

## Using support vector machine regression to reduce cloud security risks in developing countries

Sanaa Hammad Dhahi<sup>1</sup>, Estqlal Hammad Dhahi<sup>2</sup>, Ban Jawad Khadhim<sup>3</sup>, Shaymaa Taha Ahmed<sup>3</sup>

<sup>1</sup>Department of Hotel Studies, College of Tourism Sciences, University of Kerbala, Kerbala, Iraq

<sup>2</sup>Computer Center, University of Kerbala, Kerbala, Iraq

<sup>3</sup>Department Computer Science, College of Basic Education, University of Diyala, Diyala, Iraq

### Article Info

#### Article history:

Received Nov 29, 2022

Revised Jan 16, 2023

Accepted Jan 26, 2023

#### Keywords:

Cloud in developing countries

Cloud security risk

Mean square error

Root mean square error

Support vector machine

regression

### ABSTRACT

The use of the cloud by governments throughout the world is being aggressively investigated to increase efficiency and reduce costs. The majority of cloud computing risk management programs prioritize addressing cloud security issues that government organizations may face when they choose to adopt cloud computing systems, but these programs lack evidence of security risks, and problems with using cloud computing in developing nations are uncommon, so they called for more research in this area. The objective of this paper is to use quantitative models namely Spearman's Rank correlation coefficient, simple regression, and support vector machine regression (SVMR) for estimating cloud security issues based on cloud control factors for improving the mitigation of cloud computing security issues based on control factors using intelligent models in a government organization. Identify the proper cloud control factors for every cloud security issue from estimation errors using a standard for performance measurement like mean square error (MSE) and root mean square error (RMSE), performance measurement to evaluate and validate proposed models. SVMR is an approach to enhance practices for cloud security platforms to mitigate risks and infrastructure for cloud adoption in developing countries in this paper.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



### Corresponding Author:

Shaymaa Taha Ahmed

Department of Computer Science, College of Basic Education, University of Diyala

Baquba, Diyala Governorate, Iraq

Email: shaymaa.taha.ahmed@basicedu.uodiyala.edu.iq and mrs.sh.ta.ah@gmail.com

## 1. INTRODUCTION

While adopting cloud computing can give many government benefits, many nations are starting to recognize the advantages of employing it in institutions and companies. These countries and businesses are hesitant to utilize the cloud because of security concerns. Adopting cloud computing is frequently cited as having the highest level of security concerns. From a variety of angles, cloud computing has altered how businesses see and use IT. They truly see cloud computing as a solution to many problems, including improving efficiency and cutting costs, offering more dependable and effective services, and shortening turnaround times [1]. Government systems can greatly benefit from cloud computing, which can also alleviate problems with high startup costs, usability, increased data storage, mobile access, and scalability [2]. The benefits of using cloud computing include numerous aspects. Reduced local data storage, accessibility, backup and recovery, scalability, and green computing are a few of the benefits [3]. Compared to western nations, developing nations have not yet completely adopted cloud computing. It is crucial to comprehend that one of the major challenges associated with cloud computing is the possible and perceived security threats and advantages brought about by using such technology this will help to promote the use of cloud services [4]. Every firm should be prepared and aware of the myriad

benefits and security dangers before implementing cloud services [5]. Although cloud computing is a rapidly evolving technology, there are still security issues that must be resolved before it can become more widely used [6]. The vast amount of data that is contained in cloud computing is geographically dispersed, heterogeneous, and dynamic [7]. Consequently, a number of security challenges related to cloud computing are currently receiving a lot of attention, including data protection, network security, virtualization security, application integrity, and identity management [2]. To ensure that the proper safeguards are in place, managed IT, staff members, and the process of transferring applications and data must all be aware of the dangers involved [8]. It was away and the back was high in Figure 1. Red alert IT security is by far and away the biggest risk in the opinion of Chief Information Officers.

