Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp. 4000-4009
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.413

Secured Cloud Service Provisioning Techniques With Iot

Dr. V. UMADEVI Computer Science, New Prince Shri Bhavani Arts and Science College. Chengalpattu. drumavenkatesh2002@gmail.com

Dr. R. ARUNADEVI Associate Professor, Dept. of Vidhya Sagar Women's College, aruna130273@gmail.com

ABSTRACT

Cloud computing is an on-demand accessibility of computer system resources without any organization by the user. With cloud computing, the users access files and use the applications from any device to access the Internet. Internet of things (IoT) is the system of interrelated computing devices, objects, animals or people provided with unique identifiers (UIDs) to transmit the data over the network without interaction. Security plays an essential role during the service provisioning process in cloud server. Secured cloud service provisioning is the allocation of the resources and services to the customer in secured manner. Many researchers introduced service provisioning techniques with better security in cloud environment. But, the data confidentiality and execution time performance was not improved. In order to address these problems, cloud service provisioning can be carried out using machine learning techniques in our research work.

Keywords: cloud computing, on-demand, security, cloud service provisioning, resources, data confidentiality, machine learning

I.INTRODUCTION

Cloud Computing is used for computing resources that delivered as the service over an internet. Cloud computing is the model for providing the services where the resources are retrieved from the web through internet based tools and applications. Cloud service provisioning denotes the processes for deployment and integration of cloud computing services within an enterprise IT infrastructure. It incorporated the policies, procedures and enterprise objective in sourcing the cloud services from service provider. Cloud computing security denoted the broad set of policies, technologies, applications to preserve IP, data, applications, services and linked infrastructure of cloud computing.

This paper is organized as follows: Section 2 explains on existing secured cloud service provisioning techniques with IoT. Section 3 presents the brief discussion about secured cloud service provisioning techniques. Section 4 describes the possible comparison between them. Section 5 describes the limitations and related works. Section 6 concludes the paper.

II.LITERATURE SURVEY

An end-to-end energy model was designed in [1] for Edge Cloud-based IoT platform. The models were employed in concrete scenario where data stream analysis was created with cameras positioned on the vehicles. However, the energy efficiency of cloud infrastructures was not enhanced for small-sized data centers to limit IoT on the global energy consumption. A resource-aware virtual machine migration technique was designed in [2]. The rapid variation in sensing environment was examined through server clustering process. But, the optimization technique was not used to place virtual machine on destination server.

A new cloud computing model was designed in [3] for context-aware Internet of Things (IoT) services. However, advanced service-binding adaptation was not carried out to enhance the computing platform utilization for cloud resource control and mobility management framework. A new OAuthing model was designed in [4] for IoT to allocate the user identity and devices. Every user data was handled through personal cloud instance with an improved security and isolation for devices and cloud services. But, data confidentiality level was not improved by OAuthing model. IoT devices communicate with each other through the Constrained Application Protocol (CoAP) in [5]. CoAP was performed to link with each other through Internet. However, system prototype was not employed for commercial deployment using CoAP.

A novel authentication scheme was introduced in [6] for IoT-based architectures with cloud servers. Through formal verification by Proverif, security robustness of authentication scheme was guaranteed. But, authentication accuracy was not increased using designed scheme. A practical attribute-based access control system was designed in [7] for IoT cloud with revocable attribute-based encryption scheme that allowed data owner to manage data user credentials. However, the response time was not reduced during access control by practical attribute-based access control system.

III. SECURED CLOUD SERVICE PROVISIONING IN CLOUD ENVIRONMENT

Cloud computing provides the infrastructure and platform for storing and processing the IoT data. Cloud presented infrastructure as a Service (IaaS) for storing the sensed data. Platform as a Service (PaaS) from cloud is employed to run analytics on data. Software as a Service (SaaS) presented the software to analyze the IoT data. Data generated by environment is stored in cloud for computation and analytics. The computation process is handled by virtual machines running on physical server in cloud.

