A New Security Mechanism For VCC Based On The Newly Modified Structure Of DES-3L Algorithm Using FC System

[1]S. Jerald Nirmal Kumar, [2]N.Suresh Kumar, [3]A.Suresh Kumar, [4]N.V.Kousik, [5]G.Kavithaa

[1&2&5]Assistant Professor, [3&4]Associate Professor,
[1,2,3&4]School of Compting Science and Engineering,
[1,2,3&4]Galgotias University, Greater Noida,
GautamBuddh Nagar District, Uttarpradesh – 201203
[5]Department of ECE, Government College of Engineering, Salem, TamilNadu - 636011

Abstract
Newly, vehicular cloud computing (VCC) has developed a striking explanation for vehicular computing and storage analysis requests. This calculation method can ensure low energy and traffic congestion. Counting, technology changed, making sure to obtain one on an imaginary platform when dealing with server data, such as power supply infrastructure or distributed data used by vehicles. The calculation does not guarantee security after the traditional contract was put in place, and its keys were leaked for purchase ensure that safe driving platform, Calculations are based on the use of a predictive cloud server configuration utility that introduces a newly modified method of the DES-3L algorithm, such as alternative data protection, privacy. The solution is used by way of an alternate to stunning data safety, reliability, and an automotive cloud server by an improved distributed clustering algorithm. In the case of user behavior and project analysis of mechanism, it can be advantageous to render bait files so that it is different from the records.

Keywords: -Vehicular cloud Computing (VCC), VANET, Cloud Computing, DES-3L, Improved distributed clustering algorithm (IDCA).

1. INTRODUCTION

Nowadays, auto companies use the computing cloud on both sides of the roads and streets for their smart vehicles to take advantage of the services provided to protect their data and through this technology. VCC services are usually based on subscription services. VCC Resource, Equipment Used by end-user or shared pool between vehicles. The nature of vehicles and how information and personal data are stored in cloud computing clusters lead to new security challenges.

The systematic security mechanism used to protect our VCC data today is not reasonably sufficient to prevent unauthorized users or vehicles from obtaining original user data access. The previous traditional information system, known as local network access, can only be parked locally using us locally. Through cumulative capacity and sum of related vehicles distributed vehicle computing technology by way of observed developing new computing models used by VCC, and Exposed entrance to databases from somewhere in the universe carries many security problems, especially confidence matters.

By registering with the VCC community, vehicles and users can contact their employees / create any resources they need to get out of work, anywhere in the world. However, the inconvenience above carries the safety of data leakage and security. To deal with VCC security and privacy issues, introduced a security mechanism based on IDCA. The vehicle will benefit from our service without changing the VCC registration system automatically through our network or adding any of their vehicle's hardware settings.

Existing encryption security mechanisms are not usually eligible for intruders and attackers' secure smart vehicle systems. Importantly, when accessing the available resources, the only focus of the encryption mechanism is the amount that the user pays for the key delivered without authenticating their individuality. So, these mechanisms do not show efficiency to ensure safety. A considerable quantity of private and isolated data is kept in the VCC cluster. Defensive all of the system is still one of the biggest challenges this information has to keep from intruding on others. Cloud computing has been implemented to mitigate the vulnerabilities that 330 million users have after the theft of Twitter data, as many technologies can do to the entrants. Recently, major system functions.

In direction to dazed VCC safety and trust problems, an innovative security mechanism based on IDCA attacked the system. By arrangement, display, and detect requests for unusual data access methods. In this system, as long as the original user data of the unattended attempts is accessed, the vehicle cloud can be implemented with various features similar to arranged request cloud, stable cloud, or both. The cloud on-demand develops a provisional resolution, which can be retrieved through enumerated members.

Through the Vehicular Network and Cloud Computing. Security and Privacy Issues These unregistered and malicious nodes are vulnerable to VC, which includes many security issues, including vehicle location, privacy, and members. Usually talking, owed to safety, then confidentiality here are main problems with the room being able to use networks that permit users toward a similar resource.

