# Cloud Computing Information Protection Security Model Using a Whale-Optimized Swarm-Based Glowworm Structure

**Yogita Deepak Sinkar ***

## Abstract

Privacy-Preserving is a modern technology, cloud computing has a wide range of applications. Since it enables increased security, portability, and flexibility, cloud computing is crucial. Similar to this, maintaining privacy in cloud computing is crucial to maintaining the integrity of data kept there. This review article on privacy-preserving cloud services can open the door for further investigation into related topics. In addition to analysing the latest scenario in research in this field, this study establishes a layered structure, a life cycle, and an environment for privacy-preserving cloud environments. The data retained for security is created using the filtering matrix, with the filter vector focusing on the integration of the Glowworm Swarm Optimization (GSO), Glowworm Swarm Whale Optimization Algorithm (GWOA), and Whale Optimization Algorithm (WOA).

The data stored resulting in privacy is subjected to the data storage system, where the stored data is registered. Instead, the retained data is stored in the information environment's information management system to allow user access with greater privacy and utility.



**Key Words:** Cloud computing, security, Glowworm Swarm Optimization (GSO), Glowworm Swarm Whale Optimization Algorithm (GWOA), and Whale Optimization Algorithm (WOA), Trend Analysis, Future Roadmap

**DOI Number: 10.14704/nq.2022.20.8.NQ44715** **NeuroQuantology 2022; 20(8):6883-6892**

## 1. Introduction

The scientific community has recently shown a lot of interest in cloud computing [1] [2]. It is employed in a wide range of applications, including geospatial technologies [5], autonomous cars [6–7], and healthcare [3–4]. Since cloud technology is actively integrating with other technical disciplines including edge [8] and fog computing [9], the Internet of Things (IoT) [10], sensor technology [11], and big data [12] [13], it plays a vital role in contemporary technology. Edge computing is described as a distributed computing topology in which data is stored and processed near to its source. Distributed system architecture that sits in the space between a data source and a cloud is referred to as fog computing. Real-time computing [14], virtualization [15], and artificial intelligence [16] are only a few examples of enabling technologies that underpin cloud computing. Performance [19], dependability [20], and fault tolerance [21] are only a few of the design goals that are taken into account while designing a cloud computing system. Cloud computing experts have been particularly worried about a variety of security issues, such as attack resilience [22], [23] [24] and secrecy [25] [26]. But when it comes to cloud computing, privacy seems to be the most important security factor. In this study, we initially set up an architecture for big data, the Internet of Things (IoT), the smart home, apps, healthcare, automotive technologies, social networking, and data centres for privacy-preserving cloud computing. Then, a life cycle was created and examined at each stage: design, verification, implementation, and deployment. The following stage involves creating a layered architecture with privacy-preserving computing, services, and infrastructure.

**Corresponding author:** Yogita Deepak Sinkar
**Address:** [1,2,3] SVPM College of Engineering, Malegaon(Bk.), Tal. Baramati, Pune, Maharashtra, India
E-mail: gtsinkar186@gmail.com

Finally, we lay forth a potential roadmap for quantum- and bio-inspired artificial intelligence. As these new technologies advance, we hope that by presenting our work, we might inspire others to continue researching these issues. It needs to be highlighted that even though analogous survey studies may already exist, they have limitations that drive our work in this study. We want to provide the most thorough coverage of privacy-preserving cloud computing that is feasible.

The remainder of this essay is structured as follows. Existing surveys are summarised in Section 2. The applications and technology that make up the cloud computing ecosystem are described in Section 3. The whole four-stage life cycle of a cloud system is described in Section 4. The cloud computing roadmap for the future is presented in Section 5, the conclusion is present.

## 2. Current Studies

Numerous surveys have been conducted about cloud computing security.

However, some of them are too old for such a developing field of study. Others don't emphasise cloud computing's privacy [27]. Some current studies only look at a few specific uses of cloud computing, and some of them fall short of creating a vision for the future. Our efforts in this study are motivated by these flaws. Cloud Service Providers should take the necessary actions to address the security and privacy issues that come with data storage [28]. Previous investigations and their results have been examined in this section. Despite the fact that Mobile Cloud Computing (MCC) offers a means of accommodating our demands for numerous resources on portable devices, there are security and confidentiality issues. To that goal, security concerns and difficulties in mobile cloud computing have been examined in [29]. [30] has researched availability, data integrity (DI), and data confidentiality (DC), all of which are crucial for cloud storage. Storage as a Service is another well-known and well-liked technology that cloud computing has made available to businesses and individual consumers (StaaS). According to developing concerns about STaaS, the security and privacy risks have been laid forth in [31]. The primary activity that has been examined in [32], [33] and for which writers have provided solutions is the reduction of security threats in cloud computing. Since it is unclear how the data is kept and regulated, these issues were further investigated in [34] and [35]. The Pixel key pattern and Image Steganography approaches have been presented in [36] to address insurmountable data security difficulties in cloud computing, however in [37], possible problems with user data access and privacy have been investigated in an effort to draw urgent attention. Data breaches, account takeovers, and multitenancy are three dangers that led to security problems that were examined in [38], and it was expected that cloud computing would become more common if these problems were resolved. Although the needs and solutions for cloud computing security were thoroughly covered in [39], that book's publication year makes its answer potentially outdated for today's technology given its rapid advancement. Similar approaches have been put out in [40] and [41] to get around three main categories—cryptographic, data storage, and data semantics—of cloud computing challenges.

