ISSN 22773061

Singleto Multi Clouds for Security in Cloud Computing by using Secret Key Sharing

K Chandra Mouli* U Sesadri
M Tech (CSE) HOD of CSE
chandu.kathi@gmail.com*

Abstract:

Now a day Cloud Computing is rapidly using computing technology. For low cost and high-end benefits this cloud computing is utilized. The major issue in this cloud computing is Ensuring the security, because the often store sensitive data with third party cloudproviders but these providers may beuntrusted.Working with single cloud is prevented, because in customer's perception the failure in service availability and thepossibility of viciousgang in single cloud. To overcome these types of failures, a recent and popular technology is emerged called cloud of clouds or multi clouds or inters clouds. In this paper we illustrated the recent research towards multi clouds from single cloud and addressed possible solutions in security concern.Here we used the SSS (Secret Key Sharing) technique to share the key between servers. From this we can found that there is less attention in the field of multi cloud security compare with single cloud providers. The main intention of this work is to reduce the security risks related to cloud users and to encouragetheuse of cloud- of -clouds due to its ability.

Keywords: Cloud computing, single cloud, multi-clouds, data integrity, data intrusion, service availability.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 10, No 4

editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 22773061

1. Introduction

Cloud Computing

The cloud computing satisfied critical needs of secure storage, manage, share and analyze huge amount of complex data to predict the patterns and trends of information in order to improve the quality of healthcare systems, better nation safeguard and to explore alternative energy. Because the applications nature is critical, so the secure cloud is important. The main cloud security threat is that the owner dints have control on his/her own data and where the data is placed. This is done due to the utilization of resource allocation and scheduling of cloud benefits. Therefore, we need to escort the data in the hub of unreliable processes

Fig 1: Cloud Computing

Cloud computing is a distributed IT service paradigm, resources acrossthe Internet. It provides access to heterogeneous IT resources, whichcan either be physical or virtual, as services over the Internet [1].Examples of provided resources include storage resources suchas those provided by Amazon S3 [2], computational resourcessuch as Amazon EC2 [3] and applications such as the Google AppEngine [4].

Cloud Architecture

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue (Cloud Wiki). The following figure illustrates the general cloud architecture.

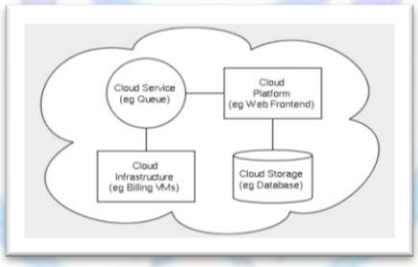

Fig 2: Cloud Architecture

Through the virtualization technology the Cloud computing is qualified which is available for mainframe systems past decade. In its quintessence,(Erica, 09) a host computer runs an application known as a hypervisor; this creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications.

At a hardware level, a number of physical devices, including processors, hard drives and network devices, are located in datacenters, independent from geographical location, which are responsible for storage and processing needs. Above this, the combination of software layers, the virtualization layer and the management layer, allow for the effective management of servers.

1.1. Cloud Data Storage Architecture

The cloud storage network architecture is illustrated in Figure 3. It consists of three types of entities followed:

• User: the user either individual or an organization, whose datato be stored in cloud and rely on the cloud for data computation.

• Cloud Service Provider (CSP): a CSP, who is responsible to provide resources and expertise to build and manage distributed cloud storage servers, owns and operates live Cloud Computing systems.

• Third Party Auditor (TPA): an optional TPA,is an expert capable to assess and expose risk of cloud storage services on behalf of the users upon request.

The cloud storage servers will run simultaneously, distributed and co-operated manner, where the user can store the information through Cloud Server Provider.