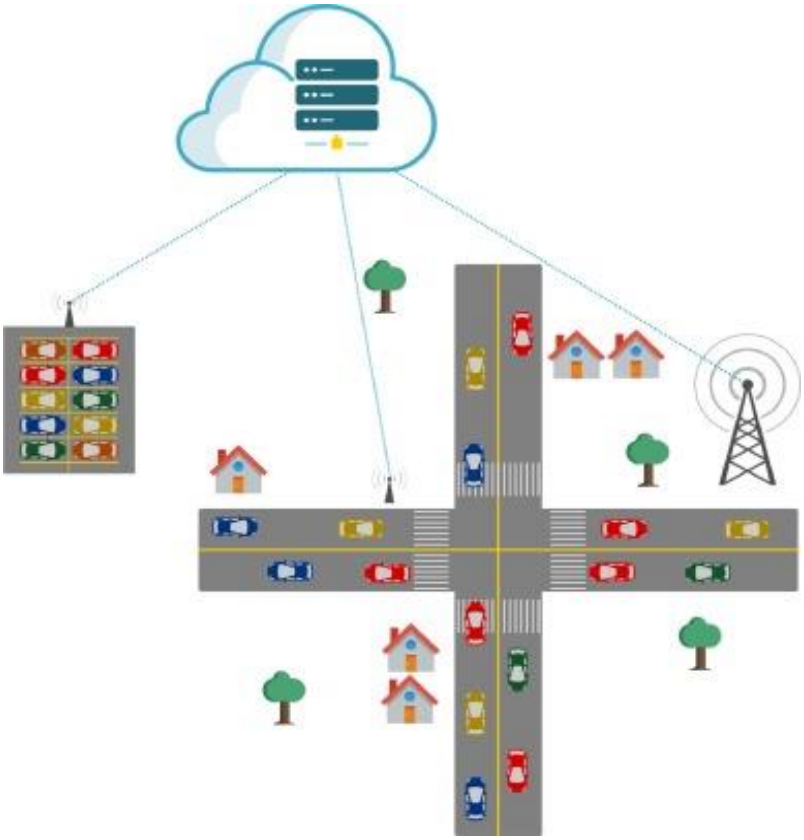


Figure.1 Vehicular Cloud Computing Architectures Applications

2. Relate Work

VCC faces poor security and privacy challenges. For example, a login data owner (DO) privacy leak could break into internal infrastructure or cloud servers to obtain sensitive data which could endanger the lives of travelers. To solve this problem, introduced Communist Abe [1], which also encrypted data which introduced particle access control of tools. However, the vehicle condition and environment were completely the same. The access system was monotonous before Ostrovsky et al. Compared to previous work on decision-making Daffier-Hellman defense linear, Lewko et al. (DBDH) attempts to build on attribute-based encryption, which is not a

proven monotony based on assumptions. Construction [2] has proven to be a fully committed and selective safe project.
Communist Abe is a promising research field that has attracted a great deal of attention from researchers.The attribute cancellation granted by the Confederate Communist Abbey, [3] is mediated. Like KP-Abe, there are a lot of power studies on Communist Abe. Further improvements are being made in this area[4]. In the case of personal health records, Li et al. It has gained security and scalability and granular access control, and supports modification of access policies and attributes. Liu et al. Do not think that privacy has a distinct significance, and that Communist Abe [5]. Adding to the existing, physicalfull efficient and secure Communist Abbey program sequel does not weaken its security.

The access permit system can be called an access tree with a certain size access tree at its node-shaped opening gate[6]. All existing programs enhance the functionality of the original CPABE [7] to suit different contexts. In this article,to introduce a new program to improve the compatibility of the original Communist Abbey with the VCC. Various investigative VANETs reported. Most of them provide the solution based on the encryption technology for counter attacks after VANETs. In calculation, the investigation work absorbed on security facilitiesdeprived ofseeing the needs of VANETs to be converted into hands-on applications.

A comprehensive study of VANETs covering architecture, protocols, simulation, and their full use areas has been launched [8]. However, they did not discuss threats and attacks on VANETs. [9], NidhalMejri et al. Release VANETs security and encryption solutions to respond to threats and attacks investigation. These VANETs do not include reliable models for dealing with threats and attacks. In addition, cleaners etc. [10] VCC has published a comprehensive study of its structure, security and privacy issues.Furthermore, it discusses the challenges and future directions of open research. Patel also conducted a study to ensure that Jhaveri [11] guided trust management based ethics by using trust management.

Sharma and Kaul[12] are discussing security threats and attacks, and are involved in counter-measures to ensure secure communications, Vcc introduced. VANETs use trust management through multiple intelligence reports. Note The company type cancellation insurance discusses goals, data-based and mixed trust model. Does execution work, do not know where the trust model entrusted with financial management in different ways will be used instead of cryptographic technology? VANETs are the problems and solutions that exist. The encryption method discussed by Khan and Gupta [13] only refers to the threat of VANETs and describes the Sibyl attack and its possible solutions.Mainly focused on security challenges[14], threats and attacks on VANETs, as well as authentication programs and privacy protection.

