*International Journal on Recent and Innovation Trends in Computing and Communication*
***ISSN: 2321-8169 Volume: 11 Issue: 5***
***Article Received:** 25 February2023 **Revised:** 12 March 2023 **Accepted:** 30 April 2023*

# Securing The Future: A Proactive Approach to Cloud Computing Security

**[1]Syed Imran Patel, [2]Dr. Sumit Bhattachar**
[1]Research Scholar, Department of Computer Science, Singhania University, Pacheri Bari, Jhunjhunu, Rajasthan.
[2]Associate Professor, Department of Computer Science, Singhania University, Pacheri Bari, Jhunjhunu, Rajasthan

***Abstract :*** The research focuses on two main contributions to the field of cloud computing, which is a source of information for many sectors and on which the next generation will rely heavily. Users can access a wide range of services, including software, storage platforms, and hardware, from the cloud, and they can use these resources according to their needs. As a first contribution, we provide a privacy protection technique that makes use of sequential encryption to ensure that sensitive data stored in the cloud is adequately safeguarded.

***Keywords:*** *Cloud, computing, information, generation.*

## INTRODUCTION

The ability to manage data and provide consumers with on-demand services is a key feature of cloud providers. Data stored in the cloud may be accessed by users according to their service needs; these needs are met via a variety of conventional networks together referred to as cloud storage. Information about the company, user profiles stored in the cloud, and data of online backups are all kept in the cloud. The cloud stores user profiles, company logs, and backup information for internet logging, and it provides a number of services to cloud users over a number of conventional networks.

Among the difficulties associated with cloud computing include online data backup, data archiving, data compliances, disaster recovery, and compliance regulations. One of cloud computing's numerous advantages is that it makes data transfers between service providers simple for customers, which is especially useful in the corporate sector (Chandramohan Dhasarathan 2017). Data stored in the cloud may be accessed by users according to their service needs; these needs are met via a variety of conventional networks together referred to as cloud storage. Information about the company, user profiles stored in the cloud, and data of online backups are all kept in the cloud.

Users see the expansion of cloud computing and store data there, whether it's sensitive or not, in order to share it or save money. Despite these advantages, cloud computing is nevertheless plagued by privacy and security issues, which are limiting its expansion. Users want to ensure that only 472ptimizati users may access their data while using cloud computing, which involves outsourcing the data. Data owners using cloud computing must be responsible for making choices about data access rules.

The computer infrastructure that provides customers with the resources, services, and data they need is what the cloud platform is all about. One explanation is that cloud customers may avoid the large upfront costs of establishing and maintaining their own IT infrastructure by paying for the services they use on an as-needed basis. When people talk about their private data being stored on the cloud, they often wonder whether it is safe since there are no restrictions on what may be stored there. One major issue with cloud computing is the lack of privacy protections; consumers will quit using the service if they discover their data is not secure.

Since data publish-subscribe systems place a premium on privacy, users lose faith in the cloud server when they use it as a broker. In cloud computing, CSPs may exchange data internally or provide it to 472ptimizati consumers. Although CP may be obligated to transmit the data with a sticky policy, service providers make sure that the user or requestor who got the data applies a comparable policy on it.

Sticky or privacy policies can only be implemented at the receiving end if both the sender and the receiver have the same policy. Unfortunately, the policy for protecting data privacy lacks a clear definition. The lack of a universally accepted privacy policy is largely attributable to the fact that no one policy language has a set of rules that are universally applicable. Consequently, developing a privacy policy using a single policy language is an impossibility. The XACMLv2 (OASIS 2005), XACMLv3 (OASIS 2010), PERMIS, P3P, Keynote (W3C 2002), and many more are among the policy languages. To provide just one example, XACMLv3 and PERMIS both allow delegation of power, while XACMLv2 does not. Never has XACML's policy language been effective for a state-based policy rule, despite its assumption of possessing a stateless Privacy-Preserving Data Publication.

***Article Received:*** *25 February2023* ***Revised:*** *12 March 2023* ***Accepted:*** *30 April 2023*

PERMIS generally helps with both static and dynamic separation of duties (SoD) as it enables state-based rules.

## LITERATURE AND REVIEW

**Wishnu Kusumo Agung Erlangga et al (2022)** Computer users may face new challenges as the digital landscape changes. Cybersecurity risks are ever-changing and growing. The majority of people who use computers, however, fail to grasp this concept. Despite cloud computing's meteoric rise in popularity, the models provided by different public cloud providers mostly revolve on infrastructure resources, application platforms, and software packages. To have a better grasp of the available cloud service models, this research will begin with a literature review. This research makes use of publications published between 2010 and 2020. The information was culled from relevant and associated cyber security and cloud computing publications. This structure is based on the following principles. To begin, the perimeter scanner is the primary point of entry for external cyberattacks in the architecture that has been detailed. If the attacker manages to breach the initial line of Defence, the firewall and subsequent levels of protection will step in. Machine learning, on the other hand, will be able to spot any attack that manages to circumvent the various protection measures. Consequently, many assaults are 473ptimizatio according to a wide range of perspectives. Through the consolidation of previous research and the establishment of global guidelines, cloud-related cyber security may make strides forward.

