

12-2017

Attribute Based Encryption for Secure Data Access in Cloud

Anirudh Mittal

St. Cloud State University, anirudhm2803@gmail.com

Follow this and additional works at: https://repository.stcloudstate.edu/msia_etds

Recommended Citation

Mittal, Anirudh, "Attribute Based Encryption for Secure Data Access in Cloud" (2017). *Culminating Projects in Information Assurance*. 39.
https://repository.stcloudstate.edu/msia_etds/39

This Starred Paper is brought to you for free and open access by the Department of Information Systems at theRepository at St. Cloud State. It has been accepted for inclusion in Culminating Projects in Information Assurance by an authorized administrator of theRepository at St. Cloud State. For more information, please contact rswexelbaum@stcloudstate.edu.

Attribute Based Encryption for Secure Data Access in Cloud

by

Anirudh Mittal

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree, of

Master of Science

in Information Assurance

December, 2017

Starred Paper Committee:
Susantha Herath, Chairperson
Dennis Guster
Sneh Kalia
Abdullah Abu Hussein

Abstract

Cloud computing is a progressive computing worldview, which empowers adaptable, on-request, and ease use of Information Technology assets. However, the information transmitted to some cloud servers, and various protection concerns are arising out of it. Different plans given the property-based encryption have been proposed to secure the Cloud Storage. In any case, most work spotlights on the information substance security and the get to control, while less consideration towards the benefit control and the character protection. In this paper, a semi-anonymous benefit control conspires AnonyControl to address the information protection, as well as the client character security in existing access control plans. AnonyControl decentralizes the central authority to restrain the character spillage and accordingly accomplishes semi-anonymity. Furthermore, it likewise sums up the document get to control to the benefit control, by which advantages of all operations on the cloud information managed in a fine-grained way. Along these lines, display the AnonyControl-F, which ultimately keeps the character spillage and accomplish the full secrecy. Our security assessment demonstrates that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman presumption, and our execution assessment shows the attainability of our plans.

Index Terms: Anonymity, multi-authority, attribute-based encryption.

Acknowledgement

The successful completion of this paper could not have been possible without the guidance of my beloved professors, Dr. Dennis Guster and Dr. Susantha Herath. I also would like to thank Professor Sneh Kalia for being part of the committee and finding the time to read my thesis and special thanks to Dr. Abdullah Abu Hussein for his time to hear out the paper presentation.

I also would like to thank my mother Anuradha Mittal, my father, Lakshmi Narayan Mittal, and my friends who provided me immense support the entire way.

Table of Contents

	Page
List of Figures	10
Chapter	
I. Introduction.....	12
Problem Statement	13
Nature and Significance of the Problem	14
Objective of the Project	14
Limitation of the Project	15
Definition of Terms.....	15
Summary	16
II. Background and Review of Literature	17
Introduction.....	17
Background Related to the Problem	17
Literature Related to the Problem	17
Literature Related to the Methodology	21
Advantages and Disadvantages of Cloud Storages.....	23
Applications of a Cloud-Based Computing System	29
Concerns Regarding Cloud Computing	29
Summary	37
III. Data Breach in Cloud.....	38
Introduction.....	38

Chapter	Page
Types of Attacks	38
Motives of an Attacker.....	39
Guidelines for Privacy and Security in Cloud	40
Secure Data Sharing in Cloud and its Importance	43
Elements of Data Sharing Cloud.....	44
Key Management in the Cloud	45
Types of Cloud.....	47
Service Models for Cloud Computing	48
Summary	50
IV. Technology Overview	52
Introduction.....	52
Object-Oriented Programming Concepts.....	52
Java Inheritance	55
Polymorphism in Java.....	58
Logging Framework.....	61
Pipeline Framework	64
V. Methodology	67
Introduction.....	67
System Design	67
Data Flow Diagram.....	67
Use Case Diagram.....	68

Chapter	Page
Sequence Diagram	68
Activity Diagram	69
Data Flow Diagram.....	69
Data Consumer.....	69
Sequence Diagram	70
Use Case Diagram.....	71
Activity Diagram	71
Cloud Admin.....	72
Use Case Diagram.....	72
Sequence Diagram	73
Activity Diagram	73
Summary	74
VI. Feasibility Study and Implementation	75
Introduction.....	75
Feasibility Study	75
Economic Feasibility	75
Technical Feasibility.....	76
Operational Feasibility.....	76
Schedule Feasibility	77
Architecture Diagram and Main Modules	77
Registration-Based Social Authentication Module.....	78

Chapter	Page
Security Module.....	78
Attribute-Based Encryption Module.....	78
Multi-Authority Module	78
Algorithm.....	79
Anony Control and Anony Control-F	79
Summary	82
VII. System Configurations.....	83
Software Requirements	83
Hardware Requirements.....	83
VIII. Pages Designed	84
Introduction.....	84
Home Page	84
Registration Page	84
Login Page	85
Request Data Ownership.....	87
Providing Ownership	87
Data Owner Operations.....	88
Data Owner Uploads File.....	88
Data Consumer.....	90
Attribute Authority Login	91
Cloud Server Login.....	92

Chapter	Page
Summary	93
IX. System Testing.....	94
Introduction.....	94
Types of Tests	94
Unit Testing	94
Integration Testing.....	94
Functional Testing	95
System Testing.....	95
White Box Testing	96
Black Box Testing.....	96
Unit Testing	96
Test Strategy and Approach.....	96
Test Objectives.....	96
Features to be Tested	96
Integration Testing.....	97
Acceptance Testing.....	97
Summary	97
X. Results, Conclusion, and Future Work	98
Introduction.....	98
Results.....	98
Conclusion	99

Chapter	Page
Future Work	99
References	101
Appendix	105

List of Figures

Figure	Page
1. No Flow	68
2. Data Encrypted Flow	68
3. Sequence Flow	69
4. Authentication Flow.....	69
5. Data Consumption Flow	70
6. Verification Flow	70
7. Yes Flow	71
8. Decryption Flow	71
9. Cloud Admin.....	72
10. Yes Flow	72
11. Authentication Flow.....	73
12. Login Flow	73
13. Feasibility Study	75
14. System Architecture.....	77
15. Home Page	84
16. Registration Page	85
17. Success Full Registration.....	85
18. Admin Login.....	86
19. Private Cloud Login.....	86

Figure	Page
20. Data Owner Login.....	87
21. Request Data Ownership.....	87
22. Providing Ownership	88
23. Data Owner Operations.....	88
24. File Upload.....	89
25. File Details	89
26. Data Consumer Accessing Data from Cloud	90
27. Attribute Authority Login.....	91
28. Data Available in Application	92
29. Cloud Server Login.....	92
30. View File Details	93

Chapter I: Introduction

CLOUD Computing set up is a definite, advantageous, on request, arrange access to a mutual pool of configurable computing assets which could be quickly arranged and discharged with essential endeavors for administration or specialist organization association. Its primary target is to convey quick, secure, helpful information stockpiling and net computing, management, with all computing assets, imagine as administrations and conveyed over the Internet. Various computing ideas and advances could be used along with Cloud Computing to fulfill the computing needs of clients, it gives reasonable business applications online through web programs, while their information and programming are kept away on the servers.

It is an approach that could be used to boost the extension or venture up capacities vigorously without putting resources into the new system, sustenance modern workforce or permitting new programming. It gives the enormous ability to information and quick computing to clients over the web. Information security is one of the parts of the cloud which helps clients from utilizing cloud administrations. There is dread between the information proprietor particularly in strong associations that their potential information abuses by the cloud supplier without their insight. Data security of the clients is possible by utilizing the idea of virtual private systems, firewalls, and by upholding other security arrangements inside its boundaries.

Security is an essential module in any Cloud Computing Environment since it is crucial to guarantee that lone approved could be authorized, and ensured conduct acknowledged. Any safe and protection contradiction is fundamental and can create pivotal outcomes. When the strict directions and arrangements are against safety in the cloud, increasingly workforce will feel spare to receive computing. A customer might be the person or a significant association;

however, all are having the same concern, i.e., data security, so data security is the sad outcome. Data security at various levels is the crucial matter of this innovation, grouped into two classifications: Security at the External level and Security at Internal Level. Security at External level says that data are insecure contradicted to an outsider, cloud service provider or system interloper. Security at Internal level means that data is made available to approved clients or representative of an association.