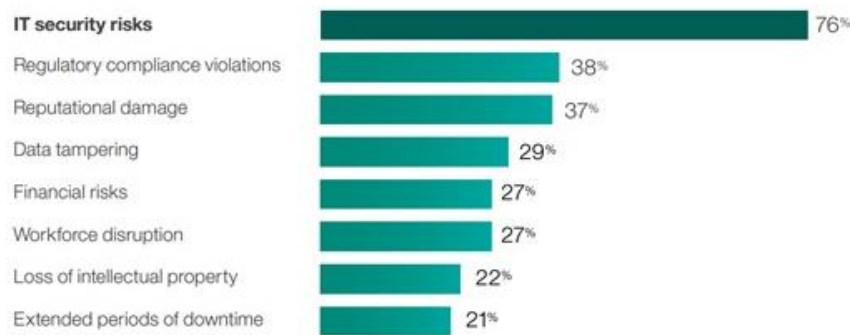


Figure 1. IT cloud security risk [9]

## 2. CLOUD IN DEVELOPING COUNTRIES

There have been few studies on cloud computing issues in developing countries. There are more challenges in developing countries because of the information technology divide between developed and developing nations. As a result, research into the issues associated with cloud computing adoption is critical to its success [10]. The dearth of studies on the advantages and difficulties of adopting cloud computing in poor nations, particularly Iraq, and recommended more research in this field. The IT department and enterprise developers in Iraq need to conduct studies to learn about the advantages and difficulties of employing cloud computing services [11]. Researchers have recently urged the expansion of the body of knowledge on the advantages and challenges of cloud computing in developing nations, including Iraq. The advantages and difficulties of employing cloud computing services from the viewpoint of users in Iraqi institutions generally [12]. When government organizations choose to implement cloud computing systems, challenges to cloud security are one of their top concerns, but there isn't enough data to support the risks and advantages of security. Furthermore, according to IT experts, cloud-based institutions will keep expanding and progressing over the coming years. However, while cloud computing has many benefits, there are also a number of issues that need to be addressed [13]. These issues, which are related to the security and privacy of the cloud, have been examined by other researchers and may have a significant impact on whether or not cloud computing is adopted by Iraqi Government organizations.

## 3. CLOUD COMPUTING SECURITY

In cloud security management is a practice of control mitigation techniques that involves of processes, methods, and tools for controlling security issues in a cloud computing project before they become problems. In addition, cloud risk management able to avoid the security issues in cloud computing environments [14]. Cloud computing is a collection of computers computing paradigm in which resources of the cloud and servers that are publicly accessible via the Internet. It is computing infrastructure are provided as services over the a significantly new idea that influence the power of internet, where a large team of systems are connected in internet to process, store and share data from a network private or public networks, to provide dynamically scalable of remote servers located anywhere in the world [15]. The existing risk management methods do not place a strong emphasis on this aspect, which has led to a high rate of software development management failure [16]. There are three stages for mitigating the cloud security issues such as cloud security identification, cloud security analysis, and cloud security monitoring, and cloud security controlling [17].

### 3.1. Cloud security identification

Identification of cloud security issues entails locating the vulnerabilities by looking at the key technologies connected to the cloud's properties and usage scenarios [18]. Additionally, the activity of

prioritizing cloud security issues takes into account all parts of all risk considerations. Based on two factors, the likelihood and effect on the cloud computing project if it succeeds, and the degree of security vulnerabilities [19]. The scope of software hazards can be determined using a variety of statistical methods. However, categorizing and figuring out the impact of the hazards is made easier by determining whether they are extreme, high, medium, low, or little. Checklists, network analysis, decision trees, an evaluation of decision drivers, cost and performance models, the project charter, guidelines, the contract agreements, work breakdown structure (WBS), and network analysis are among the techniques and approaches chosen to handle the assignment [20]. The key reason for this incident was improper identification problems throughout the assessment procedure.

### 3.2. Cloud security analysis

Cloud security analysis issues contribute to the analysis of the probabilities and outcomes in the cloud security issues' identification and estimation of the impact, sensitivity, and analysis of mitigation strategies alternatives and strategies [21]. Additionally, it examines how cloud risk management methods affect the security of cloud computing in non-profit organizations. These methods include performance models, cost models, network analysis, multivariate statistical methods, statistical decision analysis, and quality-factor analysis. The goal of the analysis of cloud security issues is to determine the levels of the identified information problems so that administrators can compare them [22]. Based on the different information problem levels, administrators will implement different issue control mitigation strategies and avoid delays in the cloud computing project [23]. As a result cloud security risk management entails evaluating and addressing the security risks associated with the cloud.