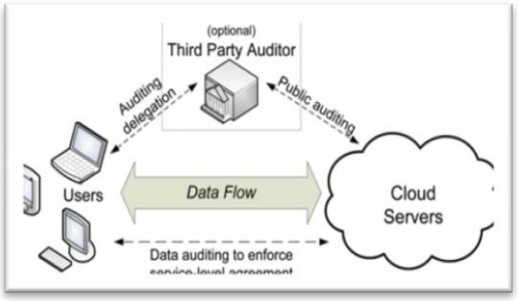

Fig 3: Cloud Data Storage

2. Preliminaries

NIST [1] describes cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly procured and freed with small administration effort or communication with service provider”.

2.1. Cloud Computing Components

There are five characteristics in the cloud computing model with four deployment models, three delivery models, two payment plans and one management policy [1]. The following are the five key characteristics: self-provisioning through a portal, scalability & elasticity, utility model, ubiquitous network access and transport interclouds access. These key characteristics are placed in the first layer in the cloud environment architecture (see Figure 4).

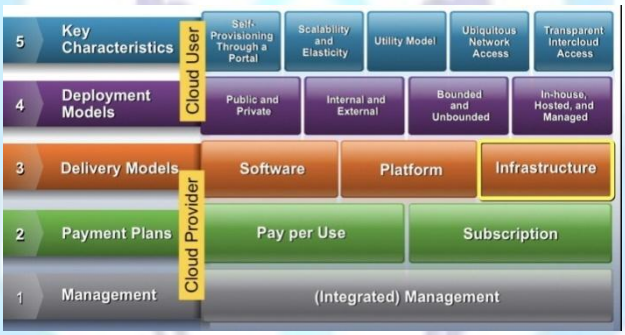

Fig 4: Key Components of Cloud Computing

The self-provisioning through a portal provides quality of service to the cloud user. The money will plays major role in this cloud as well.

The four deployment modelsexplain the governance of services and resources, public or private and internal or external, and with hybrid clouds.A great example is collaboration provided by Cisco Telepresence and Cisco WebEx solutions, actually (Ranjit, 2010).When we came to cloud delivery models there are 3 swim lanes with software, platform and infrastructure. These are famous with names SaaS, PaaS, and IaaS.

From downwards second one is Payment plans; these will work as Pay-per-use and subscriptions.However, Ranjit at el, according to the InformationWeek in the report ‘The Pubic Cloud: Infrastructure as a Service”, generally $499 per month for 1xCore CPU, 4 GBs of memory and 32 GBs seems to be a commonly found tariff.The bottom one is integrated management the way the cloud is managed with single administration work.

2.2. Cloud Service Providers

In the mercantile world, the services are grouped i.,edifferentcomputing needs. The cloud service providers have to take care of the customer needs, for example, maintaining software or purchasing expensive hardware. For instance, the service EC2, created by Amazon, provides customers with scalable servers, Mohammad et al. The academic institutions to access large scale distributed systems NSF joined with Google and IBM under the CLuE program. There are many features of cloud computing. The very first one permitted to users to access online data, for example Amazon S3, Microsoft SkyDrive, andNirvanixCLoudNAS. Amazon EC2 is the computation service for users is the second one. The third one is the online collaboration tools like Google Apps.

For customer’s sensitive data protection, the cloud service providers only responsible. A cloud provider offers many services that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, and data storage, and data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities, Mohammad et al.

Another two benefits are available for public cloud with low cost called Reliability and availability.But in public cloud the data integrity and confidentiality are the common problems.

2.3. Security issues of Cloud Computing

Even though there are many uses from cloud computing to their users, there are few major security issues. The data loss happens through the well-known online data sharing and network usage.According to a recent IDC survey[16], the top challenge for 74% of CIOs in relation tocloud computing is security. Protecting private andimportant information such as credit card details orpatients' medical records from attackers or maliciousinsiders is of critical importance [34]. Movingdatabases to a large data centre involves many securitychallenges such as virtualization vulnerability,accessibility vulnerability, privacy and control issuesrelated to data accessed from a third party, integrity,confidentiality, and data loss or theft. The following are the main security challenges data security when stored, application security, security related to application usages and third party security challenges proposed by SubashiniandKavitha.

We will address three security factors thatparticularly affect single clouds, namely data integrity,multi tenancy, data intrusion, system monitoring and logs,authenticationand service availability.

