AN INTELLIGENT SECURITY CENTERED RESOURCE-EFFICIENT RESOURCE MANAGEMENT MODEL FOR CLOUD COMPUTING ENVIRONMENTS

A PREPRINT

Deepika Saxena
Department of Computer Applications
National Institute of Technology
Kurukshetra, India
deepta_6180096@nitkkr.ac.in

Ashutosh Kumar Singh
Department of Computer Applications
National Institute of Technology
Kurukshetra, India
ashutosh@nitkkr.ac.in

November 1, 2022

ABSTRACT

This paper proposes a conceptual model for a secure and performance efficient workload management model in cloud environments. In this model, a resource management unit is employed for energy and performance proficient allocation of virtual machines while ensuring the secure processing of users’ applications by defending against the data breaches due to unauthorized access of virtual machines in real-time. The resource management unit is guided by a secure virtual machine management unit which is designed to generate information regarding unauthorized access or inter-communication links among active virtual machines. Also, a workload analyser unit operates concurrently to estimate resource utilization information to assist the resource management unit in performance efficient allocation of virtual machines. Contrary to prior works which engages access control mechanisms, and encryption and decryption of data before transfer, and use of tunnelling for prevention of an unauthorised access to virtual machines which raises excess computational cost overhead, the proposed model operates diversely for efficiently serving the same purpose.

Keywords Workload prediction · Resource allocation · Security · VM consolidation · VM migration

1 Introduction

Cloud Computing enabled with seamless pool of hardware and software resources with advanced computation and numerous benefits viz., service availability, reliability, elasticity, and maximum scalability at minimum upfront investment has driven business enterprise, scientific and research organisations towards the cloud datacentres [1–12]. The users requests or applications are executed on different virtual machines hosted on different severs within the datacentre [13–30]. The cloud virtualization technology facilitates elasticity for satisfying dynamically varying resource demands of users by allocating and deallocating required number of virtual machines on the shared physical servers [31–41]. However, the sharing of physical resources and processing of confidential applications on the third-party cloud servers prompts a biggest concern of ‘security’ among all the cloud users [9, 42–64].

The virtual machines dedicated for the processing of applications of a user needs to communicate for data exchange among them [43, 65–76]. Most of the data hacks and security attacks occur by reason of data transfer leveraging the security loopholes or vulnerabilities of compute, storage, and network devices within datacentre [77, 84]. Also, the co-location of virtual machines of multiple users on a common physical server often leads to malicious activities like, data hampering and leakage of cloud user’s sensitive information [7, 85, 95]. A malicious user or attacker may initiate one or group of virtual machines and exploit multiple network routes to attain co-residency with the target virtual

*The authors would like to thank National Institute of Technology Kurukshetra, India for financially supporting this research work.
The vulnerability and susceptibilities of hypervisor or virtual machine management layer allow malicious user to easily compromise all the virtual machines hosted on it. Therefore, the key challenge for cloud datacentre is securing user data distributed on the shared physical servers while maintaining scalability of resources along with high performance and cost optimization [106][114].

The existing approaches furnished for securing real-time data communications among virtual machines and other different entities includes encryption and decryption of data before transfer, use of virtual private networks, tunnelling, and use of passwords, captchas for prevention of an unauthorised access to virtual machines of benign user etc. Also, minimization of the physical server sharing and periodic migration of virtual machines are some practices employed for reduction of security attacks and safeguarding online data execution and communication. Despite the adoption of aforementioned security upgrading measures, the misconfiguration and mismanagement at cloud platform is the topmost cause for leakage of terabytes of sensitive data of millions of cloud users across the world. Hence, a robust security mechanism during user data processing and communication at virtual machine placement and physical resource management level is needed to combat the aforementioned bottleneck problem of security threats in cloud environments.

2 Proposed Model

This section discusses an overview of the resource distribution and allocation of virtual machines for securing data execution and unauthorized access within the cloud datacenter in a simplified format that are further explained in the detailed description of the paper. The proposed conceptual model addresses the challenges of security breaches, virtual machine hijack and data leakage, network security attacks, unauthorized data access along with performance degradation due to server under/over-utilization by proposing a novel virtual machine security ingrained cloud resource allocation model. The architectural view of proposed model is illustrated in Fig. 1.

A resource management unit is employed to receive application execution requests from numerous users across the globe. These applications maybe received in any possible format such as high-performance computing applications, scientific workflows, military, medicinal or research-based applications, online business and marketing etc. The resource management unit divides these applications into one or more components or tasks to be executed concurrently on different virtual machines. All the virtual machines engaged in processing of the component of a common application needs to communicate and exchange information with each other builds a virtual network of virtual machines with authorized access links. The resource management unit store and maintains this information of authorized virtual machine links in an Authorized Virtual machine Access Database (AVAD).