Additionally, [42] gave information that consumers should be aware of to estimate dangers associated with maintaining their data, although user privacy was not violated. Blockchain with cloud computing technology developments have been explored in [43, 44], and it was noted how both technologies may work together to improve one another's shortcomings. The authors of [45] emphasised the security risk posed by cloud service platforms in the medical industry and also offered pertinent remedies. Protecting user as well as data security and privacy was discussed in [46] along with a mechanism that can deny access to unauthorised users.

In this area, we've evaluated the recent studies on cloud computing's infrastructure and security concept. The first subsection of this also section, we look into the overall security idea in the cloud. informatics, and the sub - sections that follow, privacy, and Data storage, transmission, and authentication protocols have all been studied. Additionally, steganographic and encryption techniques, hazards associated with Secure Data Sharing have been examined in consequently, current surveys. the parts that follow, authentication as well as security audits, data provenance, and difficulties, dangers, threats, and assaults have been investigated.

In [46], the authors examined a number of studies and noted a number of security flaws that had an impact on the cloud computing environment. They come to the conclusion that the blockchain allays service providers' and consumers' security worries, much as how [47] writers suggested Advanced Security Measures and Practices to enhance the



design of present technology to address security risks and difficulties. In contrast to which described the vulnerabilities, assaults, and threats connected to cloud services and infrastructuresevaluated the structure of the blockchain method and offered a secure way of blockchain that may address security concerns and hazards. Additionally, examined the advantages and disadvantages of current security techniques, and the authors argued potential capabilities in the security of cloud services in order to overcome drawbacks in contrast to [51], where the authors conducted a thorough investigation into the security of cloud infrastructure and provided a method that can reduce problems and risks at that time. However, this approach would not work given the year the paper was done. Additionally, due to the widespread use of cloud services, authors in [52] conducted a thorough analysis on papers published between 2019 and 2020, as opposed to [53], where risk management strategies that are distinct from those in IT enterprises have been examined in cloud systems, and authors have technically shown its effectiveness in cloud security challenges. It has been determined that Intrusion Detection Systems' (IDS) accuracy assaults in [54] that were examined as being cloud-based harmful, and the authors have described IDS that uses numerous methods. detection in the cloud to increase its effectiveness while in the present security architecture has been examined to emphasise the negative aspects, shortcomings, and writers new Intrusion Detection Systems in place (IDS) and Prevention System (IPS), which enhances virtual networks.

## 3. Clouds Based On Iot And Iot Clouds

These days, Internet of Things (IoT) devices are widely used since there is no denying their benefits, but when it comes to protecting private data, the security method has been crucial [55]. IoT and cloud computing were discussed in this section because they have grown to be so entwined and nearly inseparable. While the security of data in the Internet of Things (IoT) integrated with Cloud base internet has only been analysed in [56], several infrastructures of IoT were effectively analysed from the perspective of security, and risks and threats in the Internet of Things have been highlighted. Authors observed them by conducting the man-in-the-middle attack between end devices sensor and service providers. Additionally, [57] has demonstrated the security issues associated with archiving and gathering data from IoT devices that demand immediate attention. In addition, the authors developed some potential solutions in place of [58] the analysis of threats, risks, and vulnerabilities of Supervisory Control and Data Acquisition (SCADA) systems and the reporting of some critical issues. An application used for cutting-edge medical technology is called WebSCADA.

Utilising machine learning for cloud security, including its difficulties and estimates of its accuracy [59]. How well face recognition technology works in the cloud. [60] has examined the data security environment. The primary methods for detecting and recognising cloud data behaviour elements that can aid in creating a secure data deployed surveillance system in a cloud environment that will safeguard saved data from network trespassers and security for data. You're going to need a table here. One of the aforementioned surveys is assigned to each row in the table. Each row's first column includes a citation to the relevant survey study. The survey's publication year is listed in the second row. The third row indicates if the survey emphasises cloud computing privacy (Yes/No). The survey offers a future roadmap is indicated in the fourth column (Yes/No). If a specific application of cloud computing is being studied, it is indicated in the fifth column (Yes/No).



In Figure 1, enabling sciences and technologies including optimization [61], blockchain, PUF, edge computing, fog computing, and wireless sensor networks [62] serve as the ecosystem's foundation. The Enabling Security Mechanism, which includes Anonymization, Privacy-Preserving Authentication, Privacy-Preserving Access Control, Privacy-Preserving Cryptography, and Privacy-Preserving Watermarking, are supported by pillars that stand on top of this base.

Last but not least, Applications lie on top of the structure since the technologies below them make them possible. Data centres, IoT, Smart Homes, Big Data, Industrial Environments, Vehicle Technology, Healthcare, and Social Networking are a few of these applications.