- Data Integrity: The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinetetal. given examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers.
- Data Intrusion: TheAmazon cloud service is a hacked password or data intrusion. If any third person got Amazon account password, then he is eligible to access every account information, resources and services as well. He can modify them or even he can destroy everything.
- Service Availability: Amazon [6] mentioned in its license agreement that it is possible that service unavailability some times. In (Shivakumar, 2013) the user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (MediaMax) as a cloud storage provider [12].
- Cloud standards: standards are needed across different standard developing organizations to achieve interoperability among clouds and to increase their stability and security.
- System monitoring and logs: as more business critical applications are migrated to the cloud, customers may request thatcloud providers provide more monitoring and log data for the customers' personnel.
- Authentication and trust of acquired information: as the critical data is located in the cloud provider infrastructure, the datamay be altered without the owner's consent.
- Multi-tenancy issue: this issue poses a challenge to protect user data against unauthorized access from other usersrunningprocesses on the same physical servers.

3. Multi Clouds

The cloud computing doesn't end with single cloud; because the terms inter clouds or cloud of clouds is similar to "multi-clouds" are introduced by Vukolic.

Based on his illustration the sky has different cloud structures and colors which maintains different implementations and administrative domains in our cloud computing. Recent research has focused on the multi-cloud environment [3],[8],[10],[11] which avoids dependency on single cloud and controls several clouds.The multi cloud is divided into two layers Cachin et al. inner cloud in bottom and inter cloud in top layer.

3.1.1. DepSky System: Multi-Clouds Model

This section will explain the recent work that has been done in the area of multi-clouds. Bessani et al. [8] present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes. The following figure illustrates the architecture of DepSky.

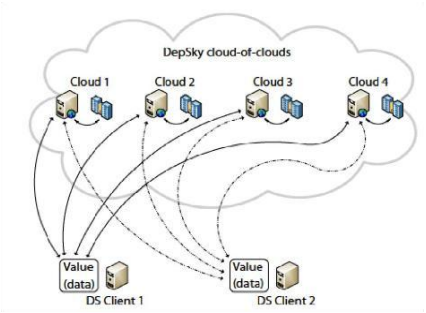

Figure 5:DepSky Architecture

Cloud storage providers in the DepSky system model,The Byzantine protocols involve a set ofstorage clouds (n) where n = 3 f +1, and f is maximum number of clouds which could be faulty. In addition, any subset of (n – f) storage cloud creates byzantine quorum protocols [8].

3.1.2. Analysis of Multi-Cloud

As perCachinetsperception “Services of single clouds are still subject to outage”. After that Bowers et al. showed that the company’s management had fear in security threats and loss of control of data and systems is more than 80%”. The main purpose to move from single to multi cloud is by distributing reliability, trust, and security among multiple cloud providers. In addition, reliable distributed storage [15] which utilizes a subset of BFT techniques was suggested by Vukolic to be used in multi-clouds.

The number of protocols is built for clouds through the recent studies. Actually RAID is used in disks for data storage, based on this RACS (Redundant Array of Cloud Storage) is developed for multiple cloud storage. Abu-Libdeh et al. [3] assume that to avoid “vender lock-in”, distributing a user’s data among multiple clouds is a helpful solution. Mohammad et al. This replication also decreases the cost of switching providers and offers better fault tolerance. Therefore, the storage load will be spread among several providers as a result of the RACS proxy.

Another example to control multiple clouds is HAIL (High Availability and Integrity Layer). HAIL is a distributed cryptographic system that allows a set of servers to secure the client’s stored data is retrievable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an intercloud [10].

As mentioned before, Bessani et al. [8] present a virtual storage cloud system called DepSky consisting of a combination of different clouds to build a cloud-of- clouds. Bessani et al. [8] discuss some limitations of the HAIL protocol and RACS system when compared with DepSky. Jayashri et al. HAIL does not guarantee data confidentiality, it needs code execution in their servers, and it does not deal with multiple versions of data.Finally, the DepSky system presents an experimental evaluation with several clouds, which is different from other previous work on multi-clouds [8].

