ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# Cost Reduction Scheme with Guaranteed Quality of Service in Heterogeneous Cloud Computing

Pappala Rajarao
M.Tech (CSE)
Department of CSE
Avanthi Institute of Engineering & Technology.

Suragali Chanti, M.Tech
Assistant Professor
Department of CSE
Avanthi Institute of Engineering & Technology.

Dr.A.Chandra Sekhar (Ph.D)
Professor & HoD
Department of CSE
Avanthi Institute of Engineering & Technology.

## ABSTRACT

*A fruitful and successful way to deal with give enlisting resources and organizations to customers on interest, appropriated registering has ended up being progressively popular. From cloud organization suppliers' perspective, advantage is a champion amongst the most basic thoughts, and it is generally controlled by the outline of a cloud organization stage under given business segment demand. In any case, a lone whole deal renting arrangement is regularly gotten to orchestrate a cloud stage, which can't guarantee the organization quality yet prompts honest to goodness resource waste. In this paper, a twofold resource renting arrangement is sketched out firstly in which transient renting and whole deal renting are joined going for the present issues. This twofold renting arrangement can sufficiently guarantee the way of organization of all sales and reduction the advantage misuse amazingly. Also, an organization structure is considered as a M/M/m+D lining model and the execution markers that impact the advantage of our twofold renting arrangement are inspected, e.g., the ordinary charge, the extent of sales that need break servers, and so forth. Thirdly, an advantage expansion issue is characterized for the twofold renting arrangement and the updated configuration of a cloud stage is gotten by handling the advantage enhancement issue. In this section, we first propose the Double-Quality- Guaranteed (DQG) resource renting scheme which combines longterm renting with short-term renting. The main computing capacity is provided by the long-term rented servers due to their low price. The short-term rented servers provide the extra capacity in peak period.*

## INTRODUCTION

### DEFINING CLOUD COMPUTING:

Distributed computing alludes to both the applications conveyed as administrations over the Internet and the equipment and frameworks programming in the server farms that give those administrations. These administrations have for quite some time been alluded to as Software as a Service (SaaS). A few terms, for example, PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) are utilized by merchants to portray their roducts, yet we stay away from these on the grounds that acknowledged definitions for despite everything them differ generally. There is no fresh line between "low-level "foundation and a gher-level "stage ". We trust both of these are more indistinguishable than various, and we do think of them as together. Likewise, some related term, for example, "grid computing," from the elite registering group, recommends conventions to offer stockpiling over long separations and shared calculation, however those conventions did not prompt to a product situation that developed past its own particular group. The server farm equipment and programming is the thing that we will call a cloud. At the point when a cloud is made accessible in a compensation as you-go way to the overall population, we call it an open cloud; the administration being sold is utility processing. We utilize the term private cloud to allude to inner server farms of a business or other association, not made accessible to the overall population, when they are sufficiently huge to profit by the benefits of distributed computing that we talk about here [1]. The distributed computing is the total of SaaS and utility figuring, yet does exclude medium estimated server farms, regardless of the possibility that these rely on upon virtualization for administration. Individuals can be clients or suppliers of SaaS, or clients or suppliers of utility registering. We concentrate on SaaS suppliers (cloud clients) and cloud suppliers, which have gotten less consideration than SaaS clients. Figure 1 makes supplier client connections clear. There are some case in which a similar performer assumes different parts. For example, a cloud supplier may likewise have its own client confronting.