The resource management unit assigns different tasks to distinct virtual machines deployed on various servers within the datacenter. During execution of tasks by different virtual machine, the resources viz., CPU, memory, disk, bandwidth utilization are recorded and Workload/Resource Usage Data Store is created and updated periodically. The information saved in this data store is provided as input for training and re-training of a machine learning based workload analyser. This workload analyser is employed to estimate the future resource utilization on different virtual machines and servers. The resource management unit utilizes estimated resource usage information in making various proactive decisions confined to load management such as creation, termination, or migration of different virtual machines, handling of over/under-load conditions of servers etc., for an efficient management of resources. The proposed model employed a Virtual Machine (VM) Security Management Unit to ensure secure execution of user application on group of virtual machines hosted on same or different servers. This unit allows monitoring of inter-communication links among active virtual machines in real-time and enable detection of attacker virtual machines for mitigation of security breaches within the datacenter. During task execution, the resource usage is collected to update workload data store and inter-communication links are monitored and stored in Current VM Access Links (CV AL) log. All the live inter-communication links among virtual machines are maintained in a log which helps to determine unauthorized access links and terminate attacker/malicious virtual machines before the occurrence of any security breaches. The proposed model is capable avoiding data security attacks because of new/unknown as well as known attacker virtual machine.

The present approach illustrates a general cloud computing environment accompanying role of management of resources within cloud environment wherein, cloud infrastructure comprises of clusters of servers connected via router networking device for communicating with one another as per the requirement. Each cluster comprises of numerous physical server machines of same or varying resource capacity. The resources may include Central Processing Unit (CPU), RAM, Disk memory, and bandwidth etc. The virtual machines which maybe in the form of computing, storage or networking instances are hosted on servers for processing of cloud user application requests. The cloud users \{User 1, User 2, ..., User n\} may send application requests to a Resource Management Unit for processing at the cloud infrastructure. The Resource Management Unit receives requests in the form of applications from various cloud users \{User 1, User 2, ..., User n\}. Moreover, it facilitates the virtual machine management including virtual machine scheduling,
Figure 1: Proposed model architectural overview
placement, migration, and handling over/under-loading conditions by reason of inefficient resource distribution among virtual machines. Further, it serves tasks management by performing the function of user application division into sub-components or tasks, assignment and scheduling of these tasks’ execution on different virtual machines. The output processed tasks belonging to an application are integrated to generate the response for the user retrieved via Resource Management Unit.

3 Secure Resource Management

Fig. 2 portrays a complete view of a secure and performance efficient load management model in cloud environment in accordance with the embodiment of the proposed model. The cloud users leverages services of cloud infrastructure by sending requests in the form of different applications to be received by the resource management unit. These applications are divided into tasks in accordance with the tasks management, which are assigned for execution to different virtual machines subject to the resource requirement of a task is lesser than or equals to the resource capacity of virtual machine in accordance with the virtual machine management. The virtual machines utilize physical resource capacity of the servers upon which they are hosted. The resource utilization or received workload information by different virtual machines on different servers are recorded in a Workload/Resource Usage Data Store. This information is used for periodic training and re-training of a machine learning algorithm based Workload Analyser Unit which is further described in detail in accordance with an embodiment of the proposed model as depicted in Fig. 3. The Workload Analyser Unit estimates future resource requirement on each server for successful execution of user requests by the respective virtual machines avoiding any performance degradation due to sudden upsurge or plunge in the forthcoming workload. This predicted resource usage information is passed to the resource management unit to provide it with the knowledge of the expected variance in the forthcoming workload and adjust the entire load with proficiency by handing all the under-utilization and over-utilization of resources proactively. The resource management unit creates
virtual networks of a group of active virtual machines by considering the trivial fact that all the virtual machines involved in execution of a common application are in communication, exchanging data with each other, are legally authorized to access data of one another. The resource management unit 208 also builds and maintains Authorized virtual machine (VM) Access Database (AVAD) by utilizing the link access information of aforesaid virtual networks of virtual machines. A virtual machine (VM) Security Management Unit in accordance with the embodiment of the proposed model, which is capable of providing an effective security during execution of user application within the cloud infrastructure. It comprises of a monitor which observes live communication links among active virtual machine continuously in real-time. This monitor analyses virtual machine link access patterns wherein, the group of virtual machines involved in exchanging data among them generates live virtual networks of active virtual machines. The knowledge produced by these access links is utilized to create Online VM Access Log which is further utilized by the secure VM allocation unit which makes decisions of shifting, terminating, creating, re-allocating virtual machines in the favour of security of user data under processing.