3.2. Current Solutions of Security Risks

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud [12]. Mohammad et al. using a hash function is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data [12]. If the amount of data is large, then a hash tree is the solution. Many storage system prototypes have implemented hash tree functions, such as SiRiUS [20] and TDB.

Mykletun et al. and Papamanthou et al. claim that this is an active area in research on cryptographic methods for stored data authentication. Proofs of Retrievability (PORs) and Proofs of Data Possession (PDP) are protocols introduced by Juels and Kaliski and Ateniese et al. [7] to result high probability for the retrieval of the user’s data.

Computing resources are required in this approach and not only storage in the cloud, such a service provided in Amazon EC2, whereas if only storage service is available, Cachin et al. [12] suggest working with Byzantine Quorum Systems by using Byzantine Disk Paxos[2] and using at least four different clouds in order to ensure users’ atomicity operations and to avoid the risk of one cloud failure.

In October 2009, the customers data was lost this caused many problems for many users likecontacts, photos, etc. of many users of the Sidekickservice in Microsoft were lost for several days.

3.3. Limitation of Current Solutions

The problem of the malicious insider in the cloudinfrastructure which is the base of cloud computing isconsidered by Rocha and Correia.Infrastructure as a Service (IaaS) cloud providers will provide the services like virtual machines where the users can run their software’s. The old solution for this problem is to encrypt the user’s data, but the manipulations on encrypted data on virtual machines are not at all possible. If the malicious insider got the administrator details he can access the user’s data through remote servers.VanDijk and Juels et al. present somenegative aspects of data encryption in cloudcomputing. In addition, they assume that if the data isprocessed from different clients, data encryptioncannot ensure privacy in the cloud.

Although cloud providers are aware of themalicious insider danger, they assume that they havecritical solutions to alleviate the problem [22]. RochaandCorreia et al. determine possible attackers for IaaScloud providers. Grosse et al. propose another solution isto monitor all access to the servers in a cloud where theuser’s data is stored.

Rocha and Correia classified four typesofattacks that can affect the confidentiality of the user’sdata in the cloud. These four types of attacks couldoccur when the malignant insider can determine textpasswords in the memory of a VM, cryptographic keysin the memory of VM files, and other confidential data.

In addition, they argue that the recent researchmechanisms are not good enough to consider the issueof data confidentiality and to protect data from theseattacks. Some of the solutions are mechanismsand are used as part of cloud computing solutions,while different types of solutions focus on solving thewhole data confidentiality issue intrinsic to cloudcomputing [8]. Rocha and Correiasuggesttrusted computing and distributing trust among severalcloud providers as a novel solution to solving securityproblems and challenges in cloud computing. It is clear from the research has been conducted into single clouds thaninto multi-clouds. Multi–clouds can address thesecurity issues that relate to data integrity, data intrusion, and service availability in multi-clouds. Inaddition, most of the research has focused on providing

secure “cloud storage” such as in DepSky. Therefore,providing a cloud database system, instead of normal cloud storage, is a significant goal in order to runqueries and deal with databases; in other words, toprofit from a database-as-a-service facility in a cloud computing-environment.

4. Secret Sharing Scheme

In this section we’ll see how the secret sharing schemes will work to secure multi clouds in cloud computing and theapplications to Threshold Cryptography. The main theme of this scheme is split the secret key into small pieces and then shared this secret between many servers. Even though few servers got compromised still the secret is safe, this can be done when server simulation is done on key holder.

Definitions

The basic secret sharing scheme consist the two algorithms namely Sharing (Share) and Recovery (Rec).It works in the same way as we think: the Share algorithm divides entire message M into small pieces. To maintain secrete of message M, the share is probabilistic, to show this we will use arrow (→). The original message we will get back through the deterministic algorithm Rec from some orall of the shares.

Sharing: Share(M) → (S1,S2, . . . ,Sn, pub). The divided S secrets are distributedsecurely among all servers 1 to n, and pub is a public share.