A comprehensive[15] revision of trust management model VANETs was launched, and a contrast of currentanswers between encryption and models discussed.It involves a specific belief model, but does not cover the entire belief management system [16]. The survey introduced the protocol guide into a trust management technology. It focuses on the asset finance management plan, which applies to the publication of useful information in real-time applications. -en, they provided a clear overview of the trust management plan and identified some open research challenges[17], from Sakiz and Sen security attacks and VANETs compatible detection algorithms, discussed later in the proposed solutions. Discussesthe characteristics of VANETs and their challenges,safety and confidentiality requirements, proposes various types of attacks on VANETs and site-related solutions. Provided a comprehensive investigation and changed the classification of VANETs fiction strategy [18]. -N, they discuss and compare with some related standards. Finally, they stressed some of the exposedstudy challenges of VANETs lengthwaysthroughcoming research directions.
A complete study was presented covered structure [19], safety, and self-reliance management of the VANETs system. In addition, network simulation and integrated simulations were discussed, but the privacy and security coverage of VANETs is still relatively small. An investigation was proposed using VANETs location privacy in mixed areas. Fake Strategy and Hybrid Zone Project Reviewed by Technology Privacy Protection VANETs. The proposed a survey that

would includefacilities[20], complete V2Vcommunication services and vehicle resource planning. V2V is highlighted if there are any issues related to communication and possible solutions. Alhaidari Detection Services (DDoS) have launched an investigation into the distribution of attacks based on VANETs of machine learning technology.

3. METHODOLOGY

Several security challenges can occur due to excessive movement of the room, such as node verification, stabilization, access control, data protection, and secure vehicle contact nodes.

3.1. Node Verification

VC plays a very important role in allowing authentication vehicles to verify user identity and information integrity before entering the vehicle network. In automotive networks, unsignedverification is a common practice, various authors used fictional methods that could protect and conceal vehicles.

3.2. Localization

Because VCC relies on vehicle location information for many applications such as collision alert, lane change alert, emergency alert, traffic-related information, broadcast data can play an important role in making connections. There are three types of VCC rating and integrated location information. The first also served as an active location integration model that could verify vehicle location using locator then GPS positioning equipment. The additional reflexive place integrity, the vehicle's location, is challenging to access without the use of radar. Third, VC estimates from low-level accuracy by filtering in the wrong High-level stabilization accuracy are the standard location integrity models**.**

3.3. Access Control

VC is a challenging issue where user identification is access control tested before accessing network resources. There are different access control levels in front of each user network, with its dedicated clusters are related based on its characteristics.

3.4. Data Security

The described vehicle cloud provides an effective way to stay in the vehicle's computing and storage resources. If vehicle safety requirements are not considered, the car can be accessed and stored using other vehicle data. Therefore, the stored data necessity be encoded to escape illegal access.

3.5. Secure Vehicular Communication

In-vehicle communication, the safe announcement plays a significant part in providing a safe and efficient driving experience. In an open-access environment, the room may be extra exposed toward attacks such as the way of interfering with indication vehicle communications, altering or deleting the room's publicized messages. For example, the attacker changes the news; they spread misinformation on the road due to traffic jams, traffic incidents, accidents, disasters, etc.

3.6 User behavior Algorithm

Mainly (IDCA) started collecting information about users. The incoming direct data is the old system's strategy to understand the user's behavior, and the system asks the user about the required data. While the user never enters information directly in our vehicle, the IDCA method is indirectly interested in focusing on the analysis of that user's data by some operator based on the vehicle. It is a continuous monitoring process that determines if abnormal access to information on the vehicle occurs from the security side. The film depicts security-based behavior and is mainly used by fraud detection police. Most data on fraudulent personal time are as follows:

- ✓ Enormous amount of information requested in no time.

- ✓ Effort to get login into account.
- ✓ In whatever way often characteristically a document read/write.
- ✓ ExaminationPIN and trial key.