### 3.3. Cloud security controlling

Controlling cloud computing is the main way of enterprise IT optimization nowadays. A numbers of researchers have use quantitative models for mitigating the cloud computing [24]. Three quantitative models namely Spearman's Rank correlation coefficient, simple multiple regression and support vector machine regression (SVMR) are studied to complete this research work. These quantitative models that are being used by researchers for controlling cloud computing are presented. The simple multiple regression models are used to predicts future risks scientifically. This model motivates to obtain greater results for controlling the risks in IT environment.

In this stage of cloud security controlling introduces literature reviews that are related to what the control could computing. We studied more articles related to controlling could computing and identified the 26 most significant controls for controlling security in cloud computing. According to these 26 controls cloud security controls (CSC) were selected by a numbers of developers working in this filed [25].

## 4. METHOD

The method presents and describe of the framework of proposed models. These proposed models that explicitly estimate the good relation between the cloud computing security and cloud computing control for controlling the cloud security. The quantity and intelligent models namely spearman's rank correlation coefficient, simple regression, SVMR that is used to control cloud computing security is presented. The proposed model to estimate the appropriate cloud controls for specific cloud issue. The training data is divided into independent variable is cloud computing issues and dependent variable is cloud computing controls. The Z-score method has been applied for normalization data in order to achieve proper scaling for improving the proposed model. In order to examine the relationship between the cloud issues and cloud controls, the evaluation metrics are considered. The approach SVMR takes considers improving the results of quantitative models. The quantitative like simple multi regression and spearman's rank correlation coefficient have given more gaps to improve by intelligent models. Consequential, we have applied advanced intelligent models that have never been used in previous study on cloud computing risks.

### 4.1. Support vector machine regression

The support vector machine (SVM) is a ground-breaking machine learning algorithm for classification and regression purposes and is quickly supplanting neural network it is really a super arrangement of neural network algorithms as the instrument of decision for nonlinear prediction, estimation and pattern recognition system, fundamentally because of their capacity to sum up well on new information and their strong hypothetical establishment [26]. The SVM regression includes a nonlinear mapping of a n-dimensional information space into a high dimensional component space [27]. A direct relapse is then performed in this elemental space. SVMs utilize the auxiliary hazard minimization. Regression and classification are the two main uses of support vector machines one of the primary features of SVMR is the use of support vector regression (SVR), which uses prediction rather than minimizing the training error [28]. To attain good performance, the SVMR therefore makes an effort to recognize and reduce the generalized error bound as shown in Figure 2.