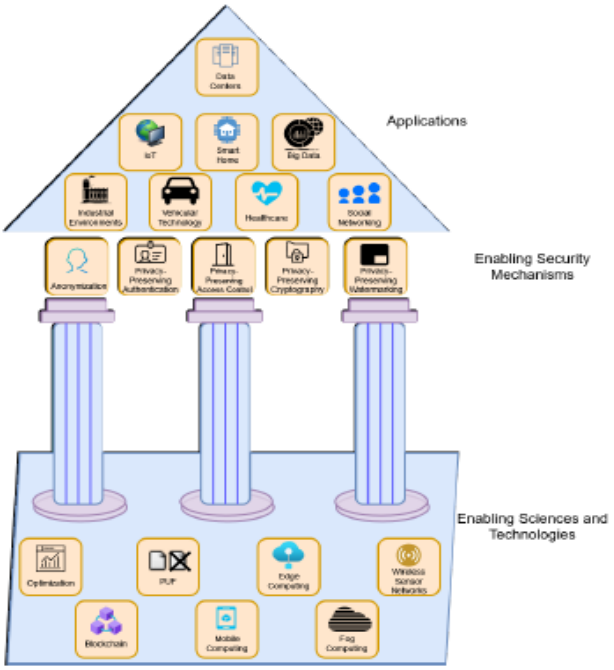


**Fig.1 Ecosystem**

We discuss the numerous uses for this technology and how they could be advantageous in these fields. The technology that makes it possible for these apps to run is discussed. There are several technologies and procedures that may be employed to protect these ecosystems. Several of these security techniques are covered. This study will finally examine the security issues associated with employing a cloud-based ecosystem.

## 3.1 Applications

### 3.1.1 Industrial Environments and IIoT

According to [69], [70], the Industrial Internet of Things is a subset of the Internet of Things that aims to maximise industrial output by giving equipment more connectivity and intelligence. The Internet of Things in the healthcare sector uses devices that can more efficiently monitor patients and gather their health data to improve services for patients.

### 3.1.2 Transportation Technology

The ourline of [71] illustrates how the integration of cloud technology with automobiles enables the use of sensors, cameras, and wireless transceivers to enhance traffic flow. According to the authors of it also aids in building a network for autonomous cars so that data may be analysed and stored remotely. The authors of proposed using this technology to enable automobiles to receive adverts via a cloud network for vehicular advertisement distribution. According to, vehicular cloud technology enables the offloading of more sophisticated calculations, such as traffic analysis and route optimization, to parked automobiles that are not required to carry out computations of a higher priority.

### 3.1.3 Medical

The authors claim that the fast expansion of healthcare data that supports eHealthcare has been made possible by cloud-based data-driven healthcare monitoring services. Some networks will employ a blind cloud structure that substitutes patient identities with produced pseudo-identities in order to secure this medical data. The authors of [72] explain how this enables the storage and analysis of unidentifiable data.

According to searchable encryption techniques may also be utilised to allow for the privacy-preserving search of health data. A technique called searchable symmetric encryption (SSE) enables users to host encrypted data discreetly on the server or other storage of a third party. As a result, the cloud service provider (CSP) does not have access to them; instead, CSP gives users access to the encrypted data when they want it.



### 3.1.4 Social Networking

It is vitally crucial to keep this data safe, as it is mentioned in how many social networking sites store user information on cloud services. User data may be protected using methods like homomorphic encryption, oblivious transmission, and secret sharing. Users can edit or examine their encrypted data using homomorphic encryption without needing to decode it.

### 3.1.5 IoT

The Internet of Things is now better able to handle enormous volumes of data thanks to cloud technologies. A user can communicate encrypted data using an identity-based encryption approach described in thanks to flexible privacy-preserving data sharing. Additionally, scalability, forward security, and privacy may be ensured via a network attestation technique as described in [73].

### 3.1.6 Smart Home

Smart homes that protect privacy can link one house to a cloud platform that collects data from every other house on the network. According to the ourline of this data may be utilised to improve house

security and energy efficiency, which will improve a resident's quality of life.

### 3.1.7 Big Data

Mobile networks are responsible for the continual and quick generation of data. Big data stream is the term used by the authors in to describe this data creation. The authors of describe how cloud computing can provide a scalable infrastructure to analyse and aggregate this enormous data stream.

### 3.1.8 Data Centers

Geo-distributed cloud data centres store and transmit enormous volumes of data daily, as described by the authors of [153]. Data transfer across borders may be challenging due to regional variations in privacy legislation.

Data centres need to make sure they adhere to the stringent data standards put in place by nations and organisations, such the General Data Protection Regulation (GDPR).

## 4. Ai In A Cloud That Preserves Privacy

The data uploaded from federated learning has been endangered by attackers despite the fact that federated learning has been developed to protect data privacy . Similar to [where the authors established an encryption method called BGV that encrypts data and uses cloud servers techniques to train for the deep computing model, authors in have provided a new methodology to maintain data privacy on cloud-edge learning systems.

In addition, the secure-centralized-computation-privacypreserving reinforcement learning method was introduced to safeguard user data privacy by implementing a completely homomorphic encryption system in a cloud computing infrastructure.