In the following, define the algorithm notations.
Vehicles = V1, V2, V3, V4, V5 up to Vn
Log detailsV1m, V2m, V3m, V4m, V5m up to Vn

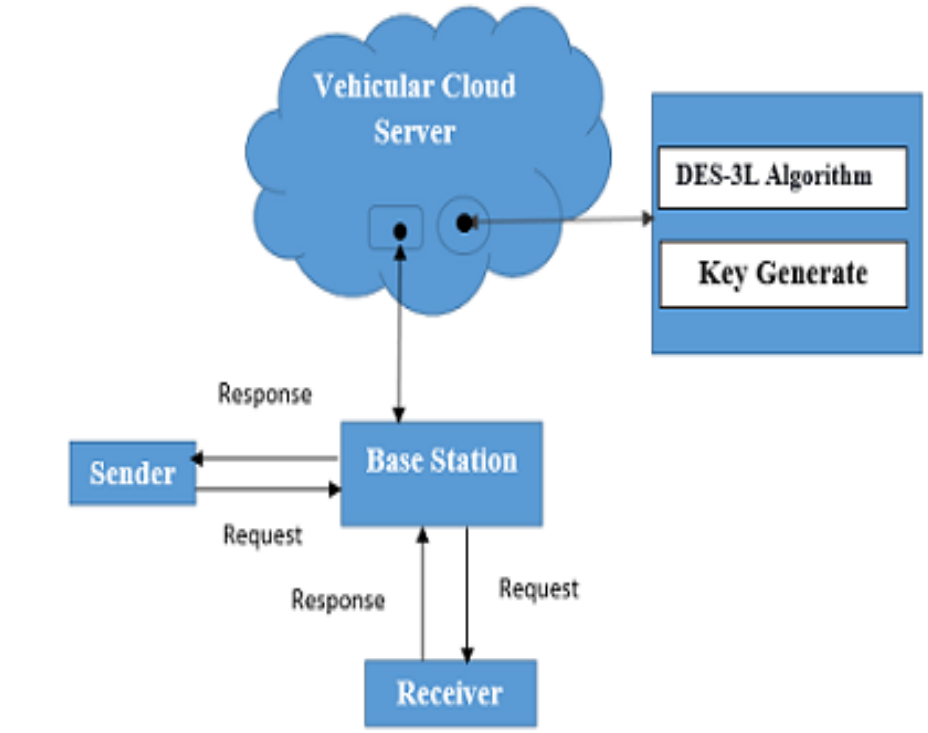
3.7 The Newly modified structure of DES-3L algorithm

Then DES (Level 3), when uploading any file from the user data privacy client, the file is encrypted. The byte insertion encryption method is accepted; you will get the key to creating a random data key. The key is changed to bite. Insert the file data key into the Bytes Insertion method. The encryption here is done with the Triple DES encryption algorithm, which is very secure and reliable. The Data Encryption Standard (DES) is the default bit encryption to prevent and transform a standard length character string into another cyber text bit string of the same length through a series of complex operations. An asymmetric encryption technology that encrypts the sender and recipient's use of that means a shared key to the encrypted data.

Algorithm 1: Algorithm For detecting Vehicles Behavior

```
Result: Detect the behavior of the vehicle Vi
BEHAVIOR 1 ILLEGAL;
BEHAVIOR 2 LEGAL;
Vi → Current Vehicle
LogDetails (Vim) →
Include all activity of Vehicle (Vi)
while TRUE do
    if Anonymous Activity (Ai) then
        ++Logdetails (Vim)
    else
        continue;
    end
    if Logdetails (Vim > T H RESOLD then
        BEHAVIOR (Vi) = 1
    else
    BEHAVIOR (Vi) = 2
    end
end
```

The three-level data encryption standard (DES) runs slower than DES in all three situations, while it is significantly safer in proper usage. Once descrambling is used, the technique is equivalent except that the latter is used to encrypt. DES is encrypted with information encoded and 64-bit bumps. Here, three properties of the user are taken as an example of Triple-DES



.

Figure.2 Proposed Architecture

Algorithm 2 :The newly modified structure of DES-3L algorithm

Step1:
Encryption.
Use three keys and three executions of the DES algorithm
(Encrypt-decrypt-encrypt)
Step2
Ct =EK3 [DK2 [Ek1 [P]]]
Ct = Cipher text Pt = Plain text
Step3:
EK [A] = encryption of A using key K
DK [B] = decryption of B using K
Encryption After, user1 obtains user 2 public key, he can send a message M.
Step4:
C = m e (mod n)
This can be done reasonably quickly, even for 500-bit numbers, using modular exponentiation. Siva then transmits c to Ram.
Step5:
Decryption
Ram can recover m from c by using her private key exponent d by computing
C= (me) d = m (mod n)
Given m, he can recover the original message M by reversing the padding scheme.
Model Algorithm // file store
Input get file Let ur []=get User file Let ar be an array, arr [3] =Get User attributes
For each value in arr
{
Convert arr[i] to 64 bit cipher key