## BENEFITS ON CLOUD FRAMEWORK:

Distributed computing offers powerfully versatile assets provisioned as an administration over the Internet. The thirdparty, on-request, self-benefit, pay-per-utilize, and flawlessly versatile figuring assets and administrations offered by the uproarious worldview guarantee to lessen capital and additionally operational consumptions for equipment and programming. Mists can be classified considering the physical area from the perspective of the client [2]. An open cloud is offered by outsider administration suppliers and includes assets outside the client's premises. In the event that the cloud framework is introduced on the client's preface—as a rule in the claim server farm—this setup is called private cloud. A half and half approach is indicated as mixture cloud. This paper will focus on open mists, in light of the fact that these administrations interest for the most noteworthy security necessities additionally—as this paper will begin contending—incorporates high potential for security prospects. In broad daylight mists, the greater part of the three basic cloud benefit layers (IaaS, Paas, SaaS) share the shared trait that the end-clients' computerized resources are taken from an intraorganizational to an interorganizational setting. This makes various issues, among which security perspectives are viewed as the most basic elements when considering distributed computing appropriation [3]. Enactment and consistence systems raise promote challenges on the outsourcing of information, applications, and procedures. The high protection measures in the European Union, e.g., and their legitimate varieties between the mainland's nations offer ascent to particular specialized and hierarchical difficulties [4]. One thought on lessening the hazard for information and applications in an open cloud is the synchronous utilization of various mists. A few methodologies utilizing this worldview have been proposed as of late. They contrast in parceling and circulation designs, advances, cryptographic strategies, and focused on situations and additionally security levels. This paper is an augmentation of [5] and contains an overview on these diverse security by multicloud selection3.approaches. It gives four unmistakable models in type of disconnected multicloud structures. These created multicloud designs permit to sort the accessible plans and to investigate them as indicated by their security benefits. An appraisal of the diverse strategies with respect to legitimate angles and consistence suggestions is given specifically. Whatever is left of this paper is sorted out as takes after: Section 2 spurs the requirement for powerful cloud security countermeasures by quickly evaluating the present condition of play. The perceptions assist prompt to the way that the greater part of the innovative work is as of now committed to devoted security plans, which don't consider the particular properties of the cloud itself. Just as of late a few recommendations on making utilization of numerous particular mists in the meantime to acknowledge security objectives began to show up. To give a formal ground to arrange and examine these proposition, we propose an arrangement of four unmistakable multicloud structures. These multi cloud models are presented in Section 3 and each of them is further examined in Sections 4, 5, 6, and 7, including contextual investigations. Segment 8 gives a thought of legitimate and consistence viewpoints. At long last, in Section 9, an appraisal and correlation of the introduced methodologies is given. Distributed computing makes a substantial number of security issues and difficulties. A rundown of security dangers to distributed computing is introduced in [6]. These issues go from the required trust in the cloud supplier and assaults on cloud interfaces to abusing the cloud administrations for assaults on different frameworks. The principle issue that the distributed computing worldview verifiably contains is that of secure outsourcing of delicate and in addition business-basic information and procedures. At the point when considering utilizing a cloud administration, the client must know about the way that all information given to the cloud supplier leave the claim control and assurance circle. Much more, if conveying information handling applications to the cloud (through IaaS or PaaS), a cloud supplier increases full control on these procedures. Thus, a solid trust relationship between the cloud supplier and the cloud client is viewed as a general essential in distributed computing. In [7], a diagram of security blemishes and assaults on cloud frameworks is given. A few cases and later advances are quickly talked about in the accompanying. Risten part et al. [8], [9] exhibited some assault methods for the virtualization of the Amazon EC2 IaaS benefit. In their approach, the aggressor distributes new virtual machines until one keeps running on an indistinguishable physical machine from the casualty's machine. In a defect in the administration interface of Amazon's EC2 was found. The SOAP-based interface utilizes XML Signature as characterized as a part of WS-Security for trustworthiness assurance and genuineness check. Gruschka and Iacono [10] found that the EC2 usage for mark check is helpless against the Signature Wrapping Attack [11]. A noteworthy episode in a SaaS cloud happened in 2009 with Google Docs [12]. Google Docs permits clients to alter archives (e.g., content, spreadsheet, presentation) on the web and impart these records to different clients. In any case, this framework had the accompanying defect: Once a report was imparted to anybody, it was open for everybody the record proprietor has ever imparted archives to some time recently. For this specialized glitch, not in any case any criminal aim was required to get unapproved access to private information. Late assaults have exhibited that cloud frameworks of significant cloud suppliers may contain serious security blemishes in various sorts of mists (see [13], [14]). Making utilization of numerous mists has been proposed by Bernstein and Celesti [15].