**Shan Ali et al (2019)** In today's cutthroat business climate, smart grids and other bidirectional communication infrastructures pose a significant risk due to their susceptibility to network assaults such as distributed denial of service (DdoS). Network nodes that have been infiltrated in a distributed denial of service assault (DdoS) flood targets, such as database servers, with connection requests, fake data packets, or incoming messages. This causes the servers to block access to real users. In order to protect the network against distributed denial of service (DdoS) assaults, researchers have recently investigated methods based on machine learning. In order to construct predictive learning systems, measurements may be taken either in batch mode or online under various system assault situations. Our work here proposes a method for efficiently detecting DdoS attacks using feature learning based on multilayer auto-encoders. To generate features, we encode the training and test data using auto-encoders that we learn in an unsupervised way, using both shallow and deep layers. After that, an effective Multiple Kernel Learning (MKL) approach is used to combine the multilayer features into a final unified detection model. Using six up-to-date approaches as a comparison, we conduct tests on two benchmark datasets and subsets of DdoS attacks. In terms of prediction accuracy, the results demonstrate that the suggested strategy surpasses the examined methods.

**A H M Jakaria et al (2017)** One sort of cyberattack that naïves both frequent and harmful naïves distributed denial of service (DdoS). Most of the traffic in a distributed denial of service assault is SYN packets. Allocate enough resources to the defence so that it can handle overwhelming DdoS attacks without significantly impacting benign traffic. This may be accomplished at a much cheaper cost with more flexibility with the help of Network Function Virtualization (NFV) technology. To counteract distributed denial of service attacks, we provide a method that uses the Network Function Virtualization platform and can adapt to different attack loads. In the event of a distributed denial of service (DdoS) assault, our suggested method employs dynamic network agents to intercept packets. Specifically, our attention is drawn to the system that dynamically deploys virtual agents in response to the intensity of the assault. The number of agents to be assigned to protect against attack traffic is determined dynamically by the associated load-balancing algorithm. The results of our simulations show that the mechanism can successfully counter DdoS attacks of varying intensities, with little impact on benign traffic and a significantly lower increase in server response time compared to a successful DdoS attack.

**Ahmed Albugmi et al (2016)** Cloud computing data security is the topic of this study. This research looks at cloud data and how it relates to security. In order to guarantee optimum data protection by lowering risks and dangers, the article will delve into specifics of data protection techniques and tactics 473ptimiza around the globe. While cloud storage has many useful uses, it also exposes data to apps that may be vulnerable due to preexisting vulnerabilities. The usage of virtualization in the cloud runs the same risk of data corruption that occurs when an untrusted guest operating system (OS) is run on a hypervisor. Information on Data-at-Rest and Data-in-Transit security measures will also be included in the article. A comprehensive understanding of SaaS, PaaS, and IaaS (Infrastructure as a Service) forms the basis of the research.

**Roy Chowdhury, Rajarshi. (2014).** Applications, storage, and platforms for highly scalable computing that are made available as a service to consumers, businesses, and governments is known as cloud computing. For these reasons, SMBs (Small and Medium Business) are slowly but surely embracing cloud computing services in an effort to save costs and boost productivity. Although the advantages and

***Article Received:*** *25 February2023* ***Revised:*** *12 March 2023* ***Accepted:*** *30 April 2023*

scalability of cloud services are easy to understand, there is growing anxiety regarding cloud computing security. "How much secure is cloud computing environment?" . It has been observed that security concerns provide a significant obstacle to the continuous expansion of cloud computing. Users and businesses alike are wary of putting their data and apps on the cloud due to a number of serious security concerns. This paper's primary goal is to identify key security risks and challenges that should be considered while developing and deploying cloud services, as well as ways to address these concerns. While it's true that cloud computing requires secure management and access, it's important to remember that the technology itself is not inherently insecure.

## DATA PRIVACY PRESERVATION

“Local recoding and proximity privacy techniques for data preserving” are used extensively in several previous publications. Nevertheless, the approach is guided in a top-down manner by the “non-monotonicity” virtue of proximity privacy. Data stored by most cloud servers is made publicly available. Nevertheless, careless cloud users have the ability to manipulate this data. Customers can lose faith if their data isn’t protected. There must be robust methods for user privacy in order for cloud computing to be a success.

Since the cloud model deals with massive amounts of data, several studies have concentrated on protecting certain attributes of data. Nevertheless, the majority of published works address dimensionality issues with small data sets. Choosing the right characteristics to safeguard privacy is crucial since the majority of database attributes include sensitive information.

### Proposed Privacy Preservation Architecture

By presenting “CIC-WOA,” this part delves into the privacy preservation architecture. The primary objective is to modify user data acquired via the construction of privacy-preserving data using a key, with the data being stored in the cloud. The original database may be retrieved from the privacy-maintained database using the key. In this research, we propose the “CIC-WOA model” as a means of constructing data sets using the original, private data sets. Figure 1 depicts the “CIC-WOA model architecture for privacy preservation in cloud” that has been proposed.