Store it in enarr[3]
}
For each value in ur[]
{
ur []+enarr[]
Store data in cloud return DK
}

After using the three keys to encrypt three times and the DES algorithm, user-1 receives user- 2's public keys, and he's able to use M. Send a message. To do this, he first opens M strictly spoken, unfilled plain text and translates it into an integer M strictly speaking, fill in plain text, i.e. 0≤M <N, using an agreed-upon reversible protocol called the fill program. Then, he calculates the cipher text C and uses it. This can be done very quickly even with 500 digits using modular exponentiation. Taking into account the male, M can retrieve the original message through the reverse fill program.

4. RESULATS AND DISCUSSION

Finally, analyze the possible changes in 60 to 70 vehicles with a specific safety mechanism and illegal behavior. The primary purpose of our backward simulation is to examine how effectively the current user's behavior can be determined to determine whether the documents are original or unlawful. In this research, we use an improved distributed clustering algorithm, where the number of positive values is how many times our defense mechanism correctly identifies attacks then non-attacks. Table.1 defines the key factors used to estimate the performance of the refuge mechanism.

Table.1 performance of security mechanism

No of vehicles	Positive value
5	95
10	196
15	264
20	360
25	425
30	585
40	652
45	850
50	975

Whether to try to calculate based on the comparison between the proposed method and the finite method is to use an enhanced distributed algorithm for the lying level. The similarities in this study together lead to a more significant lying position, where these two technologies can define the advantages of our security mechanism. The map is here to use.

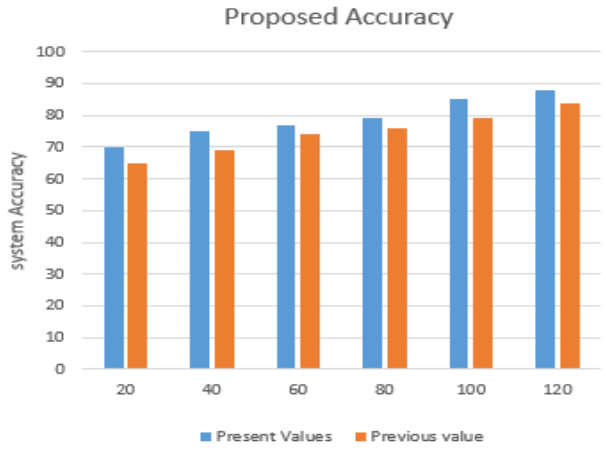


Figure 2. The proposed Accuracy for User behavior

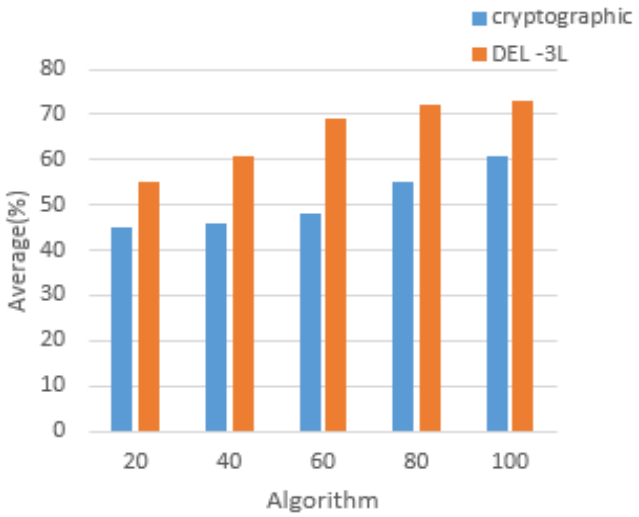


Figure 3. Proposed security level performance

5. CONCLUSION

Cloud Vehicle Forecasting While VANET vehicles are commonly used in networks using networks, they are more vulnerable to data attacks. Ensuring the security of users' private data through the system comes with a severe challenge. Among them, FC is a design, usages control devices, and user behavior prefixes toward delivering security for their records nearby. The modern system stayed first established by encryption algorithms. Instead, the present system is a dynamically generated immune file system; it is executed along with the IDCA algorithm. In unlicensed downloads, a legal document request, and then uses immunity and IDCA technology, if the fog calculation. Our security mechanism can provide the absence of a vehicle network and VCC security.