A deep neural network architecture dubbed MSCryptoNet that operates on a fully homomorphic cryptosystem in the privacy-preservation context was presented in order to give improved complexity and security. However, when it comes to machine learning, there is a rising worry regarding the security and privacy of data. As opposed, where the authors created a framework that organises sparse coding in edge and cloud networks, [350] presents a secure cloud-intelligent network architecture that protects data privacy. They used classification in this framework to identify data noise and error. Distributed deep learning (DDL) is also one of the most well-liked applications in the fog-cloud computing environment due to its effectiveness and scalability.

However, there are issues with employing DLL in fog-cloud computing, such as safeguarding user privacy during training and validating users' identities that have been falsified by outside attackers. The authors of have developed a secure and privacy-preserving DDL (SPDDL) for fog-cloud computing in response to these issues. The generation of large amounts of data is another issue with the internet of things (IoT). In a two-layer double-projection deep computation model (DPDCM) for feature learning in huge data was introduced. The authors have also created a learning method for training the DPDCM.

However, how much data we utilise during the training phase affects our neural network learning results. No party wants to share people's private information with others, thus we need a solution if we wish to use another party's data collection. The authors' useful multiparty Back-Propagation neural network 15 learning method for arbitrarily partitioned data is detailed in .In this architecture, the Cloud performs the majority of actions on uploaded ciphertext and encrypted data. While the authors of have defended the privacy of user data that is utilised for training. The privacy-preserving deep learning approach, which they introduced, encrypts users' data using their public key. Furthermore, we are working with a date whose privacy and security are crucial in smart cities where urban amenities employ technology like smart health, parking, and transportation. For the purpose of resolving this issue in smart cities, the authors of presented a privacy-preserving autoencoder-based deep learning classifier on the Cloud. Additionally, homomorphic secure multi-party computation (SMC) or homomorphic encryption (HE) algorithms have been employed to provide data privacy while maintaining the security of cloud processes. Similar to where authors developed a framework for transformation network training in cooperation for privacy-preserving deep neural networks, writers claim supervised and unsupervised machine learning capabilities using neural networks on encrypted data. Users can train a transformation network using a model from a cloud provider utilising the framework in a safe setting. Additionally, because it violates users' privacy, enterprises should first delete Personally Identifiable Information (PII) before doing big data analysis. In order to protect data privacy, a Deep Neural Network (DNN) and Mondrian-based k-



anonymity framework has been proposed. Their analysis reveals that it was appropriate similarly, in which a new algorithm for DNN training/classification that filtered images to protect cloud base privacy was presented. Additionally, the authors have offered a cloud-based federated strategy that utilises numerous clouds with various distorted data sets and shows how DNN can be used to achieve adequate accuracy with the original dataset. As an alternative, a method that analyses pictures on client devices and is not dependent on a local Convolutional Neural Network (CNN) has been introduced .Serious privacy problems are another impact of CNN-based mobile Cloud apps that operate on raw picture data. Additionally, analyses the difficulties with time delay, energy usage, and privacy level in an Edge-Cloud Collaboration (ECC) scenario with several users. The Deep Q-Network (DQN), which reduces latency and energy costs while enhancing privacy, was also presented by the authors. The MDP balances cost and privacy level. However, data protection is a crucial step in the cloud environment. To offer security and data protection in the cloud context, introduces a Machine Learning and Probabilistic Analysis based Model (MLPAM). In addition, MLPAM includes a strong sharing strategy for minimising data leakage. To that aim, an increasing number of businesses have started using machine learning software for a variety of tasks, including threat detection. With the help of a privacy-aware deployment mechanism (PDM), which has been provided, we can ensure its correctness and effectiveness. This approach allows us to provide privacy, which is difficult in cyber-physical cloud systems (CPCSs).

### 4.1 Quantum-Inspired AI

To enable improved training and learning, processing a large and complicated dataset requires changing algorithms. The authors have presented a solution that is optimising using the quantum-inspired reinforcement learning (QiRL) method that enhances the performance of an uncrewed aerial vehicle from when it starts flying to its destination because the trajectory planning problem is one of the difficulties in a wireless uplink transmission scenario. Additionally, new training methods for deep reinforcement learning (DRL) to equilibrium exploration and exploitation have been introduced. Unlike the conventional technique, this algorithm draws its inspiration from quantum processing. Additionally, has a one-shot learning and self-convergent iterative learning model called IQMAM that is influenced by quantum mechanics. According to their investigation, the model can retain a constant memory capacity and dependable recall.

In contrast, a novel Quantum-inspired Reinforcement Learning (QiRL) technique has been used in [368] to navigate autonomous mobile robots. Markovian experiments show that the QiRL approach outperforms conventional reinforcement learning in learning and beginning states. Quantum-inspired Fuzzy Based Neural Network (Q-FNN) model, which is novel in learning for difficult two-class classification, has also been presented by the authors. The accuracy, sensitivity, and specificity of this model are significantly higher.