A secure server gives an ensured establishment to facilitating Web applications, and Web server setup assumes an essential part of Web application's security. The Gravely designed server can prompt for unapproved get. An overlooked share can give an advantageous indirect access, while an unused port is an assailant's front entryway. Ignored client records can allow an aggressor to sneak past resistances unnoticed. Understanding dangers of the Web server and methods to recognize proper countermeasures grants to foresee many assaults and frustrate the steadily developing quantities of assailants. This system gives bi-directional encryption of correspondences between a customer and server, which ensures against listening in and messing with and additionally manufacturing the communication. Progressively, this provides a sensible certification that one speaks with unequivocally.

Problem Statement

Various layouts based on attribute based-encryption are proposed to secure the cloud storage, but most of the target on the data content privacy and the access control, while less attention given to the privilege control and the identity privacy. Data sharing in the cloud is very feeble to cyber-attacks since data stored on cloud servers, and multiple users access data from

unknown servers, resulting in Data security and privacy as critical issues for remote data storage.

This uncertainty of Data Privacy and User Integrity is the foundation of the study.

Nature and Significance of the Problem

A secure user enforced data access control mechanism is available to the cloud users to give them the flexibility to outsource sensitive data for cloud storage. With the need of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data. In this paper, the proposed solution guarantees a secured data exchange between the client and target server which cannot be accessed by an unauthenticated user. Secure Server Plus application has twofold login security. That is, after signing into the application client gets a mystery key on his enrolled Gmail id. The key entered on the fly up box showed in the wake of signing into SSP Application. This application has two functions, Encryption, and Decryption. Encryption is the usefulness in which the record sent over Gmail and divided into four chunks of in byte arrangement and afterward encoded utilizing various encryption calculations. After Encryption, documents delivered to the beneficiary through Gmail. At the recipient end, At the recipient end, the user downloads the documents and uses SSP Application data in the records is scrambled and consolidated.

Objective of the Project

This project aims to set up a secure layer for storing, retrieving and transfer of data across multiple users with Data Privacy, Content Privacy and User Identity intact. Proposed secrecy Control to let cloud servers to control clients' get to help without knowing their character data. The advocated plans can secure client's protection against every single expert. Halfway data revealed in secrecy Control and no evidence showed in secrecy Control-F. The proposed plans

are tolerant against specialist bargain, and trading off up to $(N - 2)$ experts do not cut the entire system down. Given formal investigation of security and execution to show attainability of the plan obscurity Control and obscurity Control-F. Initially, actualized the whole toolbox of a multi-specialist based encryption conspire secrecy Control and namelessness Control-F.

Limitation of the Project

The research has some limitation as follows: Difficult to user revocation. Whenever an owner wants to change the access right of the user, it is not possible to do efficiently. Decryption keys only support user attributes which are organized logically as a single set, so users can just use all possible combinations of characteristics in a unique set issued in their keys to satisfy the policies.

Definition of Terms

ABE. Attribute-Based Encryption: It is a Public Key encryption. Here the secret key of the user and ciphertext depend upon the attributes, i.e., on the address of the user or the kind of subscription attributes unique to the user. The two flavors of ABE are (KP-ABE)—Key Policy ABE: Here the Cipher Text along with the set of attributes and private key along with monotonic access structure like a tree, which describes the user's identity (e.g., IIT And Ph.D. or Masters). A user can decrypt the ciphertext if and only if the access tree in his private key satisfies the attributes of the ciphertext. The main drawback of KP-ABE is every time the user encrypts data the system must reissue the private keys to gain access to the file. (CP-ABE)—Ciphertext ABE: Here Cipher Text created with an access structure, which specifies the encryption policy and private keys generated according to user's attributes. A user can decrypt the ciphertext if and

only if attributes in the user's private key satisfy the access tree specified in the ciphertext. Here the private keys are not re-issued every time.

Summary

This chapter summarized on the need for the project, what the current issue is, and how it is handled with this project. Also, some project related terms have been detailed that are used in the next coming chapters. The scope and limitations are also listed in the chapter. In the following forthcoming chapter, a brief description of the background and literature review explained.

Chapter II: Background and Review of Literature

Introduction

In this chapter, the background related to the problem for which the project is a solution along with areas where analyzed to solve the problem. Reference to the analysis derived from other articles, also methodologies used in the literature.

Background Related to the Problem

Introducing bi-linear maps, give formal definitions for access structures and relevant background on Linear Secret Sharing Schemes (LSSS). Then the algorithms and security definitions of Ciphertext-Policy Attribute-Based Encryption with identity-based user revocation.

Literature Related to the Problem

According to Park (2011), the Computing service provider cannot be trusted entirely because of data security reasons, the danger of data safety and infringement of protection variables are considered. Particularly, ensuring data classification required to take care of these issues, Yu, Wang, Ren, and Lou (2010) proposed to conspire which guarantees data classification and fine-grained get to control. Be that as it may, data secrecy which was damaged by intrigue assault of repudiated client and cloud server. To take care of this issue, ensured data secrecy by putting away and separating data document into header and body. What's more, the strategy for an assignment about the entire or fractional message as indicated by delegates' consistent quality towards delegate utilizing sort based re-encryption is determined.

According to Yang and Ziaohua (2014), Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising strategy for getting to control of scrambled data, which requires a trusted expert to deal with every one of the characteristics and disseminates enters in the system.

In multi-specialist computing storage systems, the clients' qualities originated from various spaces each of which is overseen by another expert. In any case, existing CP-ABE plans cannot be connected explicitly to data get to control for multi-specialist computing storage systems, because of the wastefulness of scrambling and repudiation. In this part, the proposed DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), a robust and secure data get to control conspire with effective scrambling and disavowal.

According to Yu et al. (2010), Cloud computing is an arising computing model in which resources of the computing infrastructure is offered as services over the Internet. As promising as it is, this change also brings with it many new challenges for data security and access control when users outsource delicate information for sharing on cloud servers, which are not found within the same trusted domain as data owners. While trying to keep this sensitive, user data confidential from entrusted and prying servers, already existing solutions usually apply cryptographic methods by revealing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for the primary distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-granularity, scalability, and data confidentiality of access control remains unresolved. This paper addresses this challenging open issue by, on the one hand, defining and enforcing access policies based on data attributes, and, on the contrary, allowing the data owner to delegate most of the computation tasks involved in fine-grained facts to access control to entrusted cloud servers without disclosing the underlying data contents. This goal is achieved by putting in place the usage of techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

Our proposed scheme also has main properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed system is highly efficient and provably secure under existing security models.

According to Le, Yu, Zheng, Ren, and Lou (2013), Personal health record (PHR) is a rising patient-centric model of health information exchange, which is often outsourced to kept at a third-party, such as cloud providers. However, there have been grave privacy concerns as personal health information could be exposed to those third-party servers and unauthorized parties. To assure the patients' control access over to their PHRs, it is a promising method to encrypt the PHRs before outsourcing. Problems which includes risks of privacy exposure, scalability in the central management, flexible access, and efficient user revocation, have remained an essential challenge toward attaining fine-grained, cryptographically enforced data access control. In this paper, a novel patient-centric framework and group of mechanisms for facts access manipulate to PHRs saved in semi-relied on servers. To attain fine-grained and scalable data access control for PHRs, applications attribute-based encryption (ABE) strategies to encrypt every patient's PHR file. Different from preceding works in secure data outsourcing, the focus is on the multiple data owner situations and divides the users in the PHR system into numerous security domains that substantially reduces the key management complexity for owners and users. A high degree of patient privacy guaranteed simultaneously by exploiting multi-authority ABE. Our scheme additionally enables dynamic change of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency eventualities. Significant analytical and experimental results are represented which show the security, scalability, and efficiency of our proposed scheme.

According to Li, Yu, Ren, and Lou (2010), online personal health record (PHR) enables patients to manage their medical records in a centralized way, which greatly facilitates the storage, access, and sharing of personal health data. With the uprising of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, to enjoy the elastic resources and cut the effective cost. However, by storing PHRs in the cloud, the patients lose physical control to their health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to do fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is expandable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is essential to cut the critical distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.

According to Park (2011), Cloud computing service provider cannot be trusted due to data security reasons, the risk of data safety and violation of privacy factors accounted. Especially, guaranteeing data confidentiality needed. To solve these problems, Yu et al. (2010) proposed scheme which ensures data confidentiality and fine-grained access control. However, data confidentiality violated by collision attack of revoked user and cloud server. To solve this problem, guaranteed data confidentiality by storing and dividing data file into header and body. Also, the method of selective delegation about the or partial message according to delegator's reliability towards delegate using type-based re-encryption was specified.