A. End-to-end Energy Models for Edge Cloud-based IoT Platforms: Application to Data Stream Analysis in IoT

Internet of Things (IoT) is an increasing number of connected devices with development of data and energy-hungry services. The services are depending on the cloud infrastructure for storage and computing abilities, altering architecture into distributed one depending on the edge facilities presented by Internet Service Providers (ISP). An end-to-end energy model was introduced for edge cloud-based IoT platforms. The designed model was employed in the concrete scenario where the data stream analysis created by cameras inserted on vehicles. The validation joined measurements on real testbed running the targeted application for scaling-up with increasing number of IoT devices.

The end-to-end energy consumption of IoT platforms was carried out on the concrete use-case advantages of edge computing platforms for IoT concerning energy consumption. End-to-end energy models were introduced for estimating the consumption when offloading the computation from objects to edge or to core cloud depending on number of devices for trading-off between the response time and reliability. The validation use-case aimed Internet of Vehicles (IoV) that was convergence of mobile internet and IoT. Video streams from cameras were aimed for object detection and tracking. The energy consumption was computed through each part of the IoT platform where data lost their value when they failed to analyze.

B. Resource-aware virtual machine migration in IoT cloud

Internet of Things (IoT) is the promising model for enabling several applications to the network together through an internet. Smart city, smart grid, smart home and smart agriculture are few areas supported by IoT applications. A large volume of data is generated by IoT applications for computation, storage and analytics through the infrastructure and platform as service provided by cloud computing. In cloud-based IOT application, rapid variation in sensing environment resulted in the data flowing spikes into the cloud. Internet of Things (IoT) combined the physical world with computer-based system to function smartly. Physical devices linked with sensors collected the environmental data and suitable actuation was carried out after the data examination.

A resource-aware migration technique was introduced to provide an uninterrupted service for IoT cloud environment. IoT computation jobs were allocated in the cloud computing. The weather prediction and fertilizer suggestion was carried out for identifying the resource starvation of virtual machine. The virtual machines were migrated to the destination server depending on preference function. Resource-aware VM migration technique was introduced to accommodate the rapid resource requirement of IoT application. The resource utilization of cloud server was monitored and virtual machines were positioned on the destination server. The data from IoT application were kept intact and effective service was presented in terms of the computation and analytics. The computation and analytics were carried out by the Hadoop cloud with lesser downtime and migration time.

C. Hierarchical Cloud Computing Architecture for Context-Aware IoT Services

A new cloud computing model was introduced to construct the hierarchical macroscopic and microscopic control architecture using cloud control layer (CCL) and user control layer (UCL) for context-aware Internet of Things (IoT) services. CCL handled the cloud resource distribution, service scheduling, service profile and service adaptation policy from system quality of service (QoS) through considering all context aware IoT services. UCL handled the end-to-end service connection and service context from user performance. UCL managed every context-aware service from user QoS point of view. The designed model supported non-uniform service binding and real-time adaptation through meta-objects that presented the application-specific computing environment at platform-level.

The real-time adaptable service binding comprised application and transmission bindings. It maintained the binding-wise hierarchical adaptation management. The designed service binding utilized the meta-object-based reflective system. The designed platform presented the intelligent service context management through supervised and reinforcement learning-based machine learning technique. A lightweight prototype of computing model was introduced with uniform binding-based legacy computing techniques. The designed platform were employed for the environmental sensor, actuator, service-agent devices and network devices as core function of computing infrastructure for presenting the intelligent IoT services. The designed platform comprised innovative business opportunities in the cloud computing where service providers and network operator take co-responsibility for enhancing the reliability and scalability performance of the services.

IV.COMPARISON OF SECURED SERVICE PROVISIONING TECHNIQUES IN CLOUD ENVIRONMENT

In order to compare the secured service provisioning techniques in cloud environment, number of cloud user request is taken to perform the experiment. Various parameters are used for providing secured services with better performances.