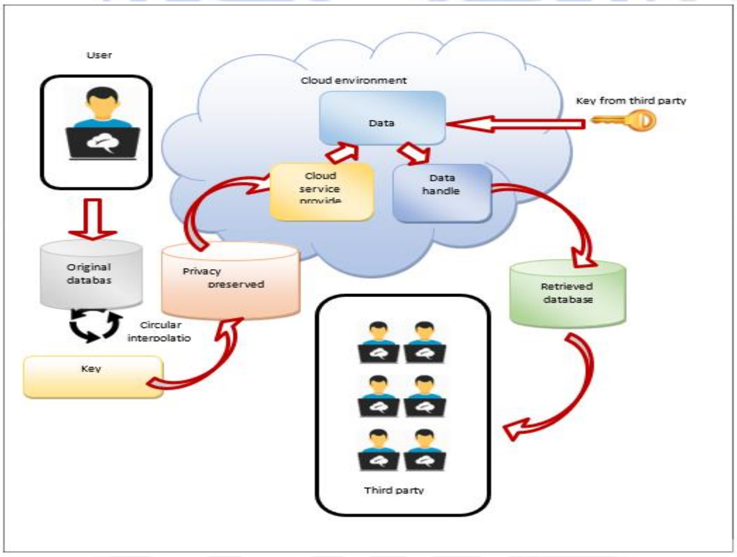


Figure 1 Privacy Preservation Architecture

### Proposed Privacy Preservation Algorithm

Our suggested method for protecting users’ privacy, “Circular Interpolation and Chronological Whale Optimisation Algorithm (CIC-WOA)”, is detailed here. Data modified in the original dataset is stored by internet users in a cloud model. Finding the user’s privacy-protected database D* is the goal of the suggested privacy-preservation methodology.

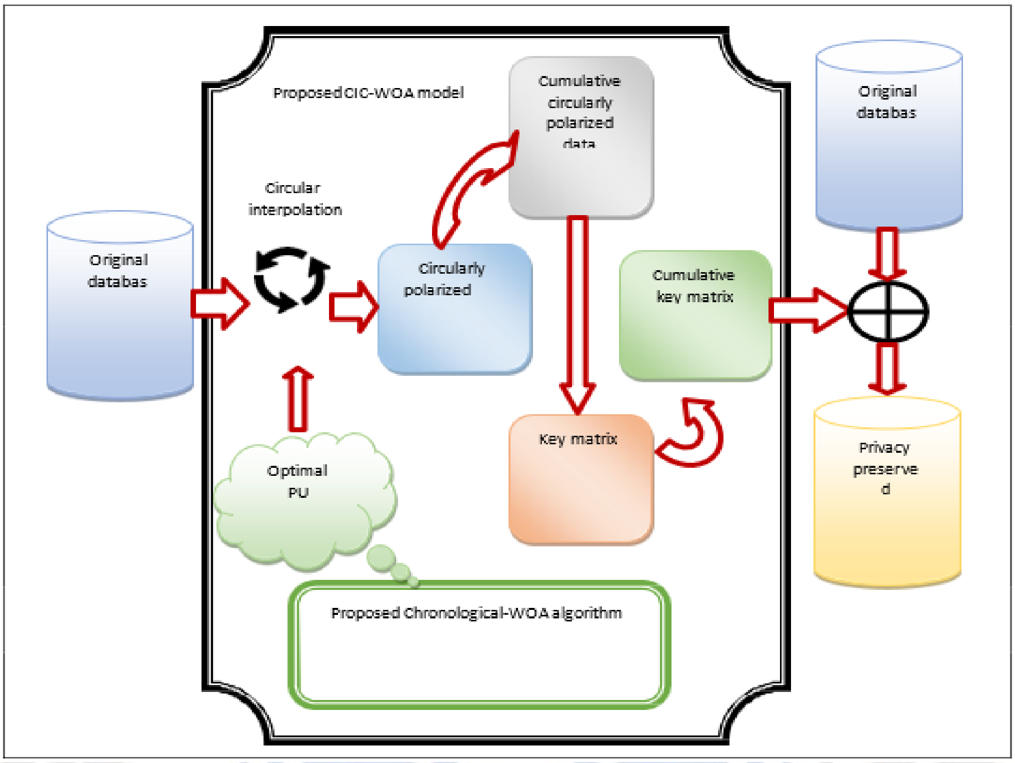


Figure 2 Schematic diagram for privacy preserved database

### Methodology for Evaluating PU Coefficients

This study presents a novel 475ptimization method for determining the best metric to use in whale searches. Using "encircle prey" and "bubble net" techniques, the humpback whale being examined in the current WOA algorithm attempts to locate its prey. Improved convergence, even in a vast solution space, is one of WOA's advantages.

## DATA PRIVACY PRESERVATION AND MEDICAL DATA CLASSIFICATION IN CLOUD

While cloud computing is undeniably necessary, IT organisations are understandably worried about data privacy, the biggest risk associated with cloud security. No matter what kind of data point it is, privacy preservation guarantees its protection. Because of the extreme sensitivity of medical records, protecting their privacy in the cloud is an important issue.