As it is clear from the risks associated with cloud storage, it is paramount to direct central focus on strategic information security for cloud-stored data. Most multinational technology company, set to have many security challenges especially those emanating from cyber-attacks. Therefore, the corporations should adopt workable strategic information security by controlling the risks. These strategies involve taking adequate protection mechanisms for an information system, address the issue of the relationship between people and safety, the legal and ethical matters about security as well as employing efficient security principle that will help in control, mitigation and recovering from security threats.

Literature Related to the Methodology

A much larger organization that deals with information always working to plan on matters of risk management and safety rules they develop within their organization endeavoring to lower imminent threats to security. Due to high risks that compromise the safety, the goals of the information security have become more advanced where the security strategies need to take into the account the cloud systems, mobile platform as well as the social ecosystem (Blakley, McDermott, & Geer, 2001).

In many cases, the significance of coming up with information security strategy ignored. The plan for the security of information plays a significant role in acting as a roadmap for setting up effective security practices that are used in dealing with foreseeable future challenges (Alberts & Dorofee, 2002 cited in Li, Schucheng, Ren, & Lou, 2010). It helps corporations to meet long-term security goals through undertakings that will aid the business in a desired future condition of security. To ascertain long-term security for an organization, determining and understanding the status within the corporation and the set long-term goals for strategic security road mapping.

The backbone of an efficient information security incorporates management of risks, classification of different types of information, policies, standards, and ways as well as employee training and communication.

For many technology companies that specialize in developing, manufacturing, licensing and selling of various computer and mobile phones' software, personal computers, consumer electronics and provision of services to their products their first dealings concern information. Due to the increasing complexity of cyber-attacks and related impacts, the firms need to advance their information security strategies to help it in discovering, responding to and recovering from various security threats (Zhang, 2010 cited in Jung, LI, Wan, & Wan, 2015). The most effective preventive measures used by these organizations involve rigorous execution of weak remedies, configuration and transform management. As the industry of technology goes ahead to adopt mobile and cloud technology in information transformation and storage, companies should continue to improve their security control and risk management techniques and balance security threats especially those that do not coincide with needs of the business.

To successfully meet goals, an organization needs to adopt practical strategies for dealing with risks associated with information security (Humphreys, 2008 cited in Chase & Chow, 2009). The process for managing risk concentrates on providing an enterprise with a clear understanding of risk to give room for effective decision-making in controlling information risks. The method for risk management is applied in the stages of planning and designing as well as in the following steps monitoring and review of the risk, working deployment and improving various scenes to ensure proper management of information security risks.

One of the most significant elements of information risk management involves the assessment of the risk itself (Jerman, 2008 cited in Bethencourt, Sahai, & Waters, 2013). It is essential to understand the need for the business information security and the risks that an enterprises' assets face. Some of the most relevant activities in the assessment of information risk include identification of assets, pointing out the business and legal requirements that are significant to the established assets, assets valuation, pointing out vulnerabilities and critical threats to assets and assessing its likelihood and finally calculating the risk. Once the risk determined, it is easier to control it to make sure integrity of information.

The Microsoft Corporation has a framework for risk management called Microsoft Enterprise Risk Management Framework (ISRM) that outlines comprehensive control strategies for identifying and managing risks related to working processes and Forester adherence to the information control requirements. As a mechanism for risk management, the ISRM provide necessary guidelines to the business executives to help them in coming up with sound decisions. Such decision-making rules involve measuring the security risk of information against the goals of the business, the needs of the customers among other requirements (Spears & Barki, 2008 citred in Chase, 2013). The ISRM is very significant to the corporation as it supports the business across the range of all contemporary business situations that often affect the application, suppliers, infrastructure and the enterprise's security boundaries. In the same way, the new system will use this assessment technique to make sure that all the risk.

Advantages and Disadvantages of Cloud Storages

Technology is changing rapidly. It is developing at a breakneck pace globally and is taking over the way people live their lives every day. Comparing what computers used when

they were first invented, to what they are now, it is remarkable. Referring to the first computer, keywords/phrases that stand out are AOL, dial-up, big bulky computers, long loading times. Those days are long gone now with compatible new software and technology updates. Almost every household owns a computer or a device that can gain internet access. Also, there are too many locations that offer free WI-FI access to connect. This era has become so technology driven. It can even prove to improve quality of work by delivering service to users, cleverly leaves one in this chapter feeling very good about cloud computing but then encourages one to also think about its upcoming challenges. When thinking about the cybersecurity issues that are on an upward trajectory in our society or the digital divide that has our nation in an endless path, one cannot help but worry. Cybersecurity will always be an issue in this state. If one has a password, someone will be able to hack it. It is as if one has the lock, somehow someone will get the key or pick one lock. However, with cloud computing, that threat appears are less likely to occur, however, should not rule out that option. Cloud computing in governments would be much more efficient in the sense of hacking and cybersecurity. Why would one want to have private and confidential data on access to everybody who can get entry to that computer/device? Why not enlist in the cloud computing software that enables to secure data with a password and permits access to get that data on any device that can gain internet access. The days had gone when personal data stored on computer's hard drive. Cloud storage is the solution to the ever-present need for all digital property storage. Cloud storage is an alternate to buy new hard disks and deleting old files to create space. It is convenient and cost-effective. Cloud storage stores data on a server and not local hard drive. It helps in having back up, sync and access to the data on all possible devices that have an internet connection.

What it feels like an excellent way to track personal information. At the same time, It also feels that the mobiles today are so high-end that they have enormous storage capacity inbuilt. Music, photos, and document. The request line which has a command, target source, name, protocol name, version number. The request headers are file type information client accepts. The sovereign entity body passes bulk information to the server.

Two crucial measures of performance of a website are Some visitors: The several times a webpage browsed for indicates the usefulness and informative feature of the site. Ease of function: The ease at which the people can browse and navigate is another essential characteristic. The sites are user-friendly. The appeal of cloud computing is that it is cost-effective. It allows companies to take advantage of software without having to install any hardware (Jung et al., 2015). Users do not need to make upgrades to the system or reconfigure their servers; the vendor of the software manages all the software changes. Storing data can get expensive quick, just look at the different prices for iPhones based on how many gigabytes of space they have. More data means more storage and more money spent. They pay for the servers and infrastructure to support those servers and pay a monthly access fee for a desired amount of space.

As defined before, cloud storage is more of a service where the data stored is done in a remote-like manner, making access to the same a cause of concern. By allowing a variety of hosts to store data in their systems online, the system is continuously at a risk of being hacked, thus making security a primary concern for such systems that offer. The advantages of the same outweigh the disadvantages, making the use of the system advantageous. For most businesses, the ability to access saved files anytime is a competitive business advantage, making high cloud

adoption go to option to most companies (Yu et al., 2010). In this regard, most of the reasons that make cloud-based systems to get full recognition in firms include usability where the users have the ease of dragging the files they need into their local storages.

For this reason, the user can take any data they need from one place to the other in the absence of searching for the same. When it comes to sending data, usability makes the same easy. In this regard, bandwidth enabled. The user can post a web link over the net, reducing risks of losing data, mainly when the data is confidential. The potential for cybercrime is thus decreasing thanks to reducing the rewards for hacking. Cloud storage is also accessible. For this reason, the user can use the saved data anywhere, provided there be a steady internet connection.

The framework promotes the evolution of the culture of risk awareness hence improving accountability throughout an organization by implanting risk management processes for stakeholders across the enterprise. Apart from risk management in the organization, the framework plays a critical role in controlling the Risk Management Council which is a body put in place by various agencies in charge of the firms' information security. It also guides the company's Enterprise Business Continuity Management program that helps recovery and resilience guidance and the most effective practices that are adopted by stakeholders for protecting various assets and processes within the organization events a disaster. The ISRM also provides guidelines for compliance and streamlined risk framework that aids organizations in ascertaining that they have put in place effective policies to help the company to comply with the government regulations and industry standards. Other importance of the ISRM includes educating and creating awareness within the employees in the organization through targeted education and broad campaign. Finally, the framework influence behavior changes within the

company's employees by proactively highlighting on significant security issues, risks, and threats that originate from people taking part in activities that may have an adverse impact on the enterprise.