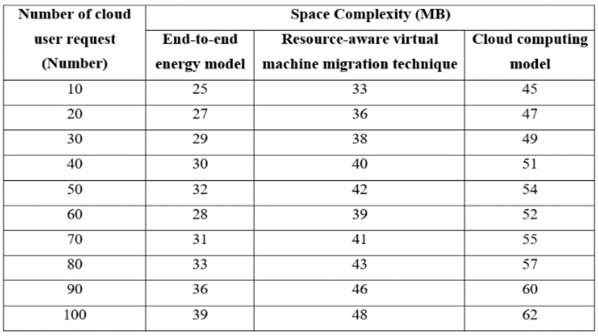
A. Space Complexity

Space complexity is defined as the amount of memory space utilized for performing the secured service provisioning in cloud. It is measured in terms of megabytes (MB). It is formulated as,

$$\text{Space complexity} = \text{Total memory} - \text{unused memory space} \qquad (1)$$

From (1), the space complexity is calculated. When the space complexity is lesser, the method is said to be more efficient.

Table 1 Tabulation for Space Complexity



Number of cloud user request (Number)	Space Complexity (MB)		
	End-to-end energy model	Resource-aware virtual machine migration technique	Cloud computing model
10	25	33	45
20	27	36	47
30	29	38	49
40	30	40	51
50	32	42	54
60	28	39	52
70	31	41	55
80	33	43	57
90	36	46	60
100	39	48	62

Table 1 explains the space complexity with respect to number of cloud user requests ranging from 10 to 100. Space complexity comparison takes place on existing end-to-end energy model, resource-aware virtual machine migration technique and cloud computing model. The graphical analysis of space complexity is illustrated in figure 1.

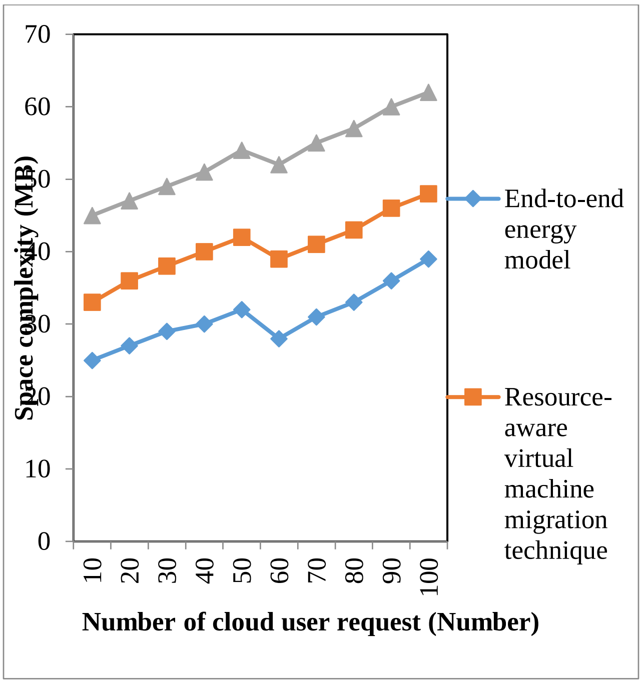


Figure 1 Measurement of Space Complexity

As described in figure 1, space complexity for different number of cloud user request is described. From the figure, it is clear that end-to-end energy model consumed lesser space when compared to the resource-aware virtual machine migration technique and cloud computing model. This is because of estimating the consumption when computation offloading from objects to the edge or to the cloud depending on number of devices and QoS application for trading-off between response time and reliability. Research in end-to-end energy model increases data confidentiality rate by 24% than resource-aware virtual machine migration technique and by 42% than cloud computing model.

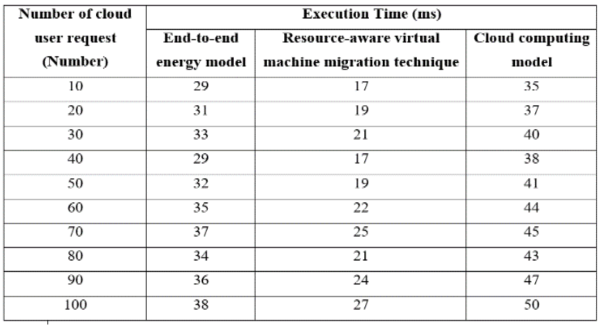
B. Execution Time

Execution time is defined as the amount of time taken to perform the secured service provisioning in cloud environment. It is defined as the difference of starting time and ending time for secured service provisioning. It is measured in terms of milliseconds (ms). It is given by,

$$\text{Execution Time} = \text{Ending time} - \quad \text{Starting time for secured service provisioning} \qquad (2)$$

From (2), the execution time is calculated. When the execution time is lesser, the method is said to be more efficient.