Data categorization techniques provide another layer of protection for the data. They sort the information according to how sensitive the medical records are. Security must be a top priority when the sensitivity level is high. "Privacy-preserved medical data classification is the researchers' area" as it renders third-party authenticators useless in safeguarding sensitive data. As a result of the intelligent approaches' ability to distinguish between "sensitive" and "non-sensitive" data, the encryption of sensitive data is made easier in the cloud. Furthermore, categorization algorithms lessen the time, memory, and computational load. The categorization of medical data is crucial when the "privacy of the data" is established, as it guarantees effective decision-making and demands on early illness prediction. While several approaches exist for classifying medical records, data mining stands out as a powerful tool for illness prediction. Support Vector Machine (SVM) and Naïve Bayesian classification are two popular classifiers that are used to secure sensitive medical data. No outside entity should be able to access the prediction models used to forecast patients' illnesses based on their medical records.

### Privacy Preserved Medical Data Classification

It is possible for a cloud computing environment to store and make available a large database including the medical records of several patients. So, patients' medical records are safely saved on the cloud, and they may be retrieved whenever needed. There must be a system in place to prevent the disclosure of personally identifiable information (PII) included in medical records. Protecting the privacy of individuals is crucial in keeping the data secure. Assuring correct categorization for illness diagnosis and protecting the privacy of patients' medical records are the primary responsibilities of this position.

***Article Received:** 25 February2023 **Revised:** 12 March 2023 **Accepted:** 30 April 2023*

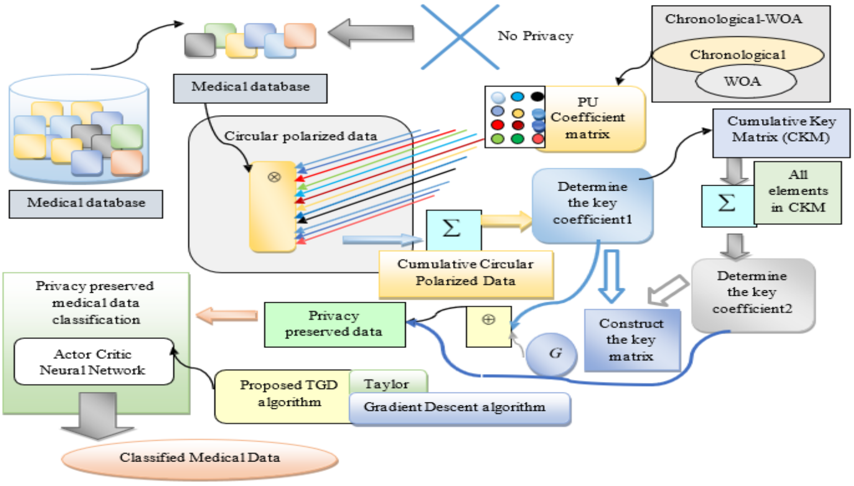


Figure 3 Block diagram of the privacy preserved medical data classification

## EXPERIMENTATION AND RESULTS

(a) Experimental setup

We utilize Windows 10 as our operating system and the Java programming language on a personal computer with at least 2 GB of RAM.

(b) Collections of data

"Cleveland, Switzerland, and Hungarian, taken from the UCI (University of California, Irvine) machine repository," the three databases mentioned before, are used to run the simulation.

(c) Analysing performance

The accuracy, True Positive Rate (TPR), and False Positive Rate (FPR) are the performance indicators used for the categorization. As for categorization, we employ accuracy, True Positive Rate (TPR), and False Positive Rate (FPR).

The following is a definition of accuracy, which is a measure of the correctness of detection:

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP}$$

where TP: True Positive, TN: True Negative, FP: False Positive, and FN: False Negative are the relevant symbols. One definition of sensitivity is the degree to which genuine positives are detected with high precision.

$$Sensitivity = \frac{TP}{TP + FN}$$

To prevent the "false rejection," a "measure that avoids the false positive rate" (FPR) is defined as,