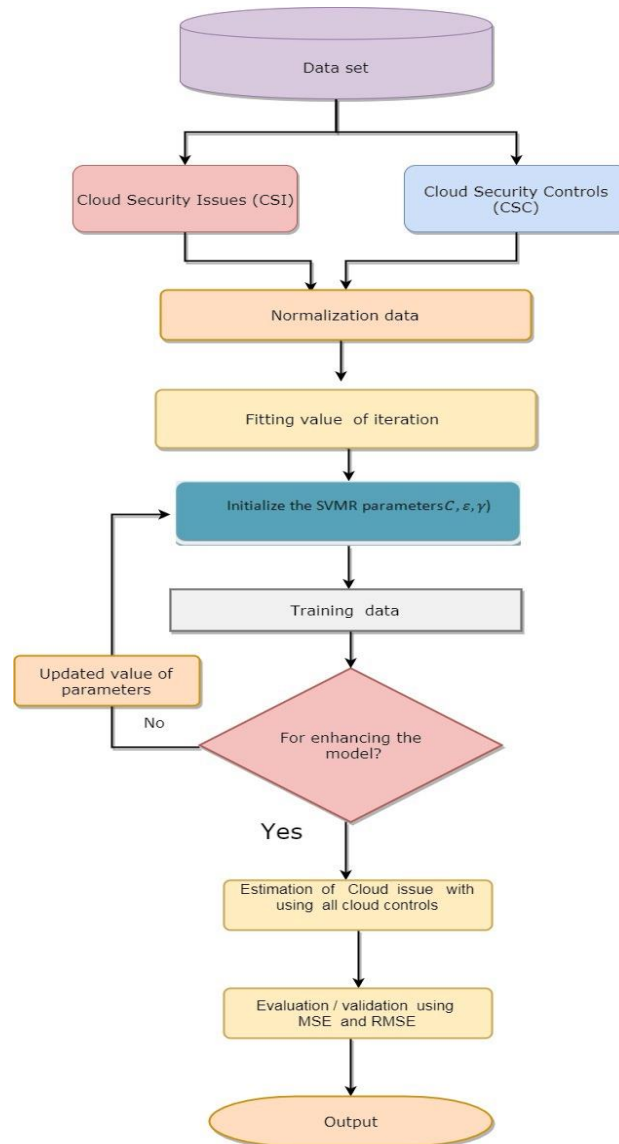


Figure 2. SVMR method for mitigating cloud security issue

## 5. RESULTS AND DISCUSSIONS

The results for controlling security issue in cloud computing in government organization. These models have made use of the spearman's rank correlation coefficient, simple linear regression, (SVMR). An approach to enhance and practices for cloud security platforms to mitigate risks and infrastructure for cloud adoption in developing countries in this paper present the details of experiments carried out on various quantitative and intelligent models and the enhanced cloud security platform and infrastructure issues in developing countries are presented in this paper. The results have been obtained from regression between the issue factors and control factors using different quantitative and intelligent models. In this research we have applied each individual issue factor with all individual control factors; and have returned the optimal results for each issue factor with all control factors.

### 5.1. Cloud platform reliability and latency

The perdition results obtained using SVMR algorithm is presented in Table 1. CSC for mitigating cloud security issues the (CSC12: - data protection and integrity for the cloud services) control is more reliable with issue (A. cloud platform reliability and latency) using SVMR approach. Furthermore, Table 1 show the prediction results of SVMR, it is observed that the CSC2 and CSC12 controls have positive impact with issue (A). The results of CSC12 control is more robust with issue (A), the values of CSC12 is mean square error (MSE)=0.941 and root mean square error (RMSE)=0.970. In Figures 3 and 4. Display the plot regression and prediction plot for CSC25 with issue (A) using SVMR approach.

Table 1. Shows a results of support vector machine regression model for issue (A)

Controls	MSE	RMSE
CSC2	0.999	0.970
CSC12	0.941	0.970

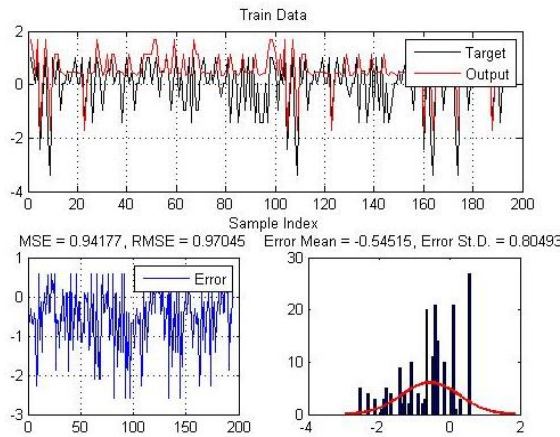


Figure 3. Prediction performance of SVMR algorithm for CSC12 with issue (A)

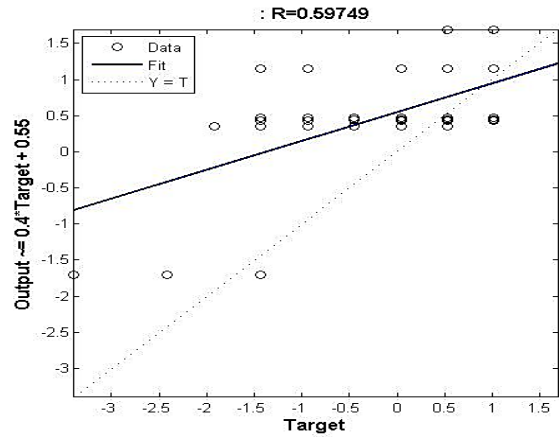


Figure 4. Performance regression plot of SVMR approach for CSC12 with issue (A)

**5.2. The multi-tenancy in the cloud**

The perdition results obtained using SVMR algorithm is presented in Table 2. CSC for mitigating cloud security issues the (CSC4: - better cloud compatibility and scalability for cloud services) control is more reliable with issue (B. the multi-tenancy in the cloud) using SVMR approach. Furthermore, Table 2 show the prediction results of SVMR, it is observed that the CSC4, CSC13, CSC20 and CSC25 controls have positive impact with issue (B). The results of CSC4 control is more robust with issue (B), the values of CSC4 is MSE=0.706 and RMSE=0.840. Figures 5 and 6 display the plot regression and prediction plot for CSC4 with issue (B) using SVMR approach.