The rapid transformation in the information technology sector calls that organization invests more in cybersecurity technology to protect their computing resources from the growing threat landscape (Stoneburner, Goguen, & Feringa, 2002). In achieving this, companies concentrate on prioritizing and evaluating purchases, acquisitions and the future capacities to implement. Through the ISRM framework, the company employs both technical and procedural controls alongside best practices to provide security services to the firm. Some of the essential elements that organizations place priority on include evaluating and carrying out research on upcoming technologies and threats associated with them such as cloud storage. The companies also adopt systematic procedure used to determine the priority of security investment. Efficient protection mechanism should employ different efficient access control processes such as authorization, authentication and the most recent development of using biometric access control.

Authentication mechanism involves verification of the claimed identity of the user of any system. This type of protection method helps in preventing access to information by unauthorized people by ascertaining that the user is in communication with the planned system. This mechanism works by requesting a match to a known element of the user and something else that is owned by the requester (). The most common method of authentication mechanism used by most cloud systems is a password to allow access to various information by authorized people.

Mass storage forms the basis for creating the cloud-based system, giving the same the ability to store data as backup. For reasons of backups, the same can act as a bank of information by storing relevant data in remote files, only accessible via the internet. Thus, disaster recovery is an added advantage for any business system. Regarding ground space, the data saved up in the cloud storage also saves on storage space in the office and libraries where the files or books are in the same cloud storage. This advantage goes a long way in protecting any area in the offices that are used for saving data physically.

On the other hand, one advantage that overweighs the others is the cost saved by using any cloud-based system. Under this consideration, the cost of maintaining any physical files systems is eliminated by utilizing these systems. Due to the ease of access, the systems make business management cheaper compared to having physical systems. One main advantage of the cost is a reduction in cases of confidential cases which are vulnerable in an office setting. With the online storage system, the access to the same is reduced by allowing access to the users. Constant changing of passwords made possible by most systems encrypted makes the system more secure.

Before discussing the disadvantage, creating a foundation by considering the broad applications cloud computing has, an understanding of the advantages of hammered home. For starters, the applications of cloud computing are limitless. One must consider the middleware where the right middleware means that any cloud computing can almost do any one task that computer can run. It implies that almost anything including generic word processing software to use for customized computer programming is compatible with the right cloud-based computing systems associated with cloud storage neutralized.

Applications of a Cloud-Based Computing System

Various applications of the same cloud-based system increase the advantages of having the system installed. For this reason, the clients can use the data and even applications from anywhere they are. In this regard, the cloud-based system is convenient as it increased ease of accessibility. The only one need is the availability of internet connections to enable the access. The costs of hardware are also drastically reduced. This consideration is because the cloud computing applications used to execute all programs just like the standard desktop or laptop would. Thus, the need for external hardware and peripheral devices have eliminated the use of the complete system. The necessity of the hard drive is also reduced since the cloud can store data.

For corporations, the cloud software provides the client and the company with a similar platform to interact, eliminating the need to buy other computers to match the numbers of users. The shared pool created provides all the clients with the available means of access to the same, making its use more accessible and prudent. For most corporations, the elimination of such excessive hardware is proper since it eases on finances. Investing in equipment is also seen as outpaced since the technology changes rapidly over time.

Concerns Regarding Cloud Computing

The most significant worries over Cloud Computing are security and privacy. The idea of passing valuable data to another company worries some people. Corporate executives might hesitate on the use of cloud computing system because they cannot keep their business's information safe.

The counterarguments to this place are that the companies that are offering cloud computing services live and die by their reputations. It benefits these businesses to have reliable security measures in place. Otherwise, the service would lose all its clients. It is in their interest to use the most advanced techniques to protect their customers' data.

Some questions about cloud computing are philosophical; Does the user or company subscribing to the cloud computing service have the data? Does the cloud computing system, which provides the real storage space, own it? Is it possible for a cloud computing company to deny a client access to that client's data? Several companies, law firms, and universities are debating these and other questions about the nature of cloud computing.

How will cloud computing affect other industries? There's a concern in the information technology sector about how cloud computing will affect the business of computer maintenance and repair. If companies switch to using streamlined computer systems, they will have fewer IT needs. Some industry experts believe that the need for IT jobs will deviate to the back-end of the cloud computing system.

Another research area in the computer science community is autonomic computing. The autonomic computing system is self-managing, which means the system monitors take measures to prevent or repair problems. Currently, autonomic computing is mostly theoretical. However, if autonomic computing becomes a reality, it could cut the need for many IT maintenance jobs.

Privacy is a different matter. If a client can log in from any place to use data and applications, the customer's privacy might be compromised. Cloud computing companies will need to find ways to protect client confidentiality (Whitman & Mattord, 2011). One way is to use

authentication techniques such as usernames and passwords. Another is to use an authorization format -- each user can use only the data and applications relevant to his or her job.

Another form of protection mechanism is authorization that involves providing users access to specific objects. A user can use certain information by having his specification among the people allowed the access. This kind of protection may involve the use of some ticket to such as a coded card that can be interpreted by a machine to let access. Finally, is the use of biometric technology to allow access to information. This system provides access by comparing the users' details and biometric properties as detected by a machine. It is one of the most efficient methods of information security as people have different and unique biometric properties hence having minimal chances of making an error (Jain, Ross, & Pankanti, 2006). It is, therefore, paramount for an organization to choose the best protection mechanism depending on the situation to make sure information security.

There has been a significant turnover of employees in organizations dealing with information systems due to the dynamic nature of professions and safety information itself (Karabacak & Sogukpinar, 2005). Turnovers of security and policy specialists can lead to adverse losses of crucial information. In the recent years, the image of the corporate to people has gone through a remarkable transformation. The information security professions and the information system play a critical role in data integrity and the overall success of an organization. The information technology industry depends significantly on the high need for total security, confidentiality and personal ethics (Karabacak & Sogukpinar, 2005). The reputation of a firm might be ruined if its procedure of information security viewed as unsatisfactory or inadequate. The advancement in technology makes it easier to breach the

integrity of information and is very difficult to identify. For instance, security and innovation secrets can be easily transferred from one organization to another when personnel leaves from one company to another. It is, therefore, very significant for a corporation to be very keen on retaining and improving its employees' skills to lower this condition.

Therefore, it is essential for organizations to realize that for the company to lower risks and improve security across the firm, it must place its priority on people who are the most valuable assets that can help the enterprise meet its diverse goals. The corporations strategically leverage a mix of drive innovation, full-time employees, and proper management of services offered across the globe to achieve its aims and objectives. As a strategy, the company seeks to employee top information security and risk managers. In strengthening the ability of its people, the firm determines to keep talents in for managing information security by conducting various events to improve its employees' skills such as strategic job orientation, on-job-training, leadership as well as technical training. Every employee in the firm comes up with and maintains a professional advancement program paying particular attention to specific development requirements. With specific programs, employees can improve their skills hence their performance (Bulgurcu, Cavusoglu, & Benbasat, 2010). Also to promote on the workability of its employees, the organization hosts various security competition to improve awareness on matters about information security. Besides, Microsoft also funds some of its executive employees to take part in graduate information security courses as a way of adequately equipping them with necessary skills of dealing with dealing information security issues within the organization.

Amazon also employs the principle of data encryption to make sure data security in its cloud. Vormetric Data Security provides data security in Amazon's cloud through data encryption (Vormetric, 2011). According to Vormetric (2011), clients using the Amazon computing cloud can control and protect their private data through encryption. Robust encryption and flexible key management Vormetric offered for Amazon ensures that both structured and unstructured data in Amazon cloud is secure (Vormetric, 2011). As such, clients using Amazon cloud computing can confidently store and search for files and database in the cloud.

Establishment and maintenance of physical security of data storage centers are also necessary to make sure secure data storage in the cloud is safe. Moreover, it is essential that data stored in the cloud be protected from accidental loss especially when there is a breakdown of facilities and infrastructure. According to Infosecurity (2010), Google ensures that security enhanced at data centers to avoid any possible attack and access to the data. For instance, data stored in the government cloud, GovCloud, is usually stored in secure United States servers. Moreover, data in Google clouds are stored in different data centers to make sure that data is always safe and available even in cases of emergency..

Furthermore, one may look forward to such avenues as negotiating terms with their cloud provider and having the cloud provider give them their security and compliance requirements (Mishra, Mishra, & Tripathy, 2011). When looking at the broader picture, there are many reasons why an organization needs to secure an EMR system.