REFERENCE

[1]. L. Wang&J. Tao and M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific cloud computing: Early definition and experience," in 10th IEEE International Conference on High Performance Computing and Communications, HPCC 2008, pp. 825–830, chn, September 2008.
[2]. T. Ercan, "Effective use of cloud computing in educational institutions" Procedia—Social and Behavioral Sciences, vol. 2, no. 2, pp. 938–942, 2010.
[3]. K. Q. Yan& S. C. Wang & C. P. Chang, and J. S. Lin, "A hybrid load balancing policy underlying grid computing environment," Computer Standards & Interfaces, vol. 29, no. 2, pp. 161–173, 2007.
[4]. R. Armstrong and D. Hensgen, & T. Kidd, "The relative performance of various mapping algorithms is independent of sizable variances in run-time predictions," in Proceedings of the 7th Heterogeneous Computing Workshop (HCW '98), pp. 79–87, IEEE, 1998.
[5]. A. Vouk, Cloud computing—issues, research and implementations, in Proceedings of the 30th International Conference on Information Technology Interfaces (ITI '08), June 2008.
[6]. N. Santos& K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the Conference on Hot Topics in Cloud Computing, p. 3, San Diego, Calif, USA, 2009.
[7]. R. Buyya& R. Ranjan, and R. N. Calheiros, "Intercloud: utility-oriented federation of cloud computing environments for scaling of application services," in Algorithms and Architectures for Parallel Processing, pp. 13–31, Springer, Berlin, Germany, 2010.
[8]. F. Halsall& D. Links, Data Communications, Computer Networks and Open Systems, Addison-Wesley Publishers, 1995.
[9]. T. D. Braun& H. J. Siegel and N. Beck et al., "A comparison of eleven static heuristics for mapping a class of independent tasks onto heterogeneous distributed computing systems," Journal of Parallel and Distributed Computing, vol. 61, no. 6, pp. 810–837, 2001.

[10]. U. Brandes, "A faster algorithm for betweenness centrality", Journal of Mathematical Sociology, vol. 25, no. 2, pp. 163–177, 2001.
[11]. S. Lor&R. Landa and R. Ali, and M. Rio, "Handling transient link failures using alternate next hop counters," in Networking 2010: 9th International IFIP TC 6 Networking Conference, Chennai, India, May 11–15, 2010, Proceedings, vol. 6091 of Lecture Notes in Computer Science, p. 186, Springer, New York, NY, USA, 2010.
[12]. G. Iannaccone,& C.-N. Chuah&R. Mortier, S. Bhattacharyya, and C. Diot, "Analysis of link failures in an IP backbone," in Proceedings of the 2nd Internet Measurement Workshop (IMW '02), pp. 237–242, ACM, Marseille, France, November 2002.
[13]. G. Iannaccone and S. Bhattacharyya & C. Chuah, and C. Diot, "Characterization of failures in an IP backbone," in Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04), vol. 4, pp. 2307–2317, IEEE, Hong Kong, 2004.
[14]. X. Lin& R. Lu and C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," IEEE Communications Magazine, vol. 46, no. 4, pp. 88–95, 2008.View at:
[15]. R. Freund& M. Gherrity and S. Ambrosius et al., "Scheduling resources in multi-user, heterogeneous, computing environments with SmartNet," in Proceedings of the Seventh Heterogeneous Computing Workshop (HCW '98), pp. 184–199, Orlando, FL, USA, March 1998.
[16]. L. Garcés-Erice& E. W. Biersack and K. W. Ross, P. A. Felber, and G. Urvoy-Keller, "Hierarchical peer-to-peer systems," Parallel Processing Letters, vol. 13, no. 4, pp. 642–657, 2003.
[17]. A. Rowstron& P. Druschel, "Pastry: scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in Middleware 2001, pp. 329–350, Springer, 2001.
[18]. H. Gangwar& H. Date, and R. Ramaswamy, "Understanding determinants of cloud computing adoption using an integrated TAM-TOE model," Journal of Enterprise Information Management, vol. 28, no. 1, pp. 107–130, 2015.
[19]. M. A. Vouk, Clouds in higher education, in Innovative Technologies in Management and Science, vol. 10 of Topics in Intelligent Engineering and Informatics, pp. 17–28, Springer, Berlin, Germany, 2015.
[20] .B. Jolliffe& O. Poppe and D. Adaletey, and J. Braa, "Models for online computing in developing countries: issues and deliberations," Information Technology for Development, vol. 21, no. 1, pp. 151–161, 2015.