Table 2. Results of support vector machine regression model for issue (B)

Controls	MSE	RMSE
CSC4	0.706	0.840
CSC13	0.888	0.942
CSC20	0.805	0.897
CSC25	0.987	0.993

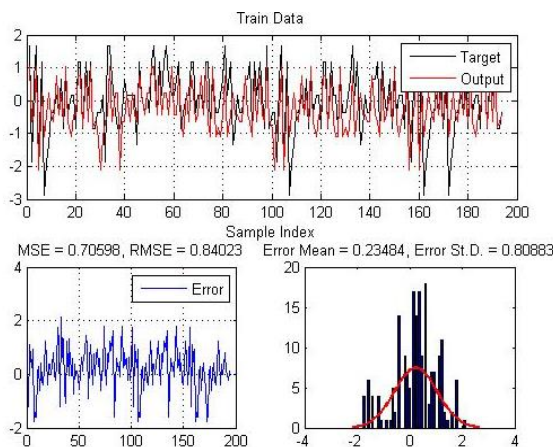


Figure 5. Prediction performance of SVMR approach for CSC4 with issue (B)

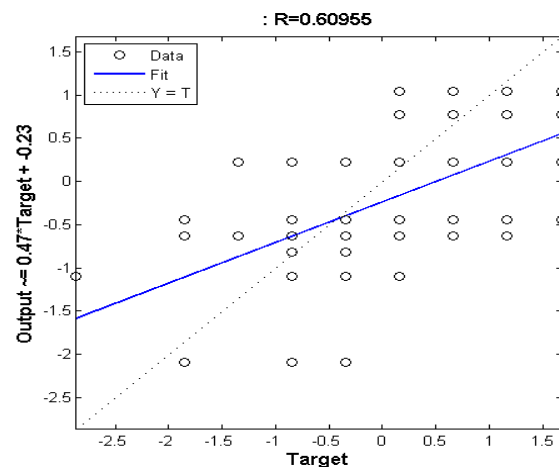


Figure 6. Performance regression plot of SVMR approach for CSC4 with issue 25

**5.3. Scalability and capability in the cloud**

The prediction results obtained using SVMR algorithm is presented in Table 3. CSC for mitigating cloud security issues the (CSC24: - implement application level for data caching) control is more reliable with issue (C. scalability and capability in the cloud) using SVMR approach. Furthermore, Table 3 shows the prediction results of SVMR, it is observed that the CSC2, CSC7, and CSC24 controls have positive impact with issue (C). The results of CSC24 control is more robust with issue (C), the values of CSC24 is MSE=0.953 and RMSE=0.976. Figures 7 and 8 display the plot regression and prediction plot for CSC24 with issue (C) using SVMR approach.

Table 3. Results of support vector machine regression model for issue (C)

Controls	MSE	RMSE
CSC2	0.987	0.993
CSC7	0.996	0.998
CSC24	0.953	0.976

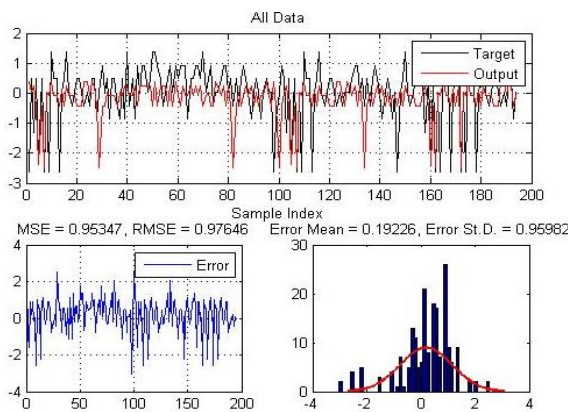


Figure 7. Performance regression plot of SVMR approach for CSC24 with issue (C)