In today's world of the computer, the internet and e-commerce, security play a big part (Whitman & Mattord, 2011). Technology has come with increased crime hence necessitating the need for a legal and ethical framework to promote information security. Laws, therefore have

become necessary to protect those facing the security threat of data integrity. A significant part of the information and computer security in the contemporary world connected to the internet, and since there are no geographic boundaries in the internet, legal measures are very critical of guiding practices within the sector (Rees, Bandyopadhyay, & Spafford, 2003). Laws and statutes related to computer and information have a direct impact on the information security of a particular organization. They detect how the intrusion of computer security dealt with and investigated as well as giving the type of evidence to prosecute perpetrators of computer information security crimes (Jain et al., 2006). An organization's security policies much rely on the type of laws on the ground.

Cloud computing is becoming one of the critical words of the IT industry. The cloud is a metaphor for the Internet or infrastructure of communication between the architectural components, based on an abstraction that hides the complexity of infrastructure. Each part of this infrastructure behaves as a service, and allocated in data centers, using hardware shared storage and computing (Buyya, Yeo, Venugopal, Brogerg, & Brandic, 2009). To use the service, users need only take their machine operating system, browser and Internet access. All computing resources are available on the Internet. Therefore, the user's machinery does not need to have high computational resources. As a result, reducing the cost of the acquisition the system.

The goal of Utility Computing is to give the building blocks such as storage, CPU, and bandwidth of a network through specialized providers with a lesser cost per unit used. Users of services based on Utility Computing do not have to worry about scalability because the storage capacity provided is practically endless.

Another significant element of information security is vast ethnic corporations such as Microsoft as well as other systems that keep massive data deal with vast expanses of the internet, a domain with no cultural, national or geographic boundaries. Since cloud storage technology involves diversified information from diverse communities around the globe, with different beliefs and values, the company needs to embrace certain etiquette and responsibility when dealing with data to promote security.

Due to the diversity and complexity of various societies around the world, it is challenging to come up with laws that are acceptable to all organizations. Unlike statutes, ethics are fair and will not be imposed on people. Different people may have different ethical beliefs. It is, therefore, crucial for an organization to set social standards that will detect individual's interaction with information within the firm.

Many organizations have thus established expected behavior codes that it encourages its stakeholders to abide by. The ethical standards work hand in hand with the laws to define the due behavior at work to promote information security. These moral codes involve the element of privacy, confidentiality, and respect for personal space. The companies also conduct educative effects to educate its employees on the acceptable ethical laws at work as a way of promoting information security.

Intelligence software such as the PRT network can play a crucial role in promoting safety in cloud storage. The PRT network is an easy to install and use program that helps in monitoring one's system. The software supports the automatic recognition of network and gives alerts when there is an intrusion into one's network. Through the network, one can trace his historic network performance hence provides an opportunity for change and adapting to new condition. It also

notifies on the shortcomings of a system. Through the software, one can see all people who tried to use their network hence gives them an opportunity to prevent adverse outcomes of information insecurity.

Based on the literature analysis in this section, for a large corporation dealing with information systems, their success is primarily based on the security of information. As it has been clear, the company that uses cloud storage has made a remarkable effort in promoting information security through paying attention to various critical factors that include controlling of risks, protection mechanism, laws, and ethics and their relationship to safety and organizational people and security. Among the four factors, many organizations have achieved excellent performance on the controlling of risks and staff and security. There is also a significant response to other elements. However, most agencies should make a few adjustment and improvement to meet absolute information security. First, they should carefully choose employees by not only considering technical skills but personal integrity too. They should also create an environment that helps in promoting moral, loyalty and job satisfaction to lower employees' turnover who can adversely affect information security. Furthermore, they should also regularly remind their employees of their responsibility of promoting information integrity and protect the secrets of the trade appropriately as employees can transfer essential and confidential information to other parties including competitors hence impacting the business operation of the company. Finally, the organizations should also take defensive actions when discharging an employee for whether because of their undoing or as a strategy of cost reduction. Such workers are not allowed to get access to the sensor system with significant information until they leave the business premises. Any security strategies such as passwords used by the

discharged employee must be changed. With proper strategic information security, the organizations utilizing the cloud storage technology will be able to protect their data integrity hence promote their performance in the market. Many useful solutions come into picture by this research to cut the threats to data integrity. Many approaches come in to picture to assure the data integrity of cloud storage system. Ensuring information storage security in cloud computing by Wang, Wang, Li, Ren, and Lou (2009) proposed a verification scheme for public verifiability and data efficient operations and enhanced the POR model by changing the classic Merkle Hash Tree (MHT) construction for block tag authentication.

According to the ACM security issues which introduced a flexible and efficient way of the distributed method which meets the combined approach of storage correctness assurance and supported efficient dynamic operations on data blocks along with and data error localization in the distributed verification of erasure-coded cloud data.

Summary

This chapter details the background related to the problem which is the scope of this project. Also refers to the literature assigned to find the problem and various other literature references to see the possible solution with this project. The next chapter details security aspects of cloud. Applications of data sharing in Cloud. Different types of clouds and the service modules involved in cloud computing.

Chapter III: Data Breach in Cloud

Introduction

This chapter enumerates details on the different ways the data could be breached in the cloud. Access to unlimited resources makes it easy for the attackers to crack the security protocols and all the encryption algorithms deployed on the cloud server. Some ways to breach in the privacy and security in the cloud is detailed in the chapter. Also in this chapter motives of an attacker will be discussed.

Types of Attacks

There are many ways in which the security and privacy of cloud can be breached, they are:

- **Embedded Signature XML Attacks:** There are different ways in which XML signature wrapping attacks using which one can completely override the administrative rights of the Cloud user thereby manipulating user data by creating, deleting or duplicating user instances.
- **Attacks using Cross Site Scripting:** Attackers use injection a piece of code injected into web applications to override all access control mechanisms. Amazon Web Services evidently proved the XSS attack. Attackers could gain free access to all customer data, authentication data, tokens as well as plaintext passwords.
- **Flooding Attack Problem:** Attacker can send multiple anonymous bogus requests to the Cloud and easily overload the server. This attack will increase the workload of the cloud server and result in data loss.

- Denial-of-Service Attacks: Attacker deploys malicious code in the browser of the user which results in opening multiple browsers thereby producing the in denial of user's privileged access to services.
- Law Enforcement Requests: Cases in which FBI or government demands a Cloud Service Provider rights to use its data, the Service Provider is least likely to deny them. Hence, an inherent threat to user privacy and confidentiality of data.
- Problem with Data Stealing: Different methods used by the attacker to steal user account and password via brute-force attacks or over-the-shoulder techniques. The privacy and confidentiality of user's data will be severely breached. It's better to add more significant values while authenticating the user to avoid the breach. This substantial value or extra value is distributed to the user via SMS or email thereby mitigating the likelihood of data confidentiality issues.

Motives of an Attacker

There are many kinds of literature on securing a system against attackers, not much attention invested in the types of attackers and their motivations for carrying out such attacks. Both types of attack and the nature of attackers depend on the motive of the attacker. The following has some examples.

- Stealing valuable data: Hackers take data stored on the internet worth millions of dollars. With access to such useful data, they can then generate revenue, promote terrorism.

- To cause controversy: Attackers find amusing exploiting the data of the users stored in cloud thereby creating chaos and users suffer from their identity stolen and data breached.
- To get revenge: Organizations who strip their employees of their rights may express dissatisfaction by hacking the organization's network. When an organization makes use of the Cloud, this becomes all too easy for the former employee, and there have been many cases of this happening in the real world. For instance, there was the case of a former employee who managed to get access to the Cloud provider's server and deleted an entire season of a children's TV show (Li et al., 2013).
- To help: Sometimes organization hires hacker to find and analyze the laws in their security framework. The hacker may misuse the opportunity and plant a bot in the organization's network thereby leaving the privacy of the organization at the attacker's will.
- To gain prestige: Attackers show off their skills and earn fame by socially able to hack a large organization with stable security mechanisms. Hackers make it profession breaching large agencies.
- Curiosity: Some attackers are curious to learn something about an organization. These attackers even though have no intention to exploit the organization's assets, but they leave the organization's security framework vulnerable for other attackers to breach and use.