## ALL SORTS OF MISTS:

Real IT organizations have burned through billions of dollars since the 1990s to shape distributed computing. Like, Sun's notable trademark "the system is the PC" was made in 1980s. Salesforce.com is the site which has been giving on-request Software as a Service (SaaS) for clients since 1999 to present time. IBM and Microsoft are the initial two organizations that began to convey Web benefits in the mid 2000s. Microsoft's Azure administration gives an 5 working framework and an arrangement of designer instruments and administrations. Google's prominent Google Docs programming gives Web-based word processing, spreadsheets and all the Microsoft office applications. Google App Engine permits framework designers to run their Python/Java applications on Google's foundation. Sun gives $1 per CPU hour. Amazon is notable for giving Web administrations, for example, EC2 and S3. Hurray! declared that it would utilize the Apache Hadoop structure to permit clients to work with a great many hubs and petabytes (1 million gigabytes) of information. These illustrations exhibit that distributed computing suppliers are putting forth benefits on each level, from various equipment (e.g., Amazon and Sun), to the distinctive working frameworks (e.g., Google and Microsoft), to programming and diverse administrations (e.g., Google, Microsoft, and Yahoo!). At present period Cloudcomputing suppliers focus on an assortment of end clients, from designers of the product to the overall population. For extra data in regards to distributed computing models, the University of California (UC) Berkeley's report gives a decent correlation of these models by Amazon, Microsoft, and Google. As distributed computing suppliers costs are low and IT headways evacuate innovation hindrances, for example, virtualization, reproduction, arrange transmission capacity — distributed computing has moved into the standard of innovation. Gartner expressed, "Associations are changing from organization proprietor equipment and programming to per-utilize benefit based models." For instance, the U.S. government site (http://www.usa .gov/) will soon start utilizing distributed computing. The New York Times utilized Amazon's EC2 and S3 benefits and utilized Hadoop application to give open access to people in general area articles from 1851 to 1922. The Times stacked 4 TB of crude TIFF pictures on web and their subordinate 11 million PDFs into Amazon's S3 in twenty-four hours at less cost. This venture is fundamentally the same as computerized library ventures keep running by scholastic libraries. Couple of years prior OCLC reported its development of 6 library administration administrations to the Web It is obvious that OCLC will convey a Web-based incorporated library framework (ILS) on web for upgrading the innovation to give another method for running an ILS. Dura Space, a joint association by Fedora Commons and D Space Foundation, reported that they would exploit distributed storage and distributed computing.

## EXISTING SYSTEM

In general, a service provider rents a certain number of servers from the infrastructure providers and builds different multi-server systems for different application domains. Each multiserver system is to execute a special type of service requests and applications. Hence, the renting cost is proportional to the number of servers in a multiserver system. The power consumption of a multiserver system is linearly proportional to the number of servers and the server utilization, and to the square of execution speed. The revenue of a service provider is related to the amount of service and the quality of service. To summarize, the profit of a service provider is mainly determined by the configuration of its service platform.

To configure a cloud service platform, a service provider usually adopts a single renting scheme. That’s to say, the servers in the service system are all long-term rented. Because of the limited number of servers, some of the incoming service requests cannot be processed immediately. So they are first inserted into a queue until they can handle by any available server.

### Disadvantages of Existing System:

- The waiting around time of the service requests is too long.
- Sharp increase of the renting cost or the electricity cost. Such increased cost may counterweight the gain from penalty lowering. In conclusion, the only renting scheme is a bad scheme for service providers.

## PROPOSED SYSTEM:

In this section, we first propose the Double-Quality-Guaranteed (DQG) resource renting scheme which combines longterm renting with short-term renting. The main computing capacity is provided by the long-term rented servers due to their low price. The short-term rented servers provide the extra capacity in peak period

### Advantages:

- In proposed system we are using the Double-Quality-Guaranteed (DQG) renting scheme can achieve more profit than the compared Single-Quality-Unguaranteed (SQU) renting scheme in the premise of guaranteeing the service quality completely.
- Since the requests with waiting time D are all assigned to temporary servers, it is apparent

that all service requests can guarantee their deadline and are charged based on the workload according to the SLA. Hence, the revenue of the service provider increases.

- Increase in the quality of service requests and maximize the profit of service providers.
- This scheme combines short-term renting with long-term renting, which can reduce the resource waste greatly and adapt to the dynamical demand of computing capacity.

## SYSTEM DESIGN

## SYSTEM ARCHITECTURE

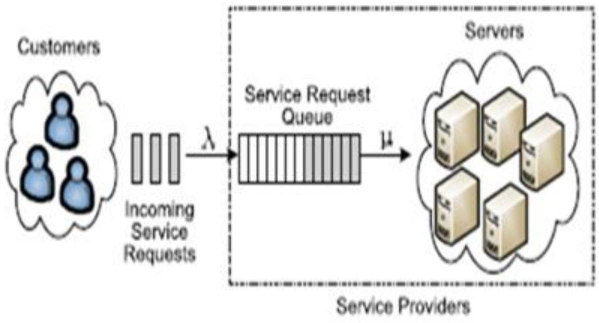


Fig 5.1: System Architecture

## IMPLEMENTATION MODULES:

- Cloud Computing.
- Queuing Model.
- Business Service Module.
- Cloud Customer Module
- Infrastructure Service Provider Module