The virtual networks for live communication among virtual machines are monitored and recorded in a log named Current VM Access Links Log (CVAL). The information captured in this log about inter-communication among active virtual machines is analysed and compared with Authorised VM Access Database (AVAD) which is generated by resource management unit. All the mis-matched link are identified for detection and termination of unauthorized access links and attacker virtual machines prior to occurrence of successful security breaches. The present approach utilizes the knowledge produced by comparative analysis between AVAD and CVAL to furnish active virtual machines security decisions in real-time.

4 Resource Management

A block diagram as illustrated in Fig. 3 is provided to elucidate an implementation of high performance and energy-proficient resource management in accordance with resource management unit presented in Fig. 2 of the proposed model. The historical and live resource utilization information from the cloud infrastructure is stored in a resource usage data store. This is information is pre-processed by applying feature selection and normalization techniques which maybe performed using any appropriate machine learning method; such as Decision Tree, Boruta Forest, ChiSquare, or Random Forest etc. for feature selection and Linear scaling, Clipping, Max-Min algorithm, Z-score etc. for normalization of input data within a specific range. The normalized resource usage data is provided to Machine Learning based Resource Usage Analyser for training and re-training periodically in real-time. This analyser maybe developed using any of the prediction methods such as Neural Network perceptron trained with help of an optimization algorithm, Deep Neural Network, Long Short Term Memory based Recurrent Neural Network (LSTM-RNN) etc. The periodic training of the prediction module rejuvenates the prediction model for improved and precise prediction of the respective resource utilization within cloud infrastructure. This prediction information is generated in the form of patterns of resource usage within a virtual machine and thus produces a pool of predicted resource usage of VMs. This estimated resource usage information is passed to resource management unit which corresponds to resource management unit for directing resource provisioning decisions. In case, the predicted capacity of resource usage is more than the physically available resource capacity of a server in the cluster, an overloading is expected. The highest resource capacity virtual machines are migrated from the respective server for alleviation of such an overloading problem that may degrade the performance of entire cloud infrastructure. The highest resource capacity virtual machines are selected for migration in order to avoid the necessity of frequent migration. Also, in case of much lesser predicted capacity of resource usage than the actual capacity of server, an underloading problem is estimated wherein, such an underloaded server maybe turned off after shifting the virtual machines hosted on them to some other active server subject to resource capacity constraints.

The resource usage information from workload data store maybe use for periodic training/re-training of machine learning based resource usage analyser for estimation of future workload and resource utilization. The information of inter-access link among active virtual machines in CVAL are compared with that of AVAD. If the outcome of the comparison block is ’NO’, any security breach is detected proactively which requires enough time for surpassing the security defence and actual occurrence of the successful attack and terminate the unauthorised links among respective VMs before initiation of data transmission, otherwise, no post-action is needed. Accordingly, the knowledge of predicted resource usage and unauthorized inter-communication links are passed to resource management unit that may allocate/deallocate or migrate virtual machines based on server resource capacity and security status of virtual machines.

5 Illustrations

The effectiveness of the present approach against a co-residency attack is provided in accordance with an engagement of the proposed model. Let us assume that User 1 application’s component tasks are executing on multiple virtual
machines, among which one of the virtual machines is co-located with an attacker’s virtual machine who may launch a side-channel or co-residency attack on all the virtual machines of User 1 by reason of networking links among them. Such an attack requires sufficient time for breaching the security boundaries of target virtual machine to launch a successful attack. The proposed model continuously monitors, records and analyses the inter-communication links among active virtual machines which successfully points out the unauthorized link as soon as it is developed. As depicted in proposed approach, the attacker virtual machine is detected and terminated providing successful defence against the security breach prior to its occurrence.

The working strategy of the present approach against a multiple virtual machines hijack attack in accordance with an embodiment of the proposed model can be illustrated as follows. Suppose an attacker launched multiple virtual machines for maximum data breaches simultaneously by exploiting co-residency effect. Since, the proposed model continuously monitors, records and analyses the inter-communication links among active virtual machines which successfully points out the multiple unauthorized links as soon as they are developed. The VM Security Analysis unit detects and terminates all attacker virtual machines involved in data breaches via unauthorized access links before occurrence of successful attack.