### 4.2 Bio-inspired AI

Claims that bio-inspired representation learning creates a visual attention map by fusing high-level semantic features with low-level contrast features. As described in Using a neural network, one may instruct bio-inspired features. You may find a few of these instances.where Technologies based on biology are employed to replicate animal motions. when employed for aerial vehicles, self-contained navigation. Using a bio-inspired metaheuristic. Spam email detection methods are utilised, and uses a bio-inspired method for improving the The Internet of Things Another potential optimization method is utilised for UAV planning ,where it may be found. Picture 5 portrays the future of Privacy-Preserving Cloud technology on the right side of the figure, while the left side depicts the technology's current condition.

The Privacy-Preserving Cloud's arrows indicate in the direction of other technologies that it can combine with to produce new technologies. The DNA sign stands for biological science.

Bio-Inspired Privacy-Preserving Cloud is created by combining Privacy-Preserving Cloud with Bio Science. The symbol for the atom stands for quantum science, which combines with privacy-preserving cloud to form quantum-inspired privacy-preserving cloud.

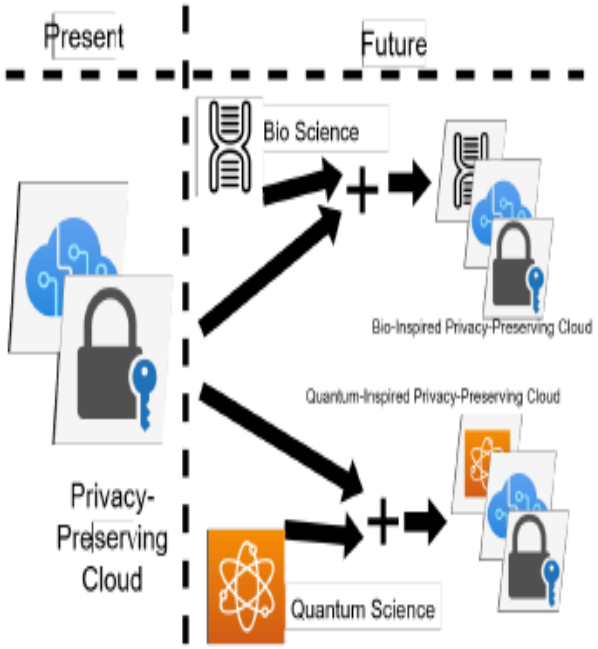


**Fig. 2. A bio-inspired and quantum-inspired AI-assisted privacy-preserving cloud is created when bioscience and quantum physics join forces.**

## 5. Conclusion

The Ecosystem, Applications, Architecture, and Lifecycle of Privacy-Preserving Cloud Computing have all been emphasised in this survey report. The advantages of cloud computing have led to its application in a variety of industries. However, a lot of sensitive data is potentially exposed due to the widespread use of cloud computing across several businesses and technologies. Regarding this topic, there is an increasing level of privacy issue with cloud computing. After considering this problem, privacy-preserving cloud computing technologies and procedures have evolved to offer security and privacy. Current surveys from 2010 have been evaluated in order to review the important topics, and the summary of them has been presented in the tables that can be found at the conclusion . The layers of a cloud computing system are also described in detail to clarify the interconnected technologies that guarantee a cloud system may remain private. Furthermore, the ecosystem has seen the advantages of privacy-preserving cloud computing. This study presents the future road map for quantum-inspired and bioinspired artificial intelligence. We would urge scholars who desire to carry on our work to look at these topics further in the future as technology advances. The applications for cloud computing as a tool might expand even further by utilising these new sectors.

## References

S. Tang, C. Yu, and Y. Li, "Fairness-efficiency scheduling for cloudcomputing with soft fairness guarantees," IEEE Transactions onCloud Computing (Early Access Article), 2020.

J. Lai, F. Guo, W. Susilo, X. Huang, P. Jiang, and F. Zhang,"Data access control in cloud computing: Flexible and receiverextendable," IEEE Transactions on Services Computing (Early AccessArticle), 2021.

Z. Yang, B. Liang, and W. Ji, "An intelligent end-edge-cloudarchitecture for visual iot assisted healthcare systems," IEEEInternet of Things Journal (Early Access Article), pp. 1–1, 2021.

Y. Zhang, Y. Sun, Y. Sun, R. Jin, K. Lin, K. Lin,W. Liu, andW. Liu,"High-performance isolation computing technology for smart iothealthcare in cloud environments," IEEE Internet of Things Journal(Early Access Article), pp. 1–1, 2021.

M. Papa, V. Mattioli, M. Montopoli, D. Casella, B. Rydberg, andF. S. Marzano, "Investigating spaceborne millimeter-wave icecloud imager geolocation using landmark targets and frequencyscalingapproach," IEEE Transactions on Geoscience and RemoteSensing (Early Access Article), pp. 1–1, 2021.

M. Pan, Y. Li, Z.-L. Zhang, and J. Luo, "Sccs: Smart cloudcommuting system with shared autonomous vehicles," IEEETransactions on Big Data (Early Access Article), pp. 1–1, 2020.

A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour,G. Srivastava, and M. Aledhari, "Enabling drones in the internetof things with decentralized blockchain-based security," IEEE nInternet of Things Journal, vol. 8, no. 8, pp. 6406–6415, 2020.

