on Emerging Trends in Information Technology and Engineering (ET-ETTE), Velbare, India, 2020.

[45] Y. B. Z. Y. B. Bahli, “Key topics in cloud computing security: A systematic literature review,” in Proceedings of 2nd International Conference on Information Security and Science (ICISS), Seoul, Korea (South), December 2015.

[46] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, “An energy-efficient sdn controller architecture for iot networks with blockchain-based security,” IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 625–638, 2020.

[47] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, “Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks,” IEEE Transactions on Network Science and Engineering, 2019.

[48] K. L. C. C. J. G. Q. L. Y. Gao, “A review of research on security of cloud service platform in medical environment,” in Proceedings of IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), Yilan, Taiwan, May 2019.

[49] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, “An efficient packet parser architecture for software-defined 5g networks,” Physical Communication, vol. 53, p. 101657, 2022.

[50] X. N. H. Soo, “Security in the cloud computing: A review,” in Proceedings of 2012 2nd International Conference on Computer Science and Network Technology, Changchun, China, December 2012.

[51] N. P. E. D. N. V. C. Lambrinoudakis, “It’s all in the cloud: Reviewing cloud security,” in Proceedings of IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, Vietri sul Mare, Italy, December 2013.

[52] G. S. V. A. G. Suganya, “A comprehensive review on cloud computing security,” in Proceedings of International Conference on Innovations in Information, Embedded and Communication Systems (ICIECS), Coimbatore, India, March 2017.

[53] V. B. P. K. B. P. Lohani, “A review of security of the cloud service platform in medical environment,” in Proceedings of International Conference on Innotation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, February 2016.

[54] S. N. S. A. G. F. D. Hutchison, “The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586–2595, 2017.

[55] M. M. A. K. D. G. A. K. N. S. P. A. Z. M. A. P. Mahmud, “Applications and evaluations of bio-inspired approaches in cloud security: A review,” IEEE Access, vol. 8, pp. 180799–180814, 2020.

[56] P. J. D. R. S. Patidar, “A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment,” in Proceedings of World Congress on Information and Communication Technologies, Mumbai, India, December 2011.

[57] B. G. A. B. P. Haller, “A survey on cloud-based software platforms to implement secure smart grids,” in Proceedings of 49th International Universities Power Engineering Conference (UPEC), Cluj-Napoca, Romania, September 2014.

[58] F. K. S. Y. F. X. Y. Yi, “Online soc estimation for li-ion batteries: A survey explore the distributed secure cloud management to battery packs,” in Proceedings of 12th IEEE Conference on Industrial Electronics and Applications (ICIEA), Siem Reap, Cambodia, June 2017.

[59] N. A. A. K. M. A. Shibli, “Survey on secure live virtual machine (vm) migration in cloud,” in Proceedings of 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, December 2013.