Furthermore, the virtual machine security mechanism of the present approach against a grouped virtual machines attack targeting a single virtual machine in accordance with the proposed model can be realised with the subsequent example. Consider an attacker launched multiple virtual machines to reach the target virtual machine via unauthorized link using network cascading effect. Since, the proposed model continuously monitors, records and analyses the inter-communication links among active virtual machines which successfully points out the multiple unauthorized links as soon as they are developed. The VM Security Analysis unit detects and terminates all attacker virtual machines involved in such an attack via unauthorized access links prior to its success.
6 Conclusions

The proposed conceptual model for security and performance efficiency of cloud computing environment is a novel approach accomplishing two conflicting objectives concurrently. This paper presented an architectural and operational design of the proposed model with essential illustrations to validate the effectiveness of the proposed approach. In future, the authors envision to implement this model and compare it with existing state-of-the-art approaches.

References

[1] A. K. Singh, D. Saxena, J. Kumar, and V. Gupta, “A quantum approach towards the adaptive prediction of cloud workloads,” IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 12, pp. 2893–2905, 2021.
[2] D. Saxena and S. Chauhan, “A review on dynamic fair priority task scheduling algorithm in cloud computing,” International Journal of Science, Environment and Technology, vol. 3, no. 3, pp. 997–1003, 2014.
[3] S. Saxena and D. Saxena, “Ewsa: An enriched workflow scheduling algorithm in cloud computing,” in 2015 International Conference on Computing, Communication and Security (ICCCS). IEEE, 2015, pp. 1–5.
[4] D. Saxena and S. Saxena, “Highly advanced cloudllet scheduling algorithm based on particle swarm optimization,” in 2015 Eighth International Conference on Contemporary Computing (IC3). IEEE, 2015, pp. 111–116.
[5] D. Saxena, R. Chauhan, and R. Kait, “Dynamic fair priority optimization task scheduling algorithm in cloud computing: concepts and implementations,” International Journal of Computer Network and Information Security, vol. 8, no. 2, p. 41, 2016.
[6] A. Singh and J. Kumar, “Secure and energy aware load balancing framework for cloud data centre networks,” Electronics Letters, vol. 55, no. 9, pp. 540–541, 2019.
[7] N. Singh and A. K. Singh, “Data privacy protection mechanisms in cloud,” Data Science and Engineering, vol. 3, no. 1, pp. 24–39, 2018.
[8] A. K. Singh and D. Saxena, “A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment,” Journal of Applied Security Research, pp. 1–24, 2021.
[9] A. K. Singh and I. Gupta, “Online information leaker identification scheme for secure data sharing,” Multimedia Tools and Applications, vol. 79, no. 41, pp. 31165–31182, 2020.
[10] S. Kumar, V. Talwar, V. Kumar, P. Ranganathan, and K. Schwan, “vmanage: loosely coupled platform and virtualization management in data centers,” in Proceedings of the 6th international conference on Autonomic computing. ACM, 2009, pp. 127–136.
[11] A. K. Singh and R. Gupta, “A privacy-preserving model based on differential approach for sensitive data in cloud environment,” Multimedia Tools and Applications, pp. 1–24, 2022.
[12] J. Kumar and A. K. Singh, “Dynamic resource scaling in cloud using neural network and black hole algorithm,” in 2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS). IEEE, 2016, pp. 63–67.
[13] N. Kumar, I. Hussain, B. Singh, and B. K. Panigrahi, “Mppt in dynamic condition of partially shaded pv system by using wode technique,” IEEE Transactions on Sustainable Energy, vol. 8, no. 3, pp. 1204–1214, 2017.
[14] J. Kumar, R. Goomer, and A. K. Singh, “Long short term memory recurrent neural network (lstm-rnn) based workload forecasting model for cloud datacenters,” Procedia Computer Science, vol. 125, pp. 676–682, 2018.
[15] I. Gupta and A. K. Singh, “A holistic view on data protection for sharing, communicating, and computing environments: Taxonomy and future directions,” arXiv preprint arXiv:2202.11965, 2022.
[16] J. Kumar and A. K. Singh, “Workload prediction in cloud using artificial neural network and adaptive differential evolution,” Future Generation Computer Systems, vol. 81, pp. 41–52, 2018.
[17] J. Kumar, D. Saxena, A. K. Singh, and A. Mohan, “Biphase adaptive learning-based neural network model for cloud datacenter workload forecasting,” Soft Computing, pp. 1–18, 2020.
[18] S. Chhabra and A. K. Singh, “Dynamic data leakage detection model based approach for mapreduce computational security in cloud,” in 2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS). IEEE, 2016, pp. 13–19.
[19] D. Varshney, B. Babukhanwala, J. Khan, D. Saxena, and A. K. Singh, “Plant disease detection using machine learning techniques,” in 2022 3rd International Conference for Emerging Technology (INCET). IEEE, 2022, pp. 1–5.
[20] J. Kumar and A. K. Singh, “Cloud resource demand prediction using differential evolution based learning,” in 2019 7th International Conference on Smart Computing & Communications (ICSCC). IEEE, 2019, pp. 1–5.