Y. Zhang and H.-Y. Wei, "Risk-aware cloud-edge computingframework for delay-sensitive industrial iots," IEEE Transactionson Network and Service Management (Early Access Article), pp. 1–1,2021.

I. M. Ali, K. M. Sallam, N. Moustafa, R. Chakraborty, M. J.Ryan, and K.-K. R. Choo, "An automated task scheduling modelusing non-dominated sorting genetic algorithm ii for fog-cloudsystems," IEEE Transactions on Cloud Computing (Early AccessArticle), pp. 1–1, 2021.

M. Aazam, S. U. Islam, S. T. Lone, and A. Abbas, "Cloud of things(cot): Cloud-fog-iot task offloading for sustainable internet ofthings," IEEE Transactions on Sustainable Computing (Early AccessArticle), pp. 1–1, 2020.

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 cloudframeworks: State-of-the-art, taxonomy, and research issues,"IEEE Sensors Journal (Early Access Article), pp. 1–1, 2021.

X. Jiang, J. Ni, J. Wu, and X. Yang, "A cloud big-data-drivendynamics control approach for unmanned ground vehicles forsafety improving," IEEE Intelligent Transportation Systems Magazine(Early Access Article), pp. 1–1, 2021.

X. Wang, C. Xu, K. Wang, F. Yan, and D. Zhao, "Memory scaling mof cloud-based big data systems: A hybrid approach," IEEETransactions on Big Data (Early Access Article), pp. 1–1, 2020.



T. S. Chang and T.-H. Chen, "Rangeseg: Range-aware real timesegmentation of 3d lidar point clouds," IEEE Transactions onIntelligent Vehicles (Early Access Article), pp. 1–1, 2021.

P. Zhao and G. Dan, "Joint resource dimensioning and placementfor dependable virtualized services in mobile edge clouds," IEEETransactions on Mobile Computing (Early Access Article), pp. 1–1,2021.

T. Sun, G. Liu, R. Li, S. Liu, S. Zhu, and B. Zeng, "Quadraticterms based point-to-surface 3d representation for deep learningof point cloud," IEEE Transactions on Circuits and Systems for VideoTechnology (Early Access Article), pp. 1–1, 2021.

Z. Su, Y. Wang, T. Luan, N. Zhang, F. Li, T. Chen, and H. Cao,"Secure and efficient federated learning for smart grid with edgecloudm collaboration," IEEE Transactions on Industrial Informatics(Early Access Article), pp. 1–1, 2021.

G. J. Portella, G. N. Rodrigues, E. Y. Nakano, A. Boukerche, andA. C. M. Melo, "A novel statistical and neural network combinedapproach for the cloud spot market," IEEE Transactions on CloudComputing (Early Access Article), pp. 1–1, 2021.

M. S. Al-Abiad, A. Douik, S. Sorour, and J. Hossain, "Throughputmaximization in cloud-radio access networks using cross-layernetwork coding," IEEE Transactions on Mobile Computing (EarlyAccess Article), pp. 1–1, 2020.

X. Tang, "Reliability-aware cost-efficient scientific workflowsscheduling strategy on multi-cloud systems," IEEE Transactionson Cloud Computing (Early Access Article), pp. 1–1, 2021.

B. Ray, A. Saha, S. Khatua, and S. Roy, "Proactive fault-tolerancetechnique to enhance reliability of cloud service in cloud federationenvironment," IEEE Transactions on Cloud Computing (EarlyAccess Article), pp. 1–1, 2020.

C. Zhao, J. S. Gill, P. Pisu, and G. Comert, "Detection of false datainjection attack in connected and automated vehicles via cloudbased msandboxing," IEEE Transactions on Intelligent TransportationSystems (Early Access Article), pp. 1–1, 2021.

A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh,H. Karimipour, and G. Srivastava, "Block hunter: Federatedlearning for cyber threat hunting in blockchain-based iiot networks,"IEEE Transactions on Industrial Informatics, pp. 1–1, 2022.

D. Cotroneo, L. D. Simone, P. Liguori, and R. Natella, "Faultinjection analytics: A novel approach to discover failure modes incloud-computing systems," IEEE Transactions on Dependable andSecure Computing (Early Access Article), pp. 1–1, 2020.

Y. Zhang, C. Xu, N. Cheng, and X. S. Shen, "Secure passwordprotectedencryption key for deduplicated cloud storage systems,"IEEE Transactions on Dependable and Secure Computing(Early Access Article), pp. 1–1, 2021.

H. Xiong, X. Huang, M. Yang, L. Wang, and S. Yu, "Unboundedand efficient revocable attribute-based encryption with adaptivesecurity for cloud-assisted internet of things," IEEE Internet ofThings Journal (Early Access Article), pp. 1–1, 2021.

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

A. Yazdinejad, R. M. Parizi, A. Bohlooli, A. Dehghantanha, andK.-K. R. Choo, "A high-performance framework for a networkprogrammable packet processor using p4 and fpga," Journal ofNetwork and Computer Applications, vol. 156, p. 102564, 2020.