### Cloud Computing:

- Cloud computing describes a type of outsourcing of computer services, similar to the way in which the supply of electricity is outsourced. Users can simply use it.
- They do not need to worry where the electricity is from, how it is made, or transported. Every month, they pay for what they consumed.
- The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally.
- Cloud computing is usually Internet-based computing. The cloud is a metaphor for the Internet based on how the internet is described in computer network diagrams; which means it is an abstraction hiding the complex infrastructure of the internet.
- It is a style of computing in which IT-related capabilities are provided “as a service”, allowing users to access technology-enabled services from the Internet ("in the cloud")without knowledge of, or control over the technologies behind these servers.

### Queuing Model:

- We consider the cloud service platform as a multi server system with a service request queue. The clouds provide resources for jobs in the form of virtual machine (VM).
- In addition, the users submit their jobs to the cloud in which a job queuing system such as SGE, PBS, or Condor is used. All jobs are scheduled by the job scheduler and assigned to different VMs in a centralized way.
- Hence, we can consider it as a service request queue. For example, Condor is a specialized workload management system for computer intensive jobs and it provides a job queuing mechanism, scheduling policy, priority scheme, resource monitoring, and resource management.
- Users submit their jobs to Condor, and Condor places them into a queue, chooses when and where to run them based upon a policy. An M/M/m+Dqueueing model is build for our multiserver system with varying system size.
- And then, an optimal configuration problem of profit maximization is formulated in which many factors are taken into considerations,

such as the market demand, the workload of requests, the server-level agreement, the rental cost of servers, the cost of energy consumption, and so forth.

- The optimal solutions are solved for two different situations, which are the ideal optimal solutions and the actual optimal solutions.

### Business Service Module:

- Service providers pay infrastructure providers for renting their physical resources, and charge customers for processing their service requests, which generates cost and revenue, respectively.
- The profit is generated from the gap between the revenue and the cost.In this module the service providers considered as cloud brokers because they can play an important role in between cloud customers and infrastructure providers ,and he can establish an indirect connection between cloud customer and infrastructure providers.

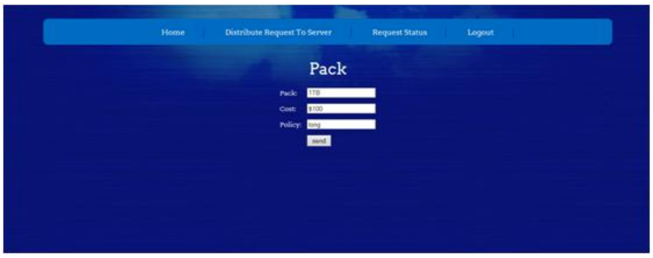
### Cloud Customer Module:

- A customer submits a service request to a service provider which delivers services on demand.
- The customer receives the desired result from the service provider with certain service-level agreement, and pays for the service based on the amount of the service and the service quality.

### Infrastructure Service Provider Module:

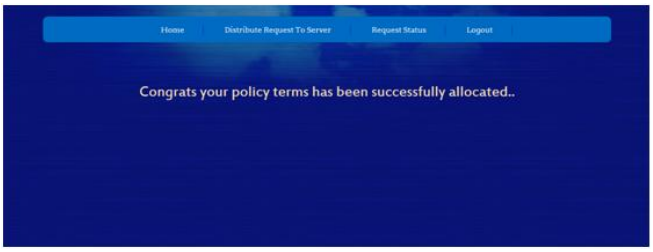
- In the three-tier structure, an infrastructure provider the basic hardware and software facilities.
- A service provider rents resources from infrastructure providers and prepares, a set of services in the form of virtual machine (VM).
- Infrastructure providers provide two kinds of resource renting schemes, e.g., long-term renting and short-term renting.
- In general, the rental price of long-term renting is much cheaper than that of short-term renting.