[21] S. Chhabra and A. K. Singh, “Oph-lb: Optimal physical host for load balancing in cloud environment.” Pertanika Journal of Science & Technology, vol. 26, no. 3, 2018.

[22] R. Patel, V. Choudhary, D. Saxena, and A. K. Singh, “Lstm and nlp based forecasting model for stock market analysis,” in 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFT). IEEE, 2021, pp. 52–57.

[23] S. Chhabra and A. K. Singh, “A probabilistic model for finding an optimal host framework and load distribution in cloud environment,” Procedia Computer Science, vol. 125, pp. 683–690, 2018.

[24] S. Chhabra and A. Singh, “Dynamic hierarchical load balancing model for cloud data centre networks,” Electronics Letters, vol. 55, no. 2, pp. 94–96, 2019.

[25] J. Kumar and A. K. Singh, “Adaptive learning based prediction framework for cloud datacenter networks’ workload anticipation.” Journal of Information Science & Engineering, vol. 36, no. 5, 2020.

[26] I. Gupta and A. K. Singh, “A confidentiality preserving data leaker detection model for secure sharing of cloud data using integrated techniques,” in 2019 7th International Conference on Smart Computing & Communications (ICSCC). IEEE, 2019, pp. 1–5.

[27] S. Chhabra and A. K. Singh, “Optimal vm placement model for load balancing in cloud data centers,” in 2019 7th International Conference on Smart Computing & Communications (ICSCC). IEEE, 2019, pp. 1–5.

[28] I. Gupta and A. K. Singh, “A probabilistic approach for guilty agent detection using bigraph after distribution of sample data,” Procedia Computer Science, vol. 125, pp. 662–668, 2018.

[29] T. N. Sasamal, A. K. Singh, and U. Ghanekar, “Efficient design of coplanar ripple carry adder in qca,” IET Circuits, Devices & Systems, vol. 12, no. 5, pp. 594–605, 2018.

[30] J. Kumar and A. K. Singh, “Cloud datacenter workload estimation using error preventive time series forecasting models,” Cluster Computing, vol. 23, no. 2, pp. 1363–1379, 2020.

[31] J. Kumar, A. K. Singh, and R. Buyya, “Ensemble learning based predictive framework for virtual machine resource request prediction,” Neurocomputing, vol. 397, pp. 20–30, 2020.

[32] J. Kumar and A. K. Singh, “A discussion and comparative study on security and privacy of smart meter data,” Journal of Communications Software and Systems, vol. 15, no. 2, pp. 173–185, 2019.

[33] N. Singh and A. K. Singh, “Sql-injection vulnerabilities resolving using valid security tool in cloud.” Pertanika Journal of Science & Technology, vol. 27, no. 1, 2019.

[34] J. Kumar, A. K. Singh, and R. Buyya, “Layer-based privacy and security architecture for cloud data sharing,” Journal of Communications Software and Applications, vol. 15, no. 2, pp. 173–185, 2019.

[35] I. Gupta and A. Singh, “A framework for malicious agent detection in cloud computing environment,” The Journal of Supercomputing, pp. 1–21, 2022.

[36] D. Saxena, K. S. Vaisla, and M. S. Rauthan, “Abstract model of trusted and secure middleware framework for multi-cloud environment,” in International Conference on Advanced Informatics for Computing Research. Springer, 2018, pp. 469–479.

[37] D. Saxena and A. K. Singh, “Auto-adaptive learning-based workload forecasting in dynamic cloud environment,” International Journal of Computers and Applications, pp. 1–11, 2020.

[38] A. K. Singh and J. Kumar, “A privacy-preserving multidimensional data aggregation scheme with secure query processing for smart grid,” The Journal of Supercomputing, pp. 1–21, 2022.

[39] I. Gupta, S. Mittal, A. Tiwari, P. Agarwal, and A. K. Singh, “Tidf-dlpm: Term and inverse document frequency based data leakage prevention model,” arXiv preprint arXiv:2203.05367, 2022.
D. Saxena and A. K. Singh, “Communication cost aware resource efficient load balancing (care-lb) framework for cloud datacenter,” *Recent Advances in Computer Science and Communications*, vol. 12, pp. 1–00, 2020.

I. Gupta, D. Gurnani, N. Gupta, C. Singla, P. Thakral, and A. K. Singh, “Compendium of data security in cloud storage by applying hybridization of encryption algorithm,” *TechRxiv*, 2022.