True Negatives are produced by FPR □1□Specificity, which is defined as,

$$Specificity = \frac{TN}{TN + FP}$$

(d) Competing Approaches

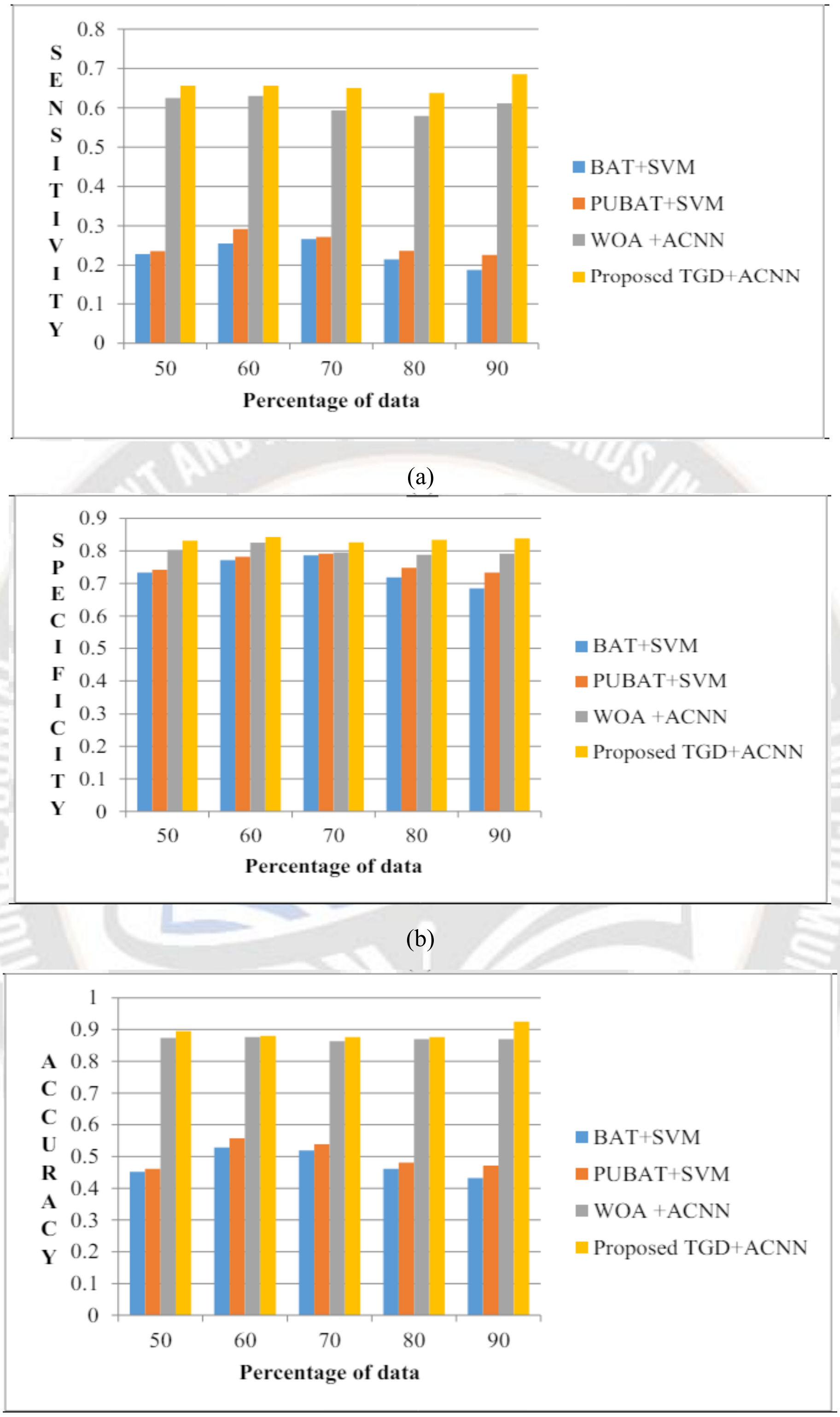
Methods such as BAT+SVM, PUBAT+SVM, and WOA+ACNN were used for comparative purposes in order to demonstrate the efficacy of the suggested approach. Using the WOA algorithm in the proposed TGD-ACNN algorithm yields WOA+ACNN, while substituting the BAT algorithm for PUBAT generates BAT+SVM.

(e) Analysing Experimental Results Comparatively

The "comparative experimental analysis of the privacy preservation methods" using three datasets is covered here.

(i) Research comparing different methods with the Cleveland dataset

***Article Received:** 25 February2023 **Revised:** 12 March 2023 **Accepted:** 30 April 2023*



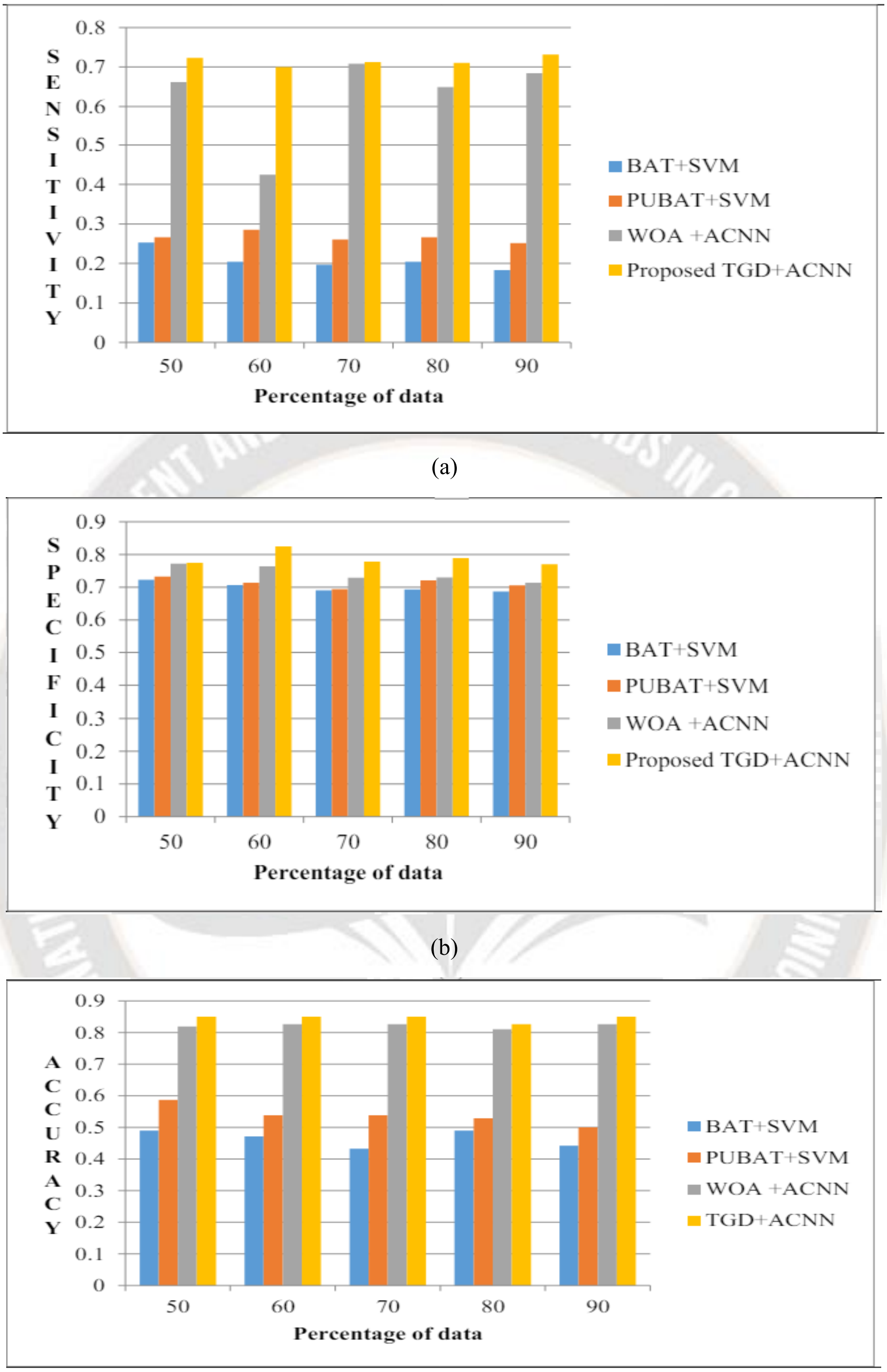
(a)