### SCREEN SHOTS

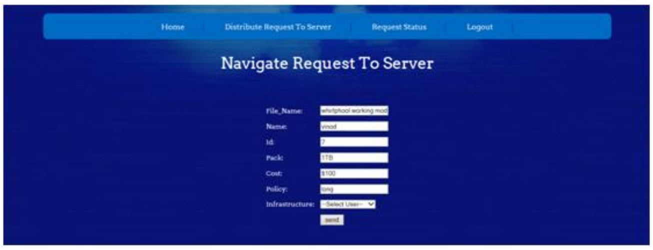


Pack

Pack: 1TB
Cost: $100
Policy: long
send

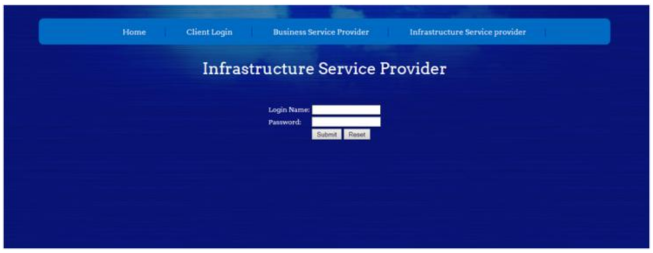


Congrats your policy terms has been successfully allocated..



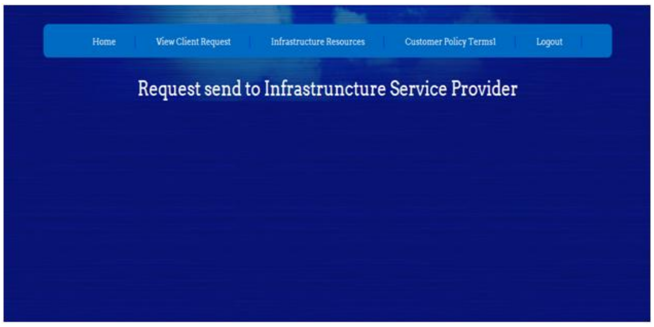
Navigate Request To Server

File_Name: whirlphool working mod
Name: vinod
Id: 7
Pack: 1TB
Cost: $100
Policy: long
Infrastructure: --Select User--
send



Infrastructure Service Provider

Login Name:
Password:
Submit Reset



Request send to Infrastrunncture Service Provider

## CONCLUSION

This paper has proposed a novel double quality guaranteed renting scheme for service providers. This scheme combines short term renting with long term renting, which can reduce the resource waste greatly and adapt to the dynamical demand of computing capacity. An M/M/m+D queuing model is build for our multiserver system with varying system size. And then, an optimal configuration problem of profit maximization is formulated in which many factors are taken , such as the market demand the workload of requests, the server level agreement the rental cost of servers, the cost of energy consumption and so forth. The optimal solutions are solved for two different situations, which are the ideal optimal solutions and the actual optimal solutions. In addition a series of calculations are conducted to compare the profit obtained by the DQG renting scheme with the single quality unguaranteed renting scheme.

## REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc. IEEE/ACM Int’l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[6] C. Gentry, “A Fully Homomorphic Encryption Scheme,” PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-Based Cloud Computing,” Proc. Third Int’l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, “Trustcloud: A Framework for Accountability and Trust in Cloud Computing,” HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10] D.F. Ferraiolo and D.R. Kuhn, “Role-Based Access Controls,” Proc. 15th Nat’l Computer Security Conf., 1992.

[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, “Adding Attributes to Role-Based Access Control,” IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.

[12] M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,” Proc. Sixth Int’l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc.

ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.

[14] G. Wang, Q. Liu, and J. Wu, “Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,” Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[15] F. Zhao, T. Nishide, and K. Sakurai, “Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems,” Proc. Seventh Int’l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

[16] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,” Proc. IEEE 10th Int’l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[17] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf, 2013.

[18] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud, 2013.

[19] S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.

[20] R.L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” Proc. Seventh Int’l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.

[21] X. Boyen, “Mesh Signatures,” Proc. 26th Ann. Int’l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.

[22] D. Chaum and E.V. Heyst, “Group Signatures,” Proc. Ann. Int’l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.

[23] H.K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance,” IACR Cryptology ePrint Archive, 2008.

[24] H.K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute-Based Signatures,” Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[25] A. Beimel, “Secure Schemes for Secret Sharing and Key Distribution,” PhD thesis, Technion, Haifa, 1996.

[26] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” Proc. Ann. Int’l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[28] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[29] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.

[30] M. Chase, “Multi-Authority Attribute Based Encryption,” Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[31] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority,” Proc.

Progress in Cryptology Conf. (INDOCRYPT), pp. 426-436, 2008.

[32] M. Chase and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

[33] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABE Ciphertexts,” Proc. USENIX Security Symp., 2011.