Recovery: Rec(S'1, S'2, . . . ,S'n,pub) = M’. Yevgeniyetal.The correctness property of thealgorithm says that for any message M, Rec(Share(M)) = M.

To quantify the security of the scheme we introduced four threshold parameters.

tp is the privacy threshold:it illustrates the maximum number of servers cannot finds the secret even if they are compromised.

tfis the fault-tolerance threshold:minimum number of servers from whom we want to recover the secret even some servers failed.

tris the robustness threshold: if some servers are compromised it shows the recover from minimum number of correct shares.

tsis the soundness threshold: This determines the minimum number of correct shares such thatyou don’t ever recover the wrong secret.

The following are the things we observed: tp+ 1 ≤tf≤tr≤n and ts ≤ tr. Yevgeniyetal.In any threshold encryption scheme, a message is encrypted such that tfor more serverswilldecrypt the message, but tpor fewer will not. We say a scheme requires t-out-of-n users to decryptwhen t =tfandtp= t - 1.

n-out-of-n Schemes

We will see how 2-out-of-2 sharing, i.e. a secret is shared between two servers, and bothcorrect shares must be present to recover the secret [25]. Suppose M ∈ G where G is a finite abeliangroup under addition. Define thesharing algorithm to be the following:

Then the recovery algorithm is Rec(SShare (M): S1, S2) = S.

An immediate generalization of the above is the n-out-of-n scheme. Select n-1 shares randomly:Share (M) : S1, S2, . . . , Sn-1←GSn= M - (S1+ SR2+ · · · + S)As before, the recovery algorithm is thenRec (S1, . . . , S'n) = S'1+ · · · + S'n. Based on this we observed that the way how secret key sharing techniques will work.

5. Analysis Discussions

Secret key sharing scheme can be used in cloud computing to secure secret values and data. Several independent systems are connected to do particular task and forms cloud computing, the main theme of this task is can be subdivided into thresholds for individual computing systems. These computing system thenstore these thresholds. If any third person got accessed the information from few servers, he will get only some pieces coded or encrypted data. It is not that much easy to enter to cloud server to an unauthorized person because it consist of many systems so, everysystem may have different functionalities like operating system, firewall system, software etc.

We will check with the following example: t-out-of-n schemes that each share of the secret must be at least as large as the secret itself. On the other hand, a system is computationallysecure if it is secure against a computationally bounded adversary; such schemesmay rely on the hardness of mathematical problems.

The perfect privacy isaspecial type of secret key sharing algorithm. If each S doesn’t provide any information without knowing secret key of M message then Share is the perfectly secret.Making perfect privacy is more desirable and if it is perfect there will be littledistinction between static and adaptable adversaries.

Conclusion

The security of cloud computing is a major concern these days but also the usage of cloud computing is increased rapidly. The cloud customer’s dint wants to lose their sensitive data by malicious insidersinthe cloud. Recently detected another

major problem is the loss of service availability due to this large number of customers is suffered.For cloud users the data intrusion causes many problems. The main theme of this paper is to detect security issues from single cloud to multi clouds to build solutions for future. We have seen that multi cloud storage has less security problems compare with single cloud by lavish research. To reduce the security risks of cloud computing we supported to migrate from single to multi clouds to the cloud users.