Guidelines for Privacy and Security in Cloud

The following are the impacts of Cloud:

- Governance. Every organization has their own set of standards, practices, protocols, policies, and ways to which every employee must abide by, and this can cover application development, testing, implementation, monitoring and so on. An organization based on Cloud services don't have proper rules and guidelines established for their employees thereby the employee unknowingly bypasses the standards required to support privacy and security of the Cloud Services.
- Compliance. This refers to set of established regulations, rules, guidelines which define the number of privacy and security laws within different countries, states, and so on. These rules followed by all the employees of the organization to avoid the breach and maintain the privacy of data since the data deployed on servers spread across multiple locations without the knowledge of the user.
- Trust. The Cloud Services Provides must make sure the trust placed by the organization is not broken. The cloud services providers have to make sure proper authentication protocols used to protect the corporation's data and all the cloud service provider employees must comply with their organization rules and prevent a data breach.
- Architecture. Cloud architecture designed must make sure provides privacy and security. For instance, IaaS Cloud providers (Li et al., 2013) can give Virtual Machine Images to consumers. Organizations which use these images store very critical data. Attackers may look at these pictures to leak information. Attackers supply a corrupted virtual machine image to users thereby breaching the user's confidential data. It is essential that the architecture of the Cloud designed in such a

way that it ensures privacy and security. Attackers are always on the lookout for security holes in Cloud architecture.

- Identity and Access Management. Apart from data sensitivity, privacy is a crucial aspect of cloud access. Current status and authorization framework for cloud access are stable but vulnerable to the insider's attack at the same time.
- Software Isolation. Multi-Tenant Cloud computing architectures, computations for different consumers executed in isolation even though the software remains in a single software stack. Applications in Cloud are susceptible to attack and quickly compromised, so isolation required to prevent such attacks.
- Data Protection. Data stored in cloud server is shared by many organizations. Some data is organization specific. Proper encryption logics are used to avoid data breach and loss of data. These data losses usually happen in data transit.
- Availability. As defined in the NIST Security and Privacy Guidelines [12], availability is the limit to which an organization's full set of computational resources is accessible and usable. Attacks such as Denial-of-Service attacks, server downtime, natural disasters affect the availability and can modify stored data and more importantly causes vulnerability to organizations data during events like server downtime.
- Incident Response. An organized method of dealing with the consequences a security attack. Cloud application has many layers such as application, operating system, network, database and so on. Event logs generated to record intrusion detection. The

complex layers and architecture consumer hours of debugging to find an attack in the Cloud.

Secure Data Sharing in Cloud and its Importance

Data in the cloud can be accessed by anyone from anywhere using any device across the planet. The organization finds this profitable since by just making their data available in the cloud they can charge customers for using their data and services irrespective of the location. With these advanced uses, there are disadvantages when it comes to privacy and security while data sharing.

Users love to share data across friend, colleagues, family thereby sharing their every instance of lives. The benefits of data sharing are listed below:

- Higher productivity: Organizations, Businesses get most of their work done by outsourcing, and this approach helps them in collaborating with their peers efficiently, finally satisfying their key to business goals. Hospitals benefit from data sharing resulting in gradual decrease of Medicare costs and access to more medicines available in different locations. Students benefit working on group projects thereby expanding their horizon to a more significant knowledge base.
- Limitless fun: Social networking channels like Facebook, Twitter, Instagram has brought a revolution in the daily living of an individual. It has enabled the ability to express and share the feelings and experiences every moment with friends and family. These applications help in socializing, marketing, business and other enormous uses which help the users to live life limitlessly. Using these apps gives limitless power to share data, access to unlimited resources.

- Promote and support opinions: People share information with the world to voice an opinion. People these days want to be heard, and social networking sites enable them in promoting their view, which was not possible without forming protests. Social networking sites such as Facebook, Twitter and YouTube are being used to raise awareness about real issues in the world. Some campaigns have led to violent protests, but the motive of online campaigns is to inform people of problems and encourage people to fight for a cause.

Elements of Data Sharing in Cloud

Enabling data sharing in the Cloud is essential that only authenticated users get access to data stored in the Cloud. Following is a summary of the ideal requirements of data sharing in the Cloud.

Data owner should specify a group of users that who can get access to his/her data. Members of the team should gain access to the data anytime without the data owner's intervention. User unauthenticated and not a member of the data owner's group should never gain access to the data, including the details Cloud Service Provider. All the grant and revoke privileges are with data owner and able to withdraw access to data for any member of the group. The data owner can add members to the team. No other member of the group can revoke rights of other members of the group or join new users to the group without the data owner's permission. Data owner specifies all the data manipulation permissions like read or write on the data owner's files.

Now let us look at the privacy and security need of data sharing in the Cloud. Achieving the requirements in the Cloud architecture depends on how many users involve adopting and embracing Cloud technology.

- Data confidentiality: Unauthenticated/malicious users should not get access to data at any given time. Confidentiality of data must remain intact in transit, at rest and on backup media. Access to information only by the authenticated user.
- User revocation: Revoked access rights to data for a user means he is no longer able to do read/write operations on the data and the dismissal should not affect other authorized users in the group for efficiency purposes.
- Scalable and efficient: Data stored in the cloud accessible by multiple users at the same instant. Cloud application must efficiently find the authenticated users, and it is operationally scalable.
- Collusion between entities: Data sharing methodologies might result in data collision in some instances which might expose data of different user groups. Cloud application must make sure that in situations of data collisions unauthenticated user must not get access to the data they are not privileged to access.

Key Management in the Cloud

Key management operations use key except encryption and decryption (Li et al., 2010) and includes creation/deletion of keys, activation/deactivation of keys, transportation of keys, storage of keys. The basic key encryption schemes for most cloud service providers to protect the data or sometimes leave it to the user to encrypt their own data.

There is always a need to encrypt data stored in Cloud. The challenges are how doing to handle the keys for encryption? Where should the keys be stored and who has access to those keys? How do to recover data if keys are lost? Encryption and key management are very important to help secure applications and data stored in the Cloud. With the advanced capabilities of Cloud providers there is indefinite need to adopt a robust key management scheme for their services. There are three ways Key Management can be effective:

- Securing key stores: The key stores is where the keys stored and created so high security protocols implanted in the key stores to protect them from malicious users. Gaining access to key means gaining the lead to the encrypted data associated to that key. Hence the key stores themselves are protected in storage, in transit and on backup media.
- Access to key stores: Access to the key stores limited to the users that have the rights to get access to data. Role authentication protocols to help control access. Key creation storing and retrieval owned by different entities with this approach the management becomes easy and in events of intrusion the cause to find and terminated quickly.
- Key backup and recoverability: Loosing a key means losing all the data associated to that key. Keys storage and backup solutions designed carefully. In case of events where keys destroyed there must be recovery options placed so that data associated to that key is retrieved and again a new key is generated to encrypt the data.

Types of Cloud

Cloud Computing has resulted in a significant workload shift wherein the local computers no longer need to run all the cumbersome processes instead of the series of computers connected on a network that forms a cloud will handle all the heavy lifting. This application of cloud computing reduces the demand for the hardware and software's employed at users end. User's computer able to run a Web Browser which is a cloud computing systems interface software and the rest handled. Three common types of clouds available are the Private, Public and Hybrid cloud.

Cloud setup and accessed over a private and secured intranet within an organization where only choose a pool of resources to share, store and retrieve data from Cloud. This kind of setup within a corporation owned and controlled by IT organizations is a Private Cloud. The cloud computing business model (Bethencourt et al., 2013) bought and managed in-house to enable shared IT services. The domain where the public Internet accesses cloud services is a Public Cloud. These are third-party cloud service providers who give their services for the interest of the public. Some examples include Salesforce.com, Google App Engine and Google search, Microsoft Azure, and Amazon Web services such as EC2. A Hybrid cloud consists of private and public clouds, where services from each domain consumed in an integrated fashion and include an extended relationship with the selected external service providers. It is imagined as an organization who have their private cloud but also depend on the data available on third-party vendors public cloud to integrate their services with the public data.

Service Models for Cloud Computing

The different cloud computing service models derived based on Private and Public Clouds implementations. Currently, the industry has been successfully adopting three common types of cloud computing service models.

Infrastructure as a Service (IaaS), is a service model around server's storage capacity, and network bandwidth. Examples include Amazon EC2 and S3, Rackspace, AT&T, and Verizon.