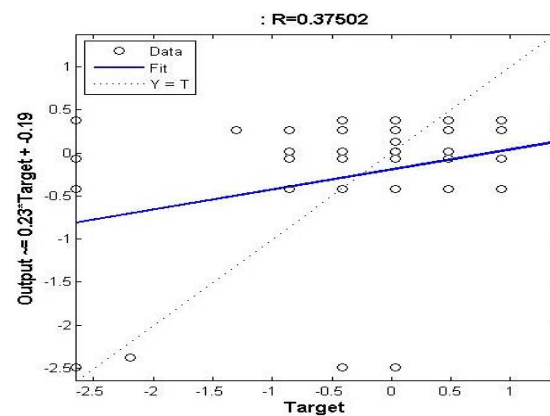


Figure 8. Prediction performance of SVMR approach for CSC24 with issue (C)

**6. EVALUATE AND VALIDATE**

To evaluate the prediction performance of SVMR approach for mitigating cloud computing security issues at cloud security platform and infrastructure using for practices for risk mitigation for the adoption of cloud computing in developing countries. Using standard like MSE and RMSE performance measurement to evaluate and validate of SVMR approach. MSE is one of the most common criterions employed to evaluate the performance of prediction models. The MSE is the square root average of the observation and forecast data. The average squared deviation of the forecast values is what this metric measures. It panelizes the most significant forecasting errors. Additionally, MSE emphasizes how huge individual errors have a significant impact on the total forecast error. Less expensive than tiny errors are large errors. The MSE formula looks like this.

$$MSE = \frac{1}{N} \sum_{k=1}^n (x_t - \bar{x}_t)^2 \tag{1}$$

The RMSE, also known as the root mean square deviation (RMSD), is a commonly used indicator of the discrepancy between values obtained from the environment being modeled at the observational level and values predicted at the predictive level. Furthermore, individual variations are also known as residuals, and the RMSE combines them into a single indicator of predictive power. The square root of the mean squared error is used to measure the RMSE when comparing prediction models to the estimated variable model. The following is the RMSE as (2).

$$RMSE = \sqrt{\frac{1}{N} \sum_{k=1}^n (x_t - \bar{x}_t)^2} \tag{2}$$

## 7. CONCLUSION AND FUTURE WORK

One of the main objectives of this research is to come up with appropriate model which can help to secure the cloud computing data. The quantity and intelligent models are implemented to control cloud computing issues. To test these models, the we have designed samples data to enhance security issue for cloud computing in government organization, these data have collected from twenty-nine cloud developers and IT developers. Furthermore, twenty-six cloud security issue factors with five domains in security system and twenty-six cloud security control mitigation approaches were presented to respondents. Furthermore, z-score method is employed in MATLAB for scaling the data. This method transformed data in the different ranges. To evaluate the proposed prediction models, the MSE, RMSE, S-err and R-squared performance measures are used. The quantity models are Pearson correlation coefficient, Simple Regression and SVMR; we have used these models for estimation on each issue with all 26 controls. Our novelty is application of intelligence models for enhancing the cloud computing security using controls factors that we have considered.

To examine potential risks before they occur and to specify any planned risk-reduction measures is considered cloud security management and control. Leading software developers now routinely adhere to the principles and practices of cloud security management. These results are included in a study that discusses how to manage security concerns in cloud computing in government organizations. These models have used simple linear regression and the spearman's rank correlation coefficient (SVMR). The adaptive neural fuzzy inference system (ANFIS) approach will be used in future work to see if it is successful in reducing the occurrence of each factor issue relationships between issues that control and evaluate the results (SVMR and ANFIS) for suitable for controlling cloud computing by using risk mitigation practices on cloud security platform and infrastructure, as well as identify and discuss cloud security controls to mitigate.