Table 2 Tabulation for Execution Time



Number of cloud user request (Number)	Execution Time (ms)		
	End-to-end energy model	Resource-aware virtual machine migration technique	Cloud computing model
10	29	17	35
20	31	19	37
30	33	21	40
40	29	17	38
50	32	19	41
60	35	22	44
70	37	25	45
80	34	21	43
90	36	24	47
100	38	27	50

Table 2 explains the execution time with respect to number of cloud user requests ranging from 10 to 100. Execution time comparison takes place on existing end-to-end energy model, resource-aware virtual machine migration technique and cloud computing model. The graphical analysis of execution time is described in figure 2.

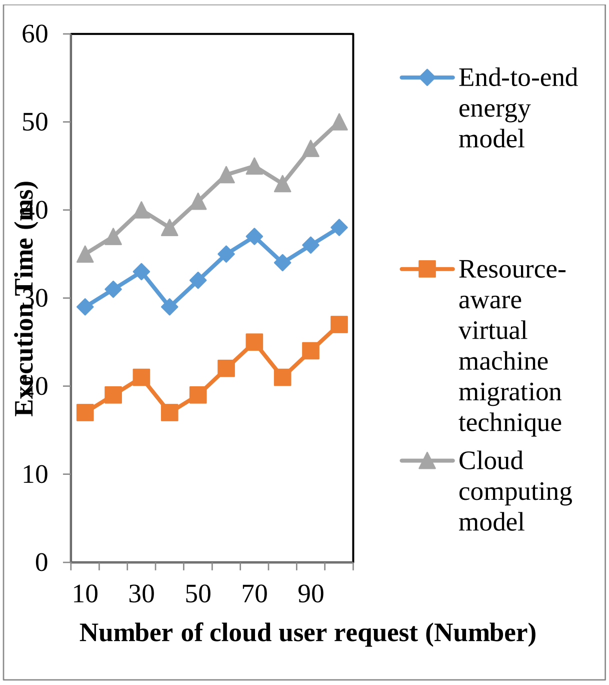


Figure 2 Measurement of Execution Time

In figure 2, execution time comparison for different number of cloud user request is explained. From figure, it is observed that resource-aware virtual machine migration technique consumed lesser time when compared to end-to-end energy model and cloud computing model. This is because, the virtual machines were migrated to destination server depending on the preference function. The designed technique was employed to accommodate the rapid resource requirement of IoT application. The designed technique presented computation and analytics with lesser downtime and migration time. Research in resource-aware virtual machine migration technique reduced the execution time by 37% than end-to-end energy model and by 50% than Cloud computing model.

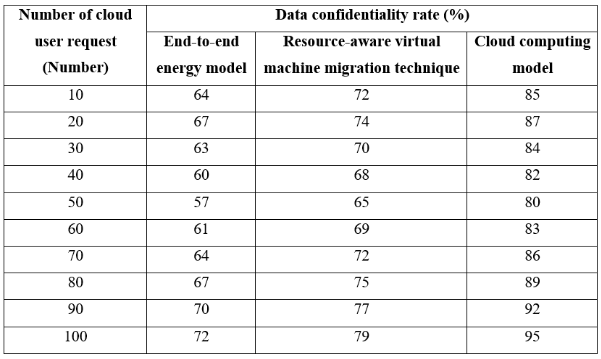
C. Data Confidentiality Rate

Data confidentiality rate is the ability to preserve the data from unauthorized access in cloud server. It is described as ratio of number of cloud user request that are accessed only by the authorized cloud server to the total number of cloud user request. It is measured in terms of percentage (%). It is formulated as,

$$\text{DCR} = \frac{\text{Number of cloud user request accessed by authorized server}}{\text{Number of cloud user request}} * 100 \qquad (3)$$

From (3), the data confidentiality rate is computed. When the data confidentiality rate is higher, the method is said to be more efficient.