S. A. . M. A. S. Elameer, "A review in security issues andchallenges on mobile cloud computing (mcc)," in Proceedings mof 1st Annual International Conference on Information and Sciences(AiCIS), Fallujah, Iraq, November 2018.

A. K. B. S. M, "A review on challenges of security for securedata storage in cloud," in Proceedings of International Conferenceon Smart Systems and Inventive Technology (ICSSIT), Tirunelveli,India, November 2019.

A. B. S. A.-Z. R. A.-S. A. Rodan, "Storage as a service (staas) securitychallenges and solutions in cloud computing environment:An evaluation review," in Proceedings of Sixth HCT InformationTechnology Trends (ITT), Ras Al Khaimah, United Arab Emirates,November 2019.

A. M. S. P. R. T. G. S. Nath, "Cloud computing security issues& challenges: A review," in Proceedings of International Conferenceon Computer Communication and Informatics (ICCCI), Coimbatore,India, January 2020.S. S. P. S. Sudhish, "Security in cloud computing systems: Areview of challenges and solutions for security in distributedcomputing environments," in Proceedings of 39th National SystemsConference (NSC), Greater Noida, India, December 2015.

A. N. D. Gupta, "A review on different security issues andchallenges in cloud computing," in Proceedings of InternationalConference on Computing, Power and Communication Technologies(GUCON), Greater Noida, India, September 2018.

C. K. G. S. G. S. R. S. Batth, "Security issues and challenges incloud computing: A mirror review," in Proceedings of InternationalConference on Computational Intelligence and Knowledge Economy(ICCIKE), Dubai, United Arab Emirates, December 2019.

R. K. J. Kaur, "Cloud computing security issues and its solution:A review," in Proceedings of 2nd International Conference on Computingfor Sustainable Global Development (INDIACom), New Delhi,India, March 2015.

J. G. S. M. Sharma, "Cloud computing and its security issues — areview," in Proceedings of Fifth International Conference on Computing,Communications and Networking Technologies (ICCCNT), Hefei,China, July 2014.

N. C. Paxton, "Cloud security: A review of current issues andproposed solutions," in Proceedings of IEEE 2nd International Conferenceon Collaboration and Internet Computing (CIC), Pittsburgh,PA, USA, November 2016.

I. I. M. Daneva, "Cloud computing security requirements: Asystematic review," in Proceedings of Sixth International Conferenceon Research Challenges in Information Science (RCIS), Valencia,Spain, 2012.

T. A. P. S. P. A. T. Bhole, "A review on contemporary securityissues of cloud computing," in Proceedings of 1st International Conferenceon Intelligent Systems and Information Management (ICISIM),Aurangabad, India, October 2017.

R. D. V. Kute, "A review paper on security concerns in cloudcomputing and proposed security models," in Proceedings of InternationalConference on Emerging



Trends in Information Technology mand Engineering (ic-ETITE), Vellore, India, 2020.

Y. B. Z. Y. B. Bahli, "Key topics in cloud computing security:A systematic literature review," in Proceedings of 2nd InternationalConference on Information Science and Security (ICISS), Seoul, Korea(South), December 2015.

A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient sdn controller architecture foriot networks with blockchain-based security," IEEE Transactionson Services Computing, vol. 13, no. 4, pp. 625–638, 2020.

A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo,"Blockchain-enabled authentication handover with efficient privacyprotection in sdn-based 5g networks," IEEE Transactions onNetwork Science and Engineering, 2019.

K. L. C. C. J. G. Q. L. Y. Guo, "A review of research on security ofcloud service platform in medical environment," in Proceedingsof IEEE International Conference on Consumer Electronics - Taiwan(ICCE-TW), Yilan, Taiwan, May 2019.

B. A. M. H. A. A. W. A. H. A. M. Ayaz, "A systematic literaturereview on cloud computing security: Threats and mitigationstrategies," IEEE Access, vol. 9, pp. 57 792–57 807, 2021.

A. S. K. P. G. Shidaganti, "Cloud storage security risks, practicesand measures: A review," in Proceedings of IEEE International Conferencefor Innovation in Technology (INOCON), Bangluru, India,November 2020.

A. M. A. Joseph, "Blockchain for cloud storage security: A review,"in Proceedings of 4th International Conference on IntelligentComputing and Control Systems (ICICCS), Madurai, India, May2020.

A. P. N. S. D. R. A. Nayak, "A detailed review of cloud security:Issues, threats & attacks," in Proceedings of 4th InternationalConference on Electronics, Communication and Aerospace Technology(ICECA), Coimbatore, India, November 2020.

A. M. S. J. J. Kizhakkethottam, "A review on cloud securitythreats and solutions," in Proceedings of International Conference onSoft-Computing and Networks Security (ICSNS), Coimbatore, India,2015.

M. I. M. U. Y. Z. S. Fong, "A critical review of security threats incloud computing," in Proceedings of 3rd International Symposiumon Computational and Business Intelligence (ISCBI), Bali, Indonesia,December 2015.

R. A. N. M. A. Almaiah, "Cyber security threats in cloud:Literature review," in Proceedings of International Conference onInformation Technology (ICIT), Amman, Jordan, July 2021.