(b)

(c)

Figure 4 Comparing with the Cleveland dataset in relation to... Accuracy, Specificity, and Sensitivity

(ii) Comparative Analysis using the Switzerland dataset



(a)

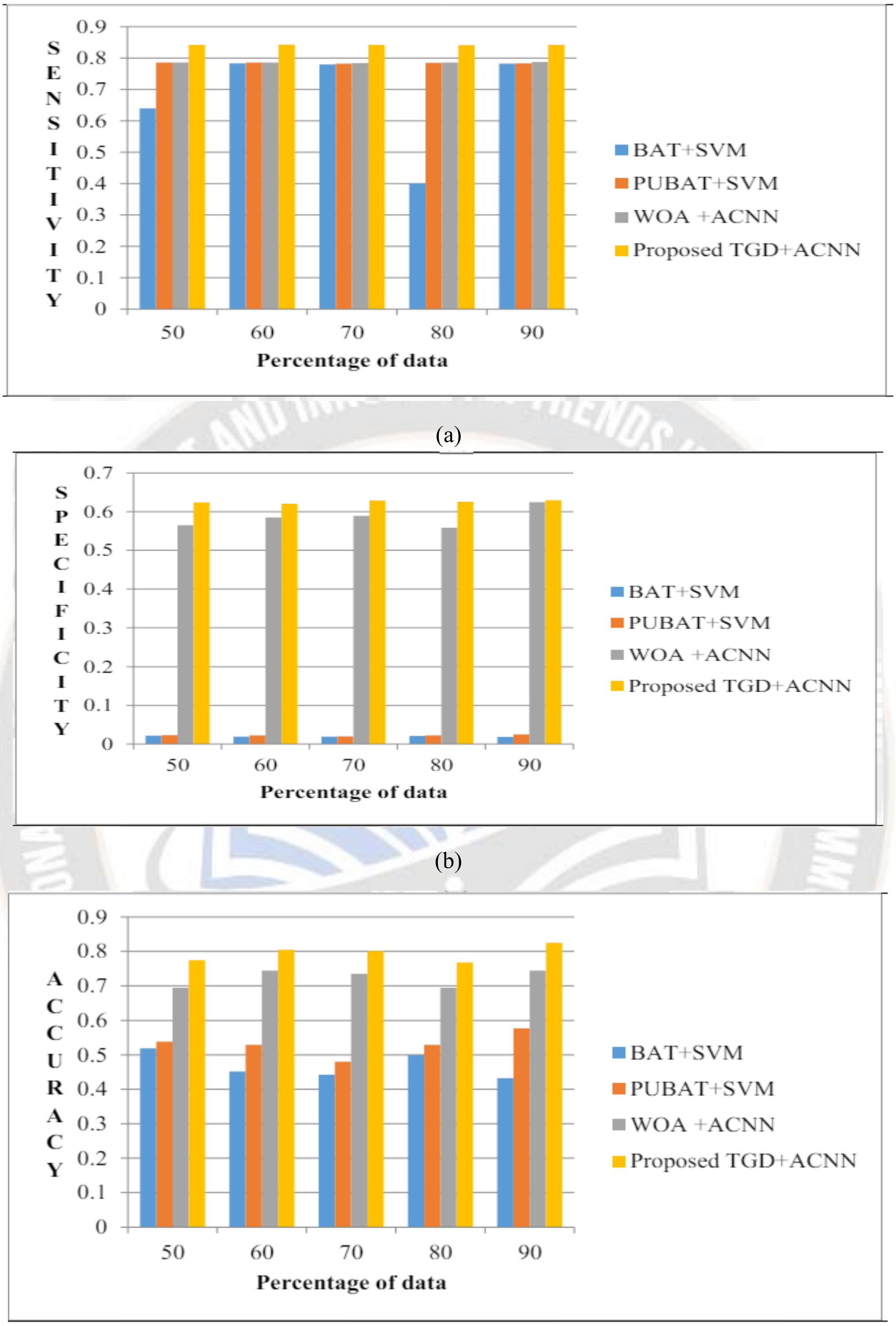
(b)