N. Raj, A. K. Singh, and A. K. Gupta, “Low voltage high output impedance bulk-driven quasi-floating gate self-biased high-swing cascode current mirror,” *Circuits, Systems, and Signal Processing*, vol. 35, no. 8, pp. 2683–2703, 2016.

I. Gupta and A. K. Singh, “Seli: statistical evaluation based leaker identification stochastic scheme for secure data sharing,” *IET Communications*, vol. 14, no. 20, pp. 3607–3618, 2020.

D. Saxena and A. Singh, “Security embedded dynamic resource allocation model for cloud datacentre,” in *Advances in communication and computational technology*. Springer, 2021, pp. 1455–1464.

I. Gupta, H. Mittal, D. Rikhari, and A. K. Singh, “Mlrm: A multiple linear regression based model for average temperature prediction of a day,” *arXiv preprint arXiv:2203.05835*, 2022.

B. Devkota, A. Alsadoon, P. Prasad, A. Singh, and A. Elchouemi, “Image segmentation for early stage brain tumor detection using mathematical morphological reconstruction,” *Procedia Computer Science*, vol. 125, pp. 115–123, 2018.

D. Saxena and A. K. Singh, “OSC-MC: Online secure communication model for cloud environment,” *IEEE Communications Letters*, 2021.

R. Gupta and A. K. Singh, “Differential and access policy based privacy-preserving model in cloud environment,” in *Advances in communication and computational technology*. Springer, 2021, pp. 1455–1464.

S. Deepika and S. A. Kumar, “A proactive autoscaling and energy-efficient vm allocation framework using online multi-resource neural network for cloud data center,” *Neurocomputing*, vol. 426, pp. 248–264, 2021.

I. Gupta, P. K. Yadav, S. Pareek, S. Shakeel, and A. K. Singh, “Auxiliary informatics system: an advancement towards a smart home environment,” 2022.

D. Saxena, I. Gupta, J. Kumar, A. Singh, and W. Xiaoqing, “A secure and multi-objective virtual machine placement framework for cloud data center,” *IEEE Systems Journal*, 2021.

I. Gupta and A. K. Singh, “Guim-smfd: guilty user identification model using summation matrix-based distribution,” *IET Information Security*, vol. 14, no. 6, pp. 773–782, 2020.

A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J. H. Park, “Secureiiot environment: Federated learning empowered approach for securing iot from data breach,” *IEEE Transactions on Industrial Informatics*, 2022.

I. Gupta and A. K. Singh, “An integrated approach for data leaker detection in cloud environment.” *Journal of Information Science & Engineering*, vol. 36, no. 5, 2020.

I. Gupta, R. Gupta, A. K. Singh, and R. Buyya, “Mlpm: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment,” *IEEE Systems Journal*, vol. 15, no. 3, pp. 4248–4259, 2020.

R. Gupta, D. Saxena, and A. K. Singh, “Data security and privacy in cloud computing: concepts and emerging trends,” *arXiv preprint arXiv:2108.09508*, 2021.

R. Gupta and A. K. Singh, “Privacy-preserving cloud data model based on differential approach,” in *2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T)*. IEEE, 2022, pp. 1–6.

S. R. Swain, A. K. Singh, and C. N. Lee, “Efficient resource management in cloud environment,” *arXiv preprint arXiv:2207.12085*, 2022.

L. Yu, L. Chen, Z. Cai, H. Shen, Y. Liang, and Y. Pan, “Stochastic load balancing for virtual resource management in datacenters,” *IEEE Transactions on Cloud Computing*, 2016.
[67] J. Kumar, A. K. Singh, and A. Mohan, “Resource-efficient load-balancing framework for cloud data center networks,” ETRI Journal, vol. 43, no. 1, pp. 53–63, 2021.

[68] H. M. Gaur, A. K. Singh, and U. Ghanekar, “An efficient design of scalable reversible multiplier with testability,” Journal of Circuits, Systems and Computers, p. 2250179, 2022.

[69] J. Kumar, A. K. Singh, and R. Buuya, “Self directed learning based workload forecasting model for cloud resource management,” Information Sciences, vol. 543, pp. 345–366, 2021.

[70] N. Singh, J. Kumar, A. K. Singh, and A. Mohan, “Privacy-preserving multi-keyword hybrid search over encrypted data in cloud,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2022.

[71] J. Nader, A. Alsadoon, P. Prasad, A. Singh, and A. Elchouemi, “Designing touch-based hybrid authentication method for smartphones,” Procedia Computer Science, vol. 70, pp. 198–204, 2015.

[72] J. Kumar, A. K. Singh, and R. Buyya, “Self directed learning based workload forecasting model for cloud resource management,” Information Sciences, vol. 543, pp. 345–366, 2021.