Table 3 Tabulation for Data Confidentiality Rate



Number of cloud user request (Number)	Data confidentiality rate (%)		
	End-to-end energy model	Resource-aware virtual machine migration technique	Cloud computing model
10	64	72	85
20	67	74	87
30	63	70	84
40	60	68	82
50	57	65	80
60	61	69	83
70	64	72	86
80	67	75	89
90	70	77	92
100	72	79	95

Table 3 describes the data confidentiality rate with respect to number of cloud user requests ranging from 10 to 100. Data confidentiality rate comparison takes place on existing end-to-end energy model, resource-aware virtual machine migration technique and cloud computing model. The graphical analysis of data confidentiality rate is explained in figure 3.

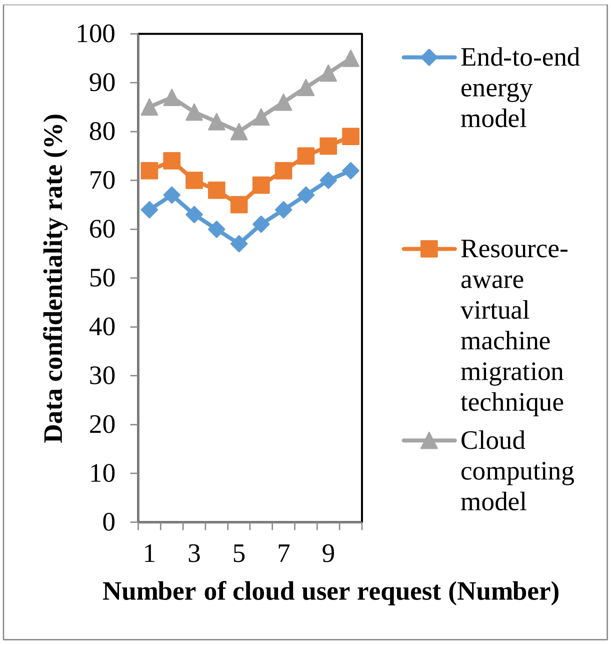


Figure 3 Measurement of Data Confidentiality Rate

From figure 3, data confidentiality rate for different number of cloud user request is illustrated. Cloud computing model attained higher data confidentiality rate when compared to end-to-end energy model and resource-aware virtual machine migration technique. This is because of constructing the cloud computing model hierarchical macroscopic and microscopic control architecture for context-aware Internet of Things (IoT) services. The designed model supported the non-uniform service binding and real-time adaptation through meta-objects at the platform-level. Research in Cloud computing model increases the data confidentiality rate by 34% than end-to-end energy model and by 20% than resource-aware virtual machine migration technique.

V. DISCUSSION AND LIMITATION ON SECURED CLOUD SERVICE PROVISIONING TECHNIQUES

An end-to-end energy models were introduced for edge cloud-based IoT platform. The designed models were used in concrete scenario where data stream analysis created through cameras positioned on vehicles. Video streams were introduced for identifying object detection and tracking ability. The validation combined dimension on real test-bed running targeted application for learning with number of IoT devices. The energy efficiency of cloud infrastructure was not enhanced for small-sized data centers to boundary IoT on global energy consumption. Cloud computing model maintained non-uniform service binding and real-time adaptation through the meta-objects. It supported intelligent service-context management by supervised and reinforcement learning framework. However, the advanced service-binding adaptation was not carried out for cloud resource control to improve the utilization of computing platform.

Resource-aware virtual machine migration technique observed fast variation in sensing field through server clustering. The data from IoT application were maintained intact and effective service was presented in terms of computation and analytics. The designed technique reduced the migration time and downtime in cloud. The designed technique introduced an uninterrupted service to an IoT environment. However, optimization technique was not used to place the virtual machine on destination server.