(c)

Figure 5 Comparing with the Switzerland dataset in relation to... Accuracy, Specificity, and Sensitivity

(iii) Analysis using the Hungarian dataset

***Article Received:*** *25 February2023* ***Revised:*** *12 March 2023* ***Accepted:*** *30 April 2023*



(a)

(b)

(c)

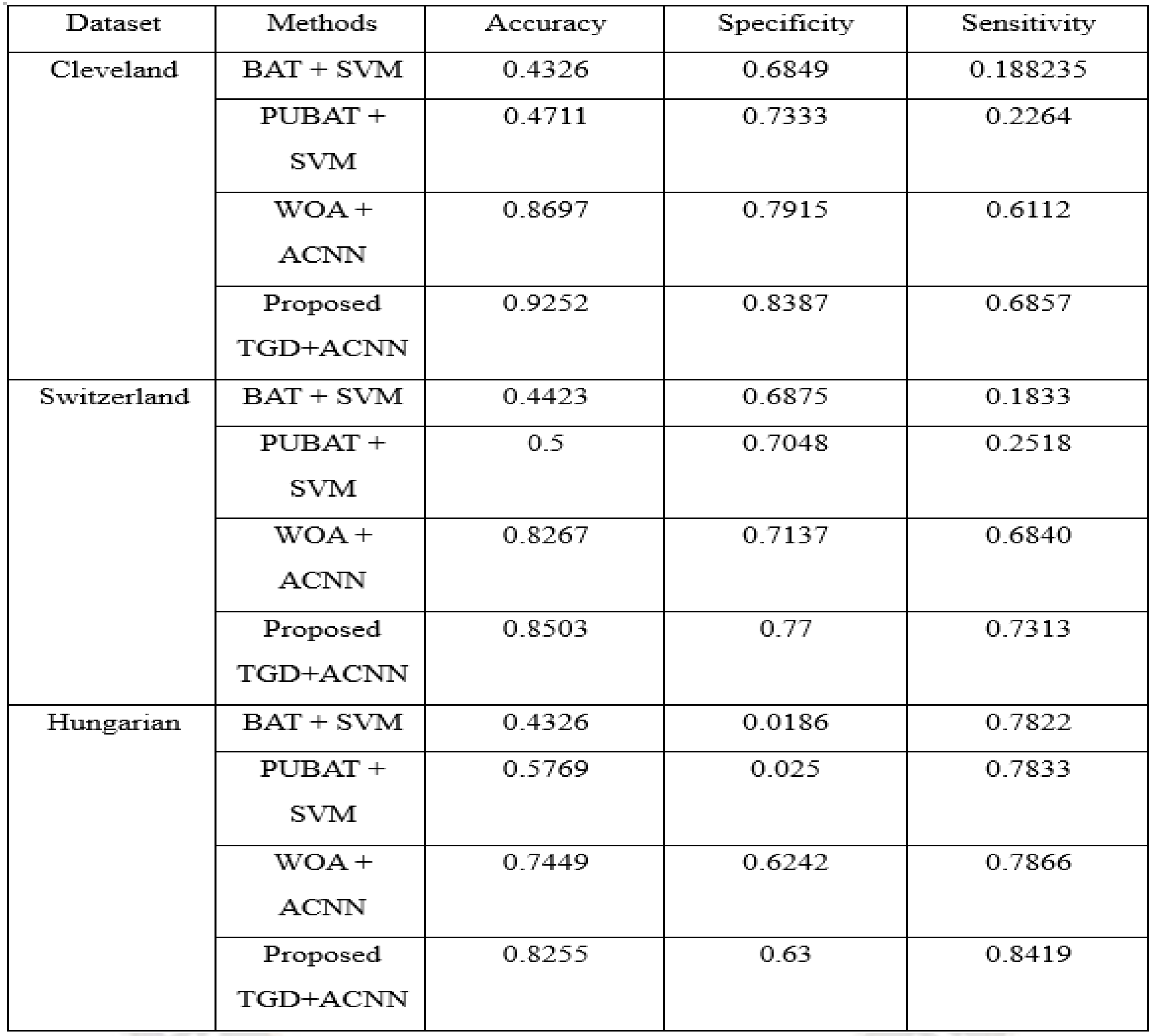
Figure 6 Comparing with the Hungarian dataset in relation to... Accuracy, Specificity, and Sensitivity

(f) Comparative Analysis

***Article Received:*** *25 February2023* ***Revised:*** *12 March 2023* ***Accepted:*** *30 April 2023*

Table 1 shows the results of a comparison of privacy preservation strategies based on the greatest performance that was achieved.