Typical things businesses do with IaaS include:

- Test and development. This mode of operation is where before launching an application there are phases in which development and testing complete. It is an iterative cycle that runs at the same time. Website hosting. Traditional website hosting platforms are expensive using IaaS it is cost efficient and time efficient.
- Storage, backup, and recovery. Organizations most significant challenge is maintaining the privacy of its customer's data and meeting the legal requirements at the same time handling the growing need for storage. IaaS is useful for controlling unpredictable demand and steadily growing storage needs. It also simplifies planning and provides flexibility in managing and designing backup and recovery systems.
- Web apps. Infrastructures of IaaS supports web apps, including storage, web and application servers, and networking resources. The organization can deploy web apps quickly. IaaS easily scale infrastructure up and down when demand for the apps is unpredictable.
- High-performance computing. Complex problems like calculating probabilities of an earthquake and protein folding simulations, climate and weather predictions, financial

modeling, and evaluating product designs involve millions of variables is possible by using IaaS as it gives High-performance computing (HPC) on supercomputers, computer grids, or computer clusters.

Platform-as-a-Service (PaaS) organization uses are:

- **Development framework.** PaaS is a framework on which the developers can develop or customize cloud-based applications. Like an Excel macro, PaaS allows developers to create applications by inheriting its built-in software components. The coding of the developers reduced since PaaS provides cloud features such as scalability, high-availability, and multi-tenant ability.
- **Analytics or business intelligence.** Service providing tools with PaaS allows organizations to analyze and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investment returns, and other business decisions.
- **Additional services.** PaaS providers also offer other services that enhance applications, such as workflow, directory, security, and scheduling.
- **Software-as-a-Service (SaaS).** A web-based email service such as Outlook, Hotmail, or Yahoo! Mail is what used a form of SaaS. With these services, the user logs into account over the Internet, often from a web browser. The email software on the service provider's network, and your messages stored there as well. The user can get access to email and saved messages from a web browser on any computer or Internet-connected device. The earlier examples are free services for personal use.

Organizational use is renting productivity apps, such as email, collaboration, and

calendaring; and advanced business applications such as customer relationship management (CRM), enterprise resource planning (ERP), and document management. These apps subscribed based on the usage.



IaaS is a framework that is used to build an application. The application developed depends on the services provided by the organization. For example, AT&T is a services provider of wireless and wireline services(Internet/TV). An organization like AT&T makes use of all the above service models. The website www.att.com is an application deployed on the web server where a customer can browse and buy desired services from the place they wish. The AT&T application developed on an IaaS infrastructure where again developer use the oracle's ATG e-commerce engine PaaS a platform/framework that has some inbuilt capabilities like all the e-commerce required engines starting from browsing the site, adding to cart, price calculation placing orders, orders reaching to Order Management System (fulfillment). AT&T also uses some SaaS base software like Apache Web app server, TDP, Rally to store the points and Cassandra database.

Summary

In this chapter the various aspects involved in cloud security along with the guidelines, importance of data sharing in cloud with the requirements inline for establishing the security. Also in this chapter the best methods for Key Management detailed. This section also details the

different types of Cloud and their application. The services models described in this chapter helps in understanding the different ways service models in cloud computing used for cost and experience benefit. The next section is for the methodologies used for the project implementation and the various stages of project development cycle like Analysis, Design Data, Collection, etc.

Chapter IV: Technology Overview

Introduction

This chapter gives an overview of the underlying technologies used to develop the project. Java is the base of the development process and is integrated with the micro-services framework. The framework has predefined libraries and functions which can be inherited to invoke existing encryption methods and on top of it the additions of the new algorithm to support enhanced encryption.

Object-Oriented Programming Concepts

Starting with the basic definition of Object which means an entity which is defined via dimensions usually refer to a thing in the real world. Like a mobile, laptop, chair, etc. A program designed using the concept of Classes and Objects. Concepts such as Object, Class, Inheritance, Polymorphism, Abstraction, and Encapsulation simplifies development and maintenance. An object is a state or behavior of an entity. It is a physical or a logical definition. Grouping or Collection of such objects which have the same behavior called a class represents the logical entity. Inheritance is using the existing functionalities and defining new methods. In other words, an object acquiring all the behaviors and functionalities of its parent object. The approach helps in code reusability as well as help in runtime polymorphism. Performing a single task in different ways refers to Polymorphism. For the word 'hello' used to greet someone can also be phrased as 'hola.' The difference is only the language, but the functional aspects are same. Hiding the inner details and just exposing the functions refers to Abstraction. For example, the cell phones are daily without knowing the internal processing involved. Java uses abstract classes and interfaces to enable abstraction. Encapsulation refers to binding or combining code and data as a single

unit. For example, a capsule is an encapsulation of different medicines. The concepts of OOPs enable data hiding and grants the ability to simulate real-life events efficiently. Naming conventions in Java provide better code readability, in a sense, it is time efficient in figuring out why the code is developed. The different naming convention in Java is:

- Class Name. Should be a noun and start with an Uppercase letter like String, Thread.
- Interface Name. Should be an adjective and start with an Uppercase letter like Remote, Event listener.
- Method Name. Should be a verb and start with a lowercase letter like print(), running().
- Variable Name, Should start with a lowercase letter like lastName, streetAddress.
- Package Name. The whole name should be in the lowercase letter like lang, util.
- Constants Name. The whole name should be in Uppercase like MAX_DURATION, SPEED_LIMIT. Every organization has their standards, but the base of Java naming concepts is the same. Rules are built on top of this base.

Objects and classes used to design a program in object-oriented programming techniques.

Object refers to a physical and logical state of an entity whereas a Class is a logical entity only.

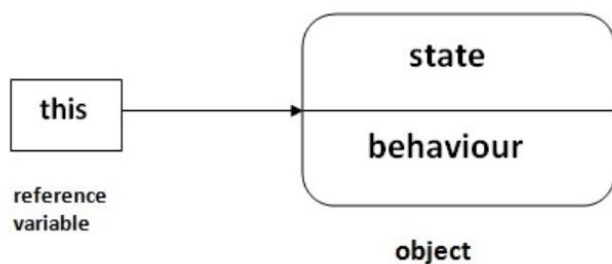
Objects are entities that have state and behavior which is physical or logical and tangible or intangible. Banking systems are an example of intangible objects. The characteristics of an object determined by its State—data or value the object represents, Behavior—describes the functional aspects like start, stop and Identity—refers to the unique ID assigned and used by JVM to find objects uniquely not visible to the user. For example, a phone is an object. It is named as Apple, color is white which indicates the state and used to call, or text is its behavior.

An object is an instance of Class, the template and blueprint of the class are used to create objects. In other words, objects are the result of a class. Objects are real and runtime entities and determined by their state and behavior.

Classes are collection or grouping objects of similar functionalities and are just logical entities. A class in Java has fields, methods, constructors, blocks, nested class, and interface. The instance is variable created inside the class but outside the method. Instance variable gets memory at runtime when an object(instance) created and doesn't get memory at compile time. To expose the behavior of object functions called methods in java. The method gives us the capability of Code Reusability and Code Optimization. New is a keyword in java that helps in allocating memory at runtime. Heap memory is where all objects get memory. Real-time development involves creating classes and use it from another class. The constructor in java are methods used to initialize the object. At the time of object creation, java constructor invoked. The constructor constructs Values/Data for an object. Rules involved in creating a constructor are it should have the same name as its class name and should not have an explicit return type. Two types of java constructors are Default Constructor—the constructor that has no parameter set, i.e., it helps in assigning default values like null, or 0 and Parameterized Constructor have parameter used to give different values to the distinct objects. Technique in java called Constructor overloading is in which a class can have any number of constructors, and they differ in parameter lists. Compiler segregates these constructors by accounting the number of parameters in the list and their type. The constructor initializes the state of an object whereas Method exposes the behavior of an object. The method has a return type because Constructor does not. Method invoked explicitly, and Constructor invoked implicitly. The compiler provides

a default constructor but does not give a method. A method is independent of the class name because constructor must have the same name as its class name. Java does not provide a copy constructor like c/c++, but one can use clone() method. Memory management is mainly performed by Static keyword in java. Static keyword applied to variables, methods, blocks and nested class. The static keyword belongs to the class than the instance of the class. The static keyword is: variable (also known as the class variable), method (also known as the class method), block and nested class.

Variable used for the current reference of the object called This keyword. Uses of this keyword refer to the current class instance variable. It is used to invoke current class method (implicitly), this() used to invoke the current class constructor, it is passed as an argument in the method call, it is passed as the argument in the constructor call, this is used to return the current class instance from the method.