[73] N. Singh, J. Kumar, A. K. Singh, and A. Mohan, “Privacy-preserving multi-keyword hybrid search over encrypted data in cloud,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2022.

[74] J. Nader, A. Alsadoon, P. Prasad, A. Singh, and A. Elchouemi, “Designing touch-based hybrid authentication method for smartphones,” Procedia Computer Science, vol. 70, pp. 198–204, 2015.

[75] H. M. Gaur, A. K. Singh, and U. Ghanekar, “Testable designs of toffoli fredkin reversible circuits,” arXiv preprint arXiv:2108.07448, 2021.

[76] D. Saxena, R. Gupta, and A. K. Singh, “A survey and comparative study on multi-cloud architectures: emerging issues and challenges for cloud federation,” arXiv preprint arXiv:2108.12831, 2021.

[77] M. Choudhary, S. Jha, D. Saxena, A. K. Singh et al., “A review of fake news detection methods using machine learning,” in 2021 2nd International Conference for Emerging Technology (INCET). IEEE, 2021, pp. 1–5.

[78] S. Makaju, P. Prasad, A. Alsadoon, A. Singh, and A. Elchouemi, “Lung cancer detection using ct scan images,” Procedia Computer Science, vol. 125, pp. 107–114, 2018.

[79] R. Patel, V. Choudhary, D. Saxena, and A. K. Singh, “Review of stock prediction using machine learning techniques,” in 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2021, pp. 840–846.

[80] D. Saxena and A. K. Singh, “Vm failure prediction based intelligent resource management model for cloud environments,” in 2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T). IEEE, 2022, pp. 1–6.

[81] R. Gupta, D. Saxena, I. Gupta, and A. K. Singh, “Differential and triphase adaptive learning-based privacy-preserving model for medical data in cloud environment,” IEEE Networking Letters, 2022.

[82] D. Varshney, B. Babukhanwala, J. Khan, D. Saxena, and A. kumar Singh, “Machine learning techniques for plant disease detection,” in 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2021, pp. 1574–1581.

[83] D. Yang, A. Alsadoon, P. C. Prasad, A. K. Singh, and A. Elchouemi, “An emotion recognition model based on facial recognition in virtual learning environment,” Procedia Computer Science, vol. 125, pp. 2–10, 2018.

[84] D. Saxena and A. K. Singh, “High availability management model based on vm significance ranking and resource estimation for cloud applications,” IEEE Transactions on Services Computing, 2022.

[85] Z. Ge, P. Prasad, N. Costadopoulos, A. Alsadoon, A. Singh, and A. Elchouemi, “Evaluating the accuracy of wearable heart rate monitors,” in 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Fall). IEEE, 2016, pp. 1–6.

[86] S. Chhabra and A. Kumar Singh, “Security enhancement in cloud environment using secure secret key sharing,” Journal of Communications Software and Systems, vol. 16, no. 4, pp. 296–307, 2020.

[87] K. L. Goh and A. K. Singh, “Comprehensive literature review on machine learning structures for web spam classification,” Procedia Computer Science, vol. 70, pp. 434–441, 2015.

[88] S. Chhabra and A. K. Singh, “Dynamic resource allocation method for load balance scheduling over cloud data center networks,” Journal of Web Engineering, pp. 2269–2284, 2021.

[89] V. Sharma, S. Jalwa, A. R. Siddiqi, I. Gupta, and A. K. Singh, “A lightweight effective randomized caesar cipher algorithm for security of data,” in Evolutionary Computing and Mobile Sustainable Networks. Springer, 2021, pp. 411–419.
[90] A. Tripathi, U. Singh, G. Bansal, R. Gupta, and A. K. Singh, “A review on emotion detection and classification using speech,” in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.

[91] A. S. Chauhan, D. Rani, A. Kumar, R. Gupta, and A. K. Singh, “A survey on privacy-preserving outsourced data on cloud with multiple data providers,” in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.

[92] V. Sharma, S. Kaur, J. Kumar, and A. K. Singh, “A fast parkinson’s disease prediction technique using pca and artificial neural network,” in *2019 International conference on intelligent computing and control systems (ICICS)*. IEEE, 2019, pp. 1491–1496.

[93] P. K. Yadav, S. Pareek, S. Shakeel, J. Kumar, and A. K. Singh, “Advancements and security issues of iot & cyber physical systems,” in *2019 International Conference on Intelligent Computing and Control Systems (ICICS)*. IEEE, 2019, pp. 940–945.

[94] K. Kaur, I. Gupta, and A. K. Singh, “Data leakage prevention: e-mail protection via gateway,” in *Journal of Physics: Conference Series*, vol. 933, no. 1. IOP Publishing, 2017, p. 012013.