A.Related Works:
A new Chinese Remainder Theorem (CRT)-based data storage mechanism was designed in [8] for storing the user data in cloud database. A new group key management scheme was designed with CRT to access encrypted data from the cloud database. However, designed mechanism failed to reduce the computational complexity over the cloud and IoT-based applications. A security-enhanced attestation technology was performed in [9] for remote terminals to attain the shielded execution for measurements and attestation programs. A policy-based measurement mechanism was introduced where sensitive data with secret keys and policy details were covered with enclave-specific keys. However, authentication was not performed in efficient way to enhance the security level. A cloud-based fine-grained health information access control framework was designed in [10] for lightweight IoT devices with data auditing and attribute revocation function. But, the data accessing time was not minimized through cloud-based fine-grained health information access control framework.

B. Future Direction
The future direction of the work can be carried out using machine learning and ensemble learning techniques for secured service provisioning in cloud environment with higher data confidentiality and lesser time consumption.

VI.CONCLUSION

A comparison of different secured service provisioning techniques in cloud environment is studied. From survival study, the energy efficiency of cloud infrastructure was not improved for small-sized data centers to boundary IoT on global energy consumption. In addition, the advanced service-binding adaptation was not carried out for cloud resource control to increase the utilization of computing platform. The optimization technique was not utilized for positioning the virtual machine on the destination server. The wide range of experiments on existing techniques computed the comparative results of different classification techniques with its limitations. Finally from the limitation identified, further research work can be carried out for improving the performance of data confidentiality and execution time during the service provisioning in cloud by using machine learning techniques.

REFERENCES

[1] Yunbo Li, Anne-Cecile Orgerie, Ivan Rodero, Betsegaw Lemma Amersho, Manish Parashar, Jean-Marc Menaud, “End-to-end Energy Models for Edge Cloud-based IoT Platforms: Application to Data Stream Analysis in IoT”, Future Generation Computer Systems, Elsevier, Volume 87, October 2018, Pages 667-678

[2] Getzi Jeba Leelipushpam Paulraj, Sharmila Anand John Francis, J. Dinesh Peter and Immanuel Johnraja Jebadurai, “Resource-aware virtual machine migration in IoT cloud”, Future Generation Computer Systems, Elsevier, Volume 85, August 2018, Pages 173-183

[3] Tae-Dong Lee, Byung Moo Lee, and Wonjong Noh, “Hierarchical Cloud Computing Architecture for Context-Aware IoT Services”, IEEE Transactions on Consumer Electronics, Volume 64, Issue 2, May 2018, Pages 222 – 230

[4] Paul Fremantle and Benjamin Aziz, “Cloud-based federated identity for the Internet of Things”, Annals of Telecommunications, Springer, Volume 73, Issue 7–8, August 2018, Pages 415–427

[5] Md. Motaharul Islam, Zaheer Khan, Yazed Alsaawy, “A framework for harmonizing internet of things (IoT) in cloud: analyses and implementation”, Wireless Networks, Springer, February 2019, Pages 1-12

[6] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su and Wayne Chiu, “Lightweight IoT-based authentication scheme in cloud computing circumstance”, Future Generation Computer Systems, Elsevier, Volume 91, February 2019, Pages 244-251

[7] Shengmin Xu, Guomin Yang, Yi Mu and Ximeng Liu, “A Secure IoT Cloud Storage System with Fine-Grained Access Control and Decryption Key Exposure Resistance”, Future Generation Computer Systems, Elsevier, Volume 97, 2019, Pages 284-294

[8] Balasubramanian Prabhu Kavin and Sannasi Ganapathy, “A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications”, Computer Networks, Elsevier, Volume 151, 2019, Pages 181–190

[9] Juan Wang, Zhi Hong, Yuhan Zhang, and Yier Jin, “Enabling Security-Enhanced Attestation with Intel SGX for Remote Terminal and IoT”, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Volume 37, Issue 1, January 2018, Pages 88-96

[10] Lo-Yao Yeh, Pei-Yu Chiang, Yi-Lang Tsai, and Jiun-Long Huang, “Cloud-based Fine-grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation”, IEEE Transactions on Cloud Computing, Volume 6, Issue 2, April-June 2018, Pages 532 - 544