[60] H. S. K. Aida, “A hybrid and secure mechanism to execute parameter survey applications on local and public cloud resources,” in Proceedings of IEEE Second International Conference on
J. Zhou, X. Lin, X. Dong, and Z. Cao, “Psmpa: Patient self-
L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang, “An efficient
X. Ye, “Privacy preserving and delegated access control for cloud
H. Liu, H. Ning, Q. Xiong, and L. T. Yang, “Shared author-
Q. Huang, W. Yue, Y. Yang, and L. Chen, “P2gt: Fine-grained genomic data access control with privacy-preserving testing in cloud computing,” (Early Access Article), pp. 1–1, 2021.
X. Ye, “Privacy preserving and delegated access control for cloud applications,” Tsinghua Science and Technology, vol. 21, no. 1, pp. 40–54, 2016.
Q. Huang, W. Yue, Y. Yang, and L. Chen, “Psmpa: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed-healthcare healthcare cloud computing system,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 6, pp. 1693–1703, 2015.
H.-Y. Lin, “Traceable anonymous authentication and key exchange protocol for privacy-aware cloud environments,” IEEE Access, vol. 13, no. 1, pp. 805–815, 2021.
Q. Lin, Y. Tian, Y. Zhang, L. Shen, and J. Guo, “Efficient privacy-preserving access control of multimodal multimedia data in cloud computing,” IEEE Access, vol. 7, pp. 131 534–131 542, 2019.
M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public clouds,” IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2268–2280, 2014.
Y. Xiong, R. Li, D. Shao, F. Yin, and H. Zhu, “Achieving practical symmetric searchable encryption with search pattern privacy over cloud,” IEEE Transactions on Services Computing (Early Access Article), pp. 1–1, 2020.
K. Gai, M. Qiu, and H. Zhao, “Privacy-preserving data encryption strategy for big data in mobile cloud computing,” IEEE Transactions on Big Data, vol. 7, no. 4, pp. 678–688, 2021.
Q. Lin, T. Huang, A. A. Yavuz, and J. G. Merchan, “A secure searchable encryption framework for privacy-critical cloud storage services,” IEEE Transactions on Services Computing (Early Access Article), pp. 1–1, 2019.
Y. Lu, J. Li, and Y. Zhang, “Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted iot,” IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2553–2562, 2020.
H. Cheng, C. Rong, M. Qian, and W. Wang, “Accountable privacy-preserving mechanism for cloud computing based on identity-based encryption,” IEEE Access, vol. 6, pp. 37 869–37 882, 2018.
Y. Yang, X. Chen, H. Chen, and X. Du, “Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing,” IEEE Access, vol. 6, pp. 18 009–18 021, 2018.
M. Zhang, Y. Chen, and J. Huang, “Se-pffm: A searchable encryption scheme supporting privacy-preserving fuzzy multi-keyword in cloud systems,” IEEE Systems Journal, vol. 2, no. 15, pp. 2980–2988, 2021.
L. Zhang, Y. Zhang, and H. Ma, “Privacy-preserving and dynamic multi-attribute conjunctive keyword search over encrypted cloud data,” IEEE Access, vol. 6, pp. 34 214–34 225, 2018.
S. Sharma, J. Powers, and K. Chen, “Privategraph: Privacy-preserving spectral analysis of encrypted graphs in the cloud,” IEEE Transactions on Knowledge and Data Engineering, vol. 15, no. 1, pp. 1–1, 2021.
S. Qiu, B. Wang, M. Li, J. Liu, and Y. Shi, “Toward practical privacy-preserving frequent itemset mining on encrypted cloud data,” IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 1–1, 2020.
K. Liang, X. Huang, F. Guo, and J. K. Liu, “Privacy-preserving and regular language search over encrypted cloud data,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2365–2376, 2016.
J. Feng, L. T. Yang, Q. Zhu, and K.-K. R. Choo, “Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 4, pp. 857–866, 2020.
C.-C. Chang, C.-T. Li, and Y.-Q. Shi, “Privacy-aware reversible watermarking in cloud computing environments,” IEEE Access, vol. 6, pp. 70 720–70 733, 2018.
J. Li, H. Yan, and Y. Zhang, “Identity-based privacy preserving remote data integrity checking for cloud storage,” IEEE Systems Journal, vol. 15, no. 1, pp. 577–585, 2021.
Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, 2017.
X. Gao, J. Yu, Y. Chang, H. Wang, and J. Fan, “Checking only when it is necessary: Enabling integrity auditing based on the keyword with sensitive information privacy for encrypted cloud data,” IEEE Transactions on Dependable and Secure Computing (Early Access Article), pp. 1–1, 2021.
B. Shao, G. Bian, Y. Wang, S. Su, and C. Guo, “Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment,” IEEE Access, vol. 6, pp. 43 785–43 797, 2018.
H. Yan and W. Gui, “Efficient identity-based public integrity auditing of shared data in cloud storage with user privacy preserving,” IEEE Access, vol. 9, pp. 45 822–45 831, 2021.
P. J. Sun, “Research on the tradeoff between privacy and trust in cloud computing,” IEEE Access, vol. 7, pp. 10 428–10 441, 2019.
[371] M. Xu, F. Chen, L. Li, C. Shen, P. Lv, B. Zhou, and R. Ji, “Bio-inspired deep attribute learning towards facial aesthetic prediction,” IEEE Transactions on Affective Computing, vol. 12, no. 1, pp. 227–238, 2021.

[372] Z. Tu, F. Fei, and X. Deng, “Bio-inspired rapid escape and tight body flip on an at-scale flapping wing hummingbird robot via reinforcement learning,” IEEE Transactions on Robotics, vol. 37, no. 5, pp. 1742–1751, 2021.

[373] H. Lehnert, M. Araya, R. Carrasco-Davis, and M.-J. Escobar, “Bio-inspired deep reinforcement learning for autonomous navigation of artificial agents,” IEEE Latin America Transactions, vol. 17, no. 12, pp. 2037–2044, 2019.

[374] S. Gibson, B. Issac, L. Zhang, and S. M. Jacob, “Detecting spam email with machine learning optimized with bio-inspired metaheuristic algorithms,” IEEE Access, vol. 8, pp. 187914–187932, 2020.

[375] Z. Yang, Y. Jin, and K. Hao, “A bio-inspired self-learning co-evolutionary dynamic multiobjective optimization algorithm for internet of things services,” IEEE Transactions on Evolutionary Computation, vol. 23, no. 4, pp. 675–688, 2019.

[376] H. Duan, P. Li, Y. Shi, X. Zhang, and C. Sun, “Interactive learning environment for bio-inspired optimization algorithms for uav path planning,” IEEE Transactions on Education, vol. 58, no. 4, pp. 276–281, 2015.