[95] R. Gupta, D. Saxena, I. Gupta, A. Makkar, and A. K. Singh, “Quantum machine learning driven malicious user prediction for cloud network communications,” *IEEE Networking Letters*, 2022.

[96] S. Tagliacane, P. Prasad, G. Zajko, A. Elchouemi, and A. K. Singh, “Network simulations and future technologies in teaching networking courses: Development of a laboratory model with cisco virtual internet routing lab (viril),” in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2016, pp. 644–649.

[97] A. Kesharwani, A. Nag, A. Tiwari, I. Gupta, B. Sharma, and A. K. Singh, “Real-time human locator and advance home security appliances,” in *Evolutionary Computing and Mobile Sustainable Networks*. Springer, 2021, pp. 37–49.

[98] A. Acharya, H. Prasad, V. Kumar, I. Gupta, and A. K. Singh, “Host platform security and mobile agent classification: A systematic study,” in *Computer Networks and Inventive Communication Technologies*. Springer, 2021, pp. 1001–1010.

[99] B. Pradhan, B. Singh, A. Bhoria, and A. K. Singh, “A comparative study on cipher text policy attribute based encryption schemes,” *International Journal of Engineering Research & Technology*, 2021.

[100] P. Tiwari, S. Mehta, N. Sakhuja, J. Kumar, and A. K. Singh, “Credit card fraud detection using machine learning: A study,” *arXiv preprint arXiv:2108.10005*, 2021.

[101] S. Jalwa, V. Sharma, A. R. Siddiqi, I. Gupta, and A. K. Singh, “Comprehensive and comparative analysis of different files using cp-abe,” in *Advances in Communication and Computational Technology*. Springer, 2021, pp. 189–198.

[102] G. S. Hura, A. K. Singh, and L. S. Hoe, *Advances in Communication and Computational Technology: Select Proceedings of ICACCT 2019*. Springer, 2020.

[103] D. Deepika, R. Malik, S. Kumar, R. Gupta, and A. K. Singh, “A review on data privacy using attribute-based encryption,” in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.

[104] R. Gupta and A. K. Singh, “A differential approach for data and classification service-based privacy-preserving machine learning model in cloud environment,” *New Generation Computing*, vol. 40, no. 3, pp. 737–764, 2022.

[105] R. Gupta, I. Gupta, D. Saxena, and A. K. Singh, “A differential approach and deep neural network based data privacy-preserving model in cloud environment,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–16, 2022.

[106] A. G. K. Leng, P. R. Kumar, A. K. Singh, and A. Mohan, “Link-based spam algorithms in adversarial information retrieval,” *Cybernetics and Systems*, vol. 43, no. 6, pp. 459–475, 2012.

[107] P. Agarwal, S. Mittal, A. Tiwari, I. Gupta, A. K. Singh, and B. Sharma, “Authenticating cryptography over network in data,” in *2019 International Conference on Intelligent Computing and Control Systems (ICICS)*. IEEE, 2019, pp. 632–636.

[108] P. Godha, S. Jadon, A. Patle, I. Gupta, B. Sharma, and A. K. Singh, “Architecture, an efficient routing, applications, and challenges in delay tolerant network,” in *2019 International Conference on Intelligent Computing and Control Systems (ICICS)*. IEEE, 2019, pp. 824–829.

[109] S. Chhabra and A. K. Singh, “A secure vm allocation scheme to preserve against co-resident threat,” *International Journal of Web Engineering and Technology*, vol. 15, no. 1, pp. 96–115, 2020.
[110] S. Islam, J. Keung, K. Lee, and A. Liu, “Empirical prediction models for adaptive resource provisioning in the cloud,” *Future Generation Computer Systems*, vol. 28, no. 1, pp. 155–162, 2012.

[111] S. Wang, H. Gu, and G. Wu, “A new approach to multi-objective virtual machine placement in virtualized data center,” in *2013 IEEE Eighth International Conference on Networking, Architecture and Storage*. IEEE, 2013, pp. 331–335.

[112] Y. Sharma, W. Si, D. Sun, and B. Javadi, “Failure-aware energy-efficient vr consolidation in cloud computing systems,” *Future Generation Computer Systems*, vol. 94, pp. 620–633, 2019.

[113] A. Beloglazov and R. Buyya, “Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers,” *Concurrency and Computation: Practice and Experience*, vol. 24, no. 13, pp. 1397–1420, 2012.

[114] A. Tripathi, U. Singh, G. Bansal, R. Gupta, and A. K. Singh, “Hedcm: Human emotions detection and classification model from speech using cnn,” *Workshop on Advances in Computational Intelligence*, 2021.