## REFERENCES

- [1] K. Q. Aziz and B. A. Mahmood, "Assured data deletion in cloud computing: security analysis and requirements," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 2, pp. 1174–1183, 2022, doi: 10.11591/ijeecs.v28.i2.pp1174-1183.
- [2] B. J. Khadhim, Q. K. Kadhim, W. M. Khudhair, and M. H. Ghaidan, "Virtualization in mobile cloud computing for augmented reality challenges," *Proc. 2021 2nd Inf. Technol. to Enhanc. E-Learning other Appl. Conf. IT-ELA 2021*, no. June 2022, pp. 113-118, 2021, doi: 10.1109/IT-ELA52201.2021.9773680.
- [3] A. Rehman, L. I. U. Jian, M. Q. Yasin, and L. I. Keqiu, "Securing cloud storage by remote data integrity check with secured key generation," *Chinese J. Electron.*, vol. 30, no. 3, pp. 489–499, 2021, doi: 10.1049/cje.2021.04.002.
- [4] M. Mustafa, M. Alshare, D. Bhargava, R. Neware, B. Singh, and P. Ngulube, "Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems," *Comput. Math. Methods Med.*, vol. 2022, no. 4, pp. 1–10, 2022, doi: 10.1155/2022/6112815.
- [5] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: a survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.
- [6] J. Kumar, "Cloud computing security issues and its challenges: A comprehensive research," *Int. J. Recent Technol. Eng.*, vol. 8, no. 1, pp. 10–14, 2019, doi: 10.1016/S1350-4789(19)30370-8.
- [7] I. Nazeeh, T. H. Hadi, Z. Q. Mohammed, S. T. Ahmed, and Q. K. Kadhim, "Optimizing blockchain technology using a data sharing model," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 1, p. 431, 2023, doi: 10.11591/ijeecs.v29.i1.pp431-440.
- [8] A. Irsheid, A. Murad, M. AlNajdawi, and A. Qusef, "Information security risk management models for cloud hosted systems: A comparative study," *Procedia Comput. Sci.*, vol. 204, pp. 205–217, 2022, doi: 10.1016/j.procs.2022.08.025.
- [9] S. T. Ahmed, B. J. Khadhim, and Q. K. Kadhim, "Cloud services and cloud perspectives: a review," in *IOP Conference Series: Materials Science and Engineering*, 2021, p. 012078, doi: 10.1088/1757-899X/1090/1/012078.
- [10] M. Ishak, R. Rahman, and T. Mahmud, "Integrating cloud computing in e-healthcare: system design, implementation and significance in context of developing countries," *2021 5th Int. Conf. Electr. Eng. Inf. Commun. Technol. ICEEICT 2021*, no. March, pp. 0–6, 2021, doi: 10.1109/ICEEICT53905.2021.9667831.
- [11] R. Mudzamba, K. v. d. Schyff, and K. Renaud, "The challenges of cloud adoption among South African small to medium enterprises: A thematic analysis," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 88, no. 6, pp. 1–18, 2022, doi: 10.1002/isd2.12235.
- [12] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, and S. F. Abdulkareem, "Iraqi e-government and cloud computing development based on unified citizen identification," *Period. Eng. Nat. Sci.*, vol. 7, no. 4, pp. 1776–1793, 2019, doi: 10.21533/pen.v7i4.840.
- [13] B. S. Shukur, M. Khanapi, A. Ghani, and M. A. Burhanuddin, "An analysis of cloud computing adoption framework for Iraqi e-Government," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. September, pp. 104–112, 2018, doi: 10.14569/IJACSA.2018.090814.
- [14] Y. A. Najm, S. Alsamarac, and A. A. Jalal, "Cloud computing security for e-learning during COVID-19 pandemic," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 3, pp. 1610–1618, 2022, doi: 10.11591/ijeecs.v27.i3.pp1610-1618.
- [15] A. Taherkordi, F. Zahid, Y. Verginadis, and G. Horn, "Future cloud systems design: challenges and research directions," *IEEE Access*, vol. 6, pp. 74120–74150, 2018, doi: 10.1109/ACCESS.2018.2883149.
- [16] H. S. M. Alsultani, Q. Kanaan, and I. Y. Khudhair, "Empirical investigation of TCP incast congestion in wireless cloud computing networks," *J. Comput. Sci.*, vol. 14, no. 5, 2018, doi: 10.3844/jcssp.2018.663.672.
- [17] M. Ali, S. Malik, Z. Khalid, M. M. Awan, and S. Ahmad, "Security issues, threats and respective mitigation in cloud computing – a systematic review," *Int. J. Sci. Technol. Res.*, vol. 9, no. 08, pp. 474–484, 2020.
- [18] Q. Kanaan, H. S. Mahdi, and H. K. Ail, "Storage architecture for network security in cloud computing," *Diyala J. Pure Sci.*, vol. 14, no. 1, pp. 1–17, 2018, doi: 10.1016/S1569-9056(18)30018-6.
- [19] V. N. KN, "Identification of data analytics security challenges for big data and cloud computing," *Elem. Educ. Online*, vol. 20, no. 1, pp. 5369–5374, 2021, doi: 10.17051/ilkonline.2021.01.570.
- [20] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 71, no. July 2017, pp. 28–42, 2018, doi: 10.1016/j.compeleceng.2018.06.006.