T. K. D. C. Balakrishna, "Cloud security risk management: Acritical review," in Proceedings of 9th International Conference onNext Generation Mobile Applications, Services and Technologies, Cambridge,UK, September 2015.

S. G. K. D. P. Theng, "A review on intrusion detection techniquesfor cloud computing and security challenges," in Proceedingsof 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 2015.

A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha,H. Karimipour, and S. R. Karizno, "Slpow: Secure and lowlatency proof of work protocol for blockchain in green iotnetworks," in 2020 IEEE 91st Vehicular Technology Conference(VTC2020-Spring). IEEE, 2020, pp. 1–5.

P. M. S. K. U. G. E. S. P. R. C. Joshi, "Security perspectives ofvarious iot cloud platforms: A review & case study," in Proceedingsof International Conference on Computing, Communication, andIntelligent Systems (ICCCIS), Greater Noida, India, 2021.

N. K. A. R. V. K. H. Walia, "Improve cloud based iot architecturelayer security - a literature review," in Proceedings of InternationalConference on Computing, Communication, and Intelligent Systems(ICCCIS), Greater Noida, India, 2021.

N. A. A. M. A. S. D. F. A. A. N. Moussa, "The security issues iniot - cloud: A review," in Proceedings of 16th IEEE International Colloquiumon Signal Processing & Its Applications (CSPA), Langkawi,Malaysia, February 2020.

A. S. H. A. K. Saleem, "Cloud-assisted iot-based scada systemssecurity: A review of the state of the art and future challenges,"IEEE Access, vol. 4, pp. 1375–1384, 2016.

E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, R. M. Parizi,and G. Srivastava, "Secure ai and blockchain-enabled frameworkin smart vehicular networks," in 2021 IEEE Globecom Workshops(GC Wkshps). IEEE, 2021, pp. 1–6.

S. M. C. Ramakrishnan, "Review of face recognition techniquesfor secured cloud data surveillance using machine learning," inProceedings of 5th International Conference on Innovative Technologiesin Intelligent Systems and Industrial Applications (CITISIA), Sydney,Australia, November 2020.

M. W. N. Kratzke, "Towards distributed clouds: A review aboutthe evolution of centralized cloud computing, distributed ledgertechnologies, and a foresight on unifying opportunities and securityimplications," in Proceedings of International Conference on HighPerformance Computing & Simulation (HPCS), Orleans, France, July2018.

D. S. M. Kumar, "Secure data communication in client-cloudenvironment: A survey," in Proceedings of 7th International Conferenceon Communication Systems and Network Technologies (CSNT),Nagpur, India, November 2017.

A. B. N. M. A. T. Q. N. H. A. F. M. Dakalbab, "Machine learningfor cloud security: A systematic review," IEEE Access, vol. 9, pp.20 717–20 735, 2021.

R. M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, andK.-K. R. Choo, "Integrating privacy enhancing techniques intoblockchains using sidechains," in 2019 IEEE Canadian Conferenceof Electrical and Computer Engineering (CCECE). IEEE, 2019, pp.1–4.

A. Yazdinejad, R. M. Parizi, A. Dehghantanha, G. Srivastava,S. Mohan, and A. M. Rababah, "Cost optimization of securerouting with untrusted devices in software defined networking,"Journal of Parallel and distributed Computing, vol. 143, pp. 36–46,2020.

M. Kazemi and A. Yazdinejad, "Towards automated benchmarksupport for multi-blockchain interoperability-facilitating platforms,"arXiv preprint arXiv:2103.03866, 2021.

A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "Performance improvementand hardware implementation of open flow switchusing fpga," in 2019 5th Conference on Knowledge Based Engineeringand Innovation (KBEI).

IEEE, 2019, pp. 515–520.

A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. mP. C. Rodrigues, "Biometrics-based privacy-preserving user authentication

scheme for cloud-based industrial internet of thingsdeployment," IEEE Internet of Things Journal, vol. 5, no. 6, pp.4900–4913, 2018.

Y. Hailemariam, A. Yazdinejad, R. M. Parizi, G. Srivastava, andA. Dehghantanha, "An empirical evaluation of ai deep explainabletools," in 2020 IEEE Globecom Workshops (GC Wkshps. IEEE,2020, pp. 1–6.

J. Sun, D. Chen, N. Zhang, G. Xu, M. Tang, X. Nie, and M. Cao, "Aprivacy-aware and traceable fine-grained data delivery systemin cloud-assisted healthcare iiot," IEEE Internet of Things Journal,vol. 12, no. 8, pp. 10 034–10 046, 2021.

Y. Zhao, L. T. Yang, and J. Sun, "Privacy-preserving tensor-basedmultiple clusterings on cloud for industrial iot," IEEE Transactionson Industrial Informatics, vol. 15, no. 4, pp. 2372–2381, 2019.

L. Zhang, X. Meng, K.-K. R. Choo, Y. Zhang, and F. Dai, "Privacypreservingcloud establishment and data dissemination schemefor vehicular cloud," IEEE Transactions on Dependable and SecureComputing, vol. 17, no. 3, pp. 634–647, 2020.