Table 1 Comparative evaluation of the categorization and privacy preservation techniques



| Dataset | Methods | Accuracy | Specificity | Sensitivity |
|---|---|---|---|---|
| Cleveland | BAT + SVM | 0.4326 | 0.6849 | 0.188235 |
| | PUBAT + SVM | 0.4711 | 0.7333 | 0.2264 |
| | WOA + ACNN | 0.8697 | 0.7915 | 0.6112 |
| | Proposed TGD+ACNN | 0.9252 | 0.8387 | 0.6857 |
| Switzerland | BAT + SVM | 0.4423 | 0.6875 | 0.1833 |
| | PUBAT + SVM | 0.5 | 0.7048 | 0.2518 |
| | WOA + ACNN | 0.8267 | 0.7137 | 0.6840 |
| | Proposed TGD+ACNN | 0.8503 | 0.77 | 0.7313 |
| Hungarian | BAT + SVM | 0.4326 | 0.0186 | 0.7822 |
| | PUBAT + SVM | 0.5769 | 0.025 | 0.7833 |
| | WOA + ACNN | 0.7449 | 0.6242 | 0.7866 |
| | Proposed TGD+ACNN | 0.8255 | 0.63 | 0.8419 |

Three datasets, including the Hungarian, Swiss, and Cleveland datasets, are used to examine the specificity, accuracy, and sensitivity of the suggested technique. These are the outcomes for the approaches shown by the study of the Cleveland dataset. In comparison to BAT + SVM (0.4326), PUBAT + SVM (0.4711), and WOA + ACNN (0.8697), the suggested technique obtained an accuracy of 0.9252. On the Cleveland dataset, the proposed TGD+ACNN received a sensitivity of 0.6857, while BAT + SVM, PUBAT + SVM, and WOA + ACNN all received sensitivity values of 0.1882, 0.2264, and 0.6112. Just as BAT + SVM, PUBAT + SVM, and WOA + ACNN all achieved, respectively, specificities of 0.6849, 0.7333, and 0.7915, the suggested technique achieves a specificity of 0.8387.

## CONCLUSION

Protecting sensitive information on the cloud, the most pressing issue in this area. "Circular interpolation and Chronological-Whale Optimisation Algorithm (CIC-WOA) for privacy preservation in cloud" was the first proposed approach to data privacy. Furthermore, the chapter introduced a novel approach called TGD-ACNN for the categorization of medical data, which is a closely connected subject to data privacy in the health sciences.

## REFERENCES

[1] Albugmi, Ahmed & Alassafi, Madini & Walters, Robert & Wills, Gary. (2016). Data Security in Cloud Computing. 10.1109/FGCT.2016.7605062.

[2] Ali, Shan & Li, YuanCheng. (2019). Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2933304.

[3] C. Everett, “Cloud computing - a question of trust,” Computer Fraud & Security, vol. 2009, no. 6, pp. 5-7, 2009.

***Article Received:** 25 February2023 **Revised:** 12 March 2023 **Accepted:** 30 April 2023*

[4] Erlangga, Wishnu & Ramadhan, Muhammad. (2022). Potential Security Issues in Implementing IaaS and PaaS Cloud Service Models. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM). 3. 143-162. 10.34010/injiiscom.v3i2.8446.

[5] G. Zhao, C. Rong, M. G. Jaatun et al., "Reference deployment models for eliminating user concerns on cloud security," Journal of Supercomputing, pp. 1-16, 2010.

[6] J. Sedayao, S. Su, M. Xiaohao et al., "A Simple Technique for Securing Data at Rest Stored in a Computing Cloud," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 553-8.

[7] Jakaria, A H M & Rashidi, Bahman & Rahman, Mohammad & Fung, Carol & Yang, Wei. (2017). Dynamic DDoS Defense Resource Allocation using Network Function Virtualization. 10.1145/3040992.3041000.

[8] K. R. Joshi, G. Bunker, F. Jahanian et al., "Dependability in the cloud: Challenges and opportunities," Proceedings of the International Conference on Dependable Systems and Networks. pp. 103-104.

[9] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security & Privacy, vol. 7, no. 4, pp. 61-4, 2009.

[10] M. L. Yiu, G. Ghinita, C. S. Jensen et al., "Enabling search services on outsourced private spatial data," VLDB Journal, vol. 19, no. 3, pp. 363-384, 2010.

[11] Marinos, and G. Briscoe, "Community Cloud Computing," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 472-84.

[12] R. Buyya, "Market-oriented cloud computing: vision, hype, and reality of delivering computing as the 5th utility," Proceedings of the 2009 Fourth ChinaGrid Annual Conference. ChinaGrid 2009. pp. 4 pp.-4 pp.

[13] Roy Chowdhury, Rajarshi. (2014). Security in Cloud Computing. International Journal of Computer Applications. 98. 975-8887.

[14] W. Cong, W. Qian, R. Kui et al., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. pp. 9 pp.-9 pp.

[15] W. Wang, Z. Li, R. Owens et al., "Secure and efficient access to outsourced data." pp. 55-65.

[16] Z. Fengzhe, H. Yijian, W. Huihong et al., "PALM: security preserving VM live migration for systems with VMM-enforced protection," 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference. pp. 9-18.