- [21] M. K. S. Alwaheidi and S. Islam, "Data-driven threat analysis for ensuring security in cloud enabled systems," *Sensors*, vol. 22, no. 15, pp. 1–24, 2022, doi: 10.3390/s22155726.
- [22] Q. K. Kadhim, R. Yusof, H. S. Mahdi, S. S. Ali Al-Shami, and S. R. Selamat, "A review study on cloud computing issues," in *Journal of Physics: Conference Series*, Jun. 2018, vol. 1018, no. 1, doi: 10.1088/1742-6596/1018/1/012006.
- [23] M. Mehrtak *et al.*, "Security challenges and solutions using healthcare cloud computing," *J. Med. Life*, vol. 14, no. 4, pp. 448–461, 2021, doi: 10.25122/jml-2021-0100.
- [24] D. Hyseni, N. Piraj, B. Çiço, and I. Shabani, "The use of reactive programming in the proposed model for cloud security controlled by ITSS," *Computers*, vol. 11, no. 5, pp. 1–14, 2022, doi: 10.3390/computers11050062.
- [25] Q. K. Kadhim, R. Yusof, and S. R. Selamat, "The cloud computing control in the government services," *Jour Adv Res. Dyn. Control Syst.*, vol. 10, no. 04, pp. 1136–1147, 2018.
- [26] L. Yang, "Research on the realization path of college english education based on the SVM algorithm model under the background of cloud computing and wireless communication," *Sci. Program.*, vol. 2021, pp. 1–7, 2021, doi: 10.1155/2021/6182824.
- [27] B. J. Khadhim, Q. K. Kadhim, W. K. Shams, S. T. Ahmed, and W. A. W. Alsiadi, "Diagnose COVID-19 by using hybrid CNN-RNN for chest X-ray," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 2, pp. 852–860, 2023, doi: 10.11591/ijeecs.v29.i2.pp852-860.
- [28] G. Cha, H. Moon, and J. Kim, "A method to improve the performance of support vector machine regression model for predicting demolition waste generation using categorical principal components analysis," *Int. J. Sustain. Build. Technol. Urban Dev.*, vol. 12, no. 3, pp. 282–294, 2021, doi: 10.22712/susb.20210023.

## BIOGRAPHIES OF AUTHORS






**Sanaa Hammad Dhahi**    is M.Sc. in Computer Science from Diyala University, Iraq, in 2020. Affiliation: University of Kerbala, Kerbala, Iraq: college of Tourism Sciences. Scientific research interest: natural language processing, machine translation, artificial intelligence, information security, information hiding, machine learning, deep learning and she can be contacted at email: sanaahammad@uodiyala.edu.iq.






**Estqlal Hammad Dhahi**    is M.Sc. in Computer Science from Science College for Women, University of Babylon Babil, Iraq. Affiliation: University of Kerbala, Kerbala, Iraq Department computer science. Scientific research interest: natural language processing, machine translation, artificial intelligence, information security, information hiding, machine learning, deep learning and she can be contacted at email: estqlal.h@uokerbala.edu.iq.



**Ban Jawad Khadhim**    is M.Sc. (at 2015) in (India). Department of Computer College of Basic Education University of Diyala, Diyala, Iraq. Research interests: artificial intelligence, deep learning, machine learning. She can be contacted at email: banJawad@uodiyala.edu.iq or ban.jawad.kadhim@basicedu.uodiyala.



**Shaymaa Taha Ahmed**    is M.Sc. (2015) in (India), Ph.D. in Computer Sciences/2022, The University of Technology, Baghdad, Iraq. Affiliation: University of Diyala Department computer science/College: basic of education Specialization: -Computer science/information system. Research interests: cloud computing-deep learning-machine learning-AI-data mining. She can be contacted at email: mrs.sh.ta.ah@gmail.com or shaymaa.taha.ahmed@basicedu.uodiyala.edu.iq.