References

[1]. (NIST), http://www.nist.gov/itl/cloud/.
[2]. I. Abraham, G. Chockler, I. Keidar and D. Malkhi,"Byzantine disk paxos: optimal resilience withByzantine shared memory", DistributedComputing, 18(5), 2006, pp. 387-408.
[3]. H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storagediversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.
[4]. D. Agrawal, A. El Abbadi, F. Emekci and A.Metwally, "Database Management as a Service:Challenges and Opportunities",ICDE'09:Proc.25thIntl. Conf. on Data Engineering,2009, pp. 1709-1716.
[5]. M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-Service",44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.
[6]. Amazon, Amazon Web Services. Web serviceslicensing agreement, October3,2006.
[7]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song, "Provable datapossession at untrusted stores", Proc. 14th ACMConf. on Computer and communications security,2007, pp. 598-609.
[8]. A. Bessani, M. Correia, B. Quaresma, F. André andP. Sousa, "DepSky: dependable and secure storagein a cloud-of-clouds", EuroSys'11:Proc. 6thConf. OnComputer systems, 2011, pp. 31-46.
[9]. K. Birman, G. Chockler and R. vanRenesse,"Toward a cloud computing researchagenda", SIGACT News, 40, 2009, pp. 68-80.
[10]. K.D. Bowers, A. Juels and A. Oprea, "HAIL: Ahigh-availability and integrity layer for cloudstorage", CCS'09: Proc. 16th ACM Conf. onComputer and communications security, 2009, pp.187-198.
[11]. C. Cachin, R. Haas and M. Vukolic, "Dependablestorage in the Intercloud", Research Report RZ,3783, 2010.
[12]. C. Cachin, I. Keidar and A. Shraer, "Trusting thecloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[13]. C. Cachin and S. Tessaro, "Optimal resilience forerasure-coded Byzantine distributed storage",DISC:Proc. 19thIntl.Conf. onDistributedComputing, 2005, pp. 497-498.
[14]. M. Castro and B. Liskov, "Practical Byzantine faulttolerance", Operating Systems Review, 33, 1998,pp. 173-186.
[15]. G. Chockler, R. Guerraoui, I. Keidar and M.Vukolic, "Reliable distributed storage", Computer,42, 2009, pp. 60-67.
[16]. Clavister, "Security in the cloud", ClavisterWhitePaper, 2008.
[17]. A.J. Feldman, W.P. Zeller, M.J. Freedman andE.W. Felten, "SPORC: Group collaboration usinguntrusted cloud resources", OSDI, October2010,pp. 1-14.
[18]. S.L. Garfinkel, "Email-based identification andauthentication: An alternative to PKI?",IEEESecurity and Privacy, 1(6), 2003, pp. 20-26.
[19]. S.L. Garfinkel, "An evaluation of amazon's gridcomputing services: EC2, S3, and SQS", TechnicalReport TR-08-07, Computer Science Group,Harvard University, Citeseer, 2007, pp. 1-15.
[20]. E. .Goh, H. Shacham, N. Modadugu and D.Boneh, "SiRiUS: Securing remote untrustedstorage",NDSS: Proc. Network and DistributedSystem Security Symposium, 2003, pp. 131–145.
[21]. G.R. Goodson, J.J. Wylie, G.R. Ganger and M.K.Reiter, "Efficient Byzantine-tolerant erasure-codedstorage",DSN'04: Proc.Intl. Conf. on DependableSystems and Networks,2004, pp.1-22.
[22]. E. Grosse, J. Howie, J. Ransome, J. Reavis and S.Schmidt, "Cloud computing roundtable", IEEESecurity& Privacy, 8(6), 2010, pp. 17-23.
[23]. J. Hendricks, G.R. Ganger and M.K. Reiter, "Lowoverheadbyzantine fault-tolerant storage",SOSP'07: Proc. 21st ACM SIGOPS symposium onOperating systems principles, 2007, pp. 73-86.
[24]. A. Juels and B.S. KaliskiJr, "PORs: Proofs ofretrievability for large files", CCS '07: Proc. 14thACM Conf. on Computer and communicationssecurity, 2007, pp. 584-597.
[25]. YevgeniyDodis Marisa DebowskyG22.3033-013 Exposure-Resilient Cryptography 17 January 2007

Author Profiles

Mr K.Chandra Mouli received his B.Tech information Technology fromKORM-Kadapa,JNTUAnantapur, and pursuing M.Tech in ComputerScience and Engineering from Vaagdevi Institute of Technology andSciences, JNTU-Anantapur.

Mr.U.Sesadri received his M.Sc (Mathematics) from Sri VenkateswaraUniversity-Tirupati. M.Tech in Computer Science and Engineering fromSatyabhama University. And working as a HOD in Computer Science andEngineering,MCA in Vaagdevi Institute of Technology and Sciences,JNTU-Anantapur