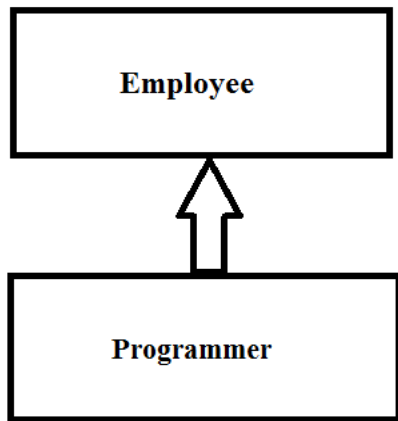


This Variable

Java Inheritance

Inheritance in Java refers to a mechanism where one object acquires/consumes all the properties and behaviors of the parent object. The idea is to create new classes built on existing classes. Inheriting from an existing class means reusing methods and fields of the parent class, and adding new methods and fields on top of it. IS-A Relationship Inheritance represents, also

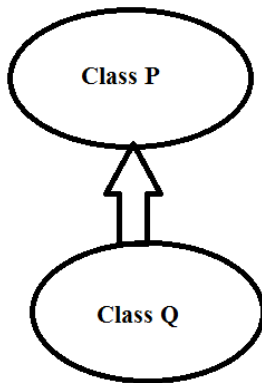
known as the parent-child relationship. Inheritance helps in method overloading that is runtime polymorphism and code reusability. Keyword Extends indicates deriving a new class from its parent's class. Extend means to increase the functionality [16]. Classes inherited is called a parent or superclass and class which inherits is child or subclass. In the below figure Employee is a parent or a superclass and Programmer is a child or subclass. It can also be said that all Programmer -> IS -> A -> Employee.



Inheritance

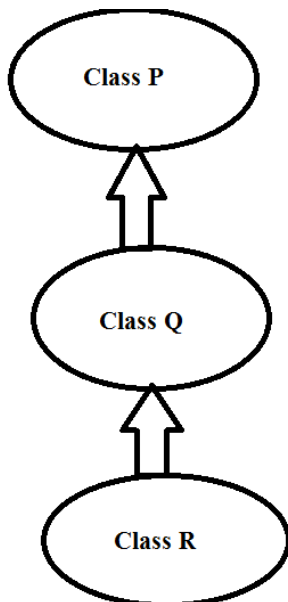
There are three types of inheritances in Java—Single, Multilevel, and Hierarchical.

Single inheritance refers to one parent and one child class. In the figure below, class P represents Parent or Superclass, and class Q represents child class or subclass.



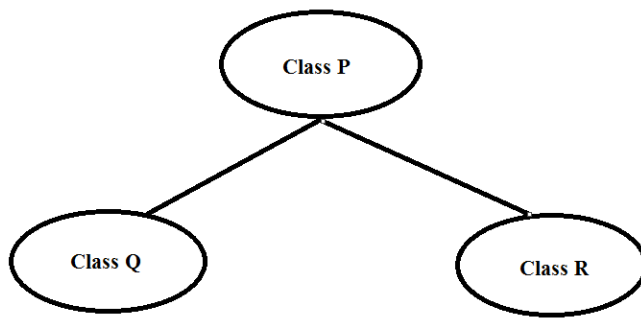
Single Inheritance

Multilevel inheritance is one in which a child class or subclass becomes a parent class or superclass. For example, in the below figure class P is the parent class for class Q and class Q is the parent class for class R. In this way the class Q is a child class for P and class R is a child class for class Q and class R inherits the capabilities of class P by inheriting class Q but not by directly inheriting class P.



Multilevel Inheritance

Hierarchical inheritance is where class P is inherited by both class Q and class R. This means that class P is the parent or superclass for both class Q and class R and class Q and class R are the child or subclasses of parent P.



Hierarchial Inheritance

Aggregation refers to a class that has entity reference. Aggregation also relates to HAS-A relationship. In the below example Employees is a class that has definitions like id, name, address, etc. Here address is an aggregation to the class employee as it has its definitions like street address, apartment number, city, state, zip code. Aggregation improves code reusability.

```

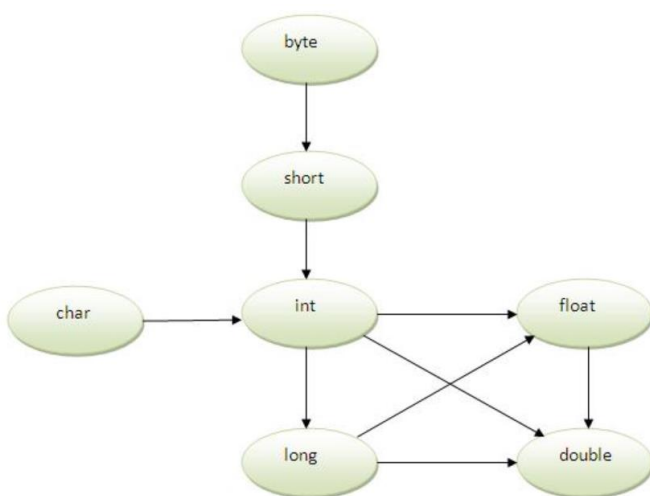
class Employee{
  int id;
  String name;
  Address address;//Address is a class
  ...
}
  
```

Class Employee

Polymorphism in Java

Method overloading refers to the classes that have the same name but different parameters. Readability of the program increased to do only one operation, having the same name as the methods. To perform addition of the given numbers with any number of arguments,

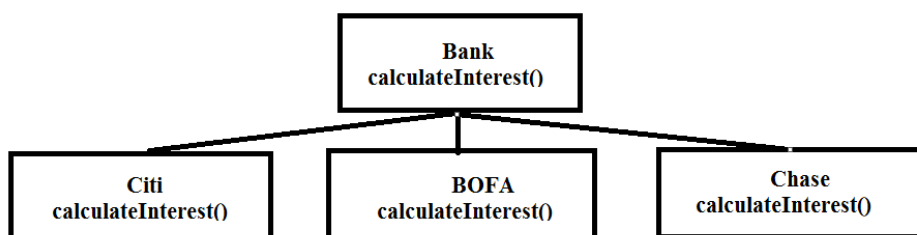
the method such as `x(int, int)` for two parameters, and `y(int, int, int)` for three parameters then it is complicated to understand the behavior of the method because its name differs. Method overloading helps us to figure out quickly. A method overloaded by changing the number of arguments or by changing the data type. Method overloading and type promotion explained if one type promoted to another implicitly and if no matching data type is found. In the following figure, byte promoted to short, int, long, float or double. The short data type promoted to int, long, float or double. The char data type promoted to int, long, float or double and so on.



Method Overloading

Method overriding in Java refers if a subclass (child class) has the same method as declared in its inherited parent class. It can also be explained as a method defined in the child class or subclass is already present in its super or parent class then overriding method concept invoked. Method overriding used to give a specific implementation of a method that is already provided by its superclass and used in runtime polymorphism. Rules involved in java method overriding are method must have the same name and parameter defined as in the parent class, and it is an IS-A relationship (inheritance). For example, the Bank as a parent class and Citi,

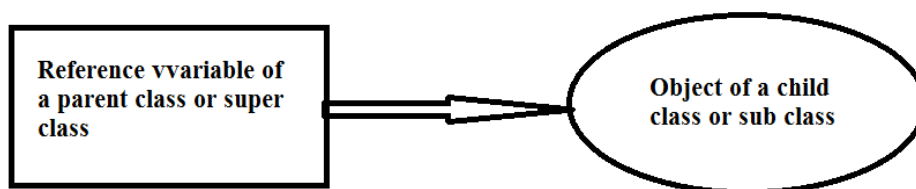
BoFA, Chase as its child or subclasses. Bank has a method to calculate the rate of interest, but Citi figures at 11%, BofA 10.11%, and Chase 13%. This means all the child classes are using the parent's method for calculating interest with the same parameter and method name but the interest value is different.



Method Overriding

Keyword `super` is a reference variable in Java and used to refer the immediate parent or superclass objects. Parent class immediate to the instance variable referred by `super` keyword. Immediate parent class constructor invoked by `super()` and immediate parent class method can also be invoked. Instance data member initialized by using Instance Initializer block. To restrict the user in many instances the java `final` keyword used Final a variable, method or class. Final keyword implemented along with a variable. An uninitialized final variable also called as the blank final variable has no value associated with the variable. It is initialized to the constructor only. The blank final variable is static and will be initialized in a static block just. Values cannot be changed for Variables declared as Final. Polymorphism in Java categorized as Compile time polymorphism and Runtime polymorphism. Method overloading and method overriding help in achieving polymorphism. Overloading static methods in java called Compile time polymorphism. Runtime polymorphism or Dynamic Method Dispatch is a Process in which call to an overridden method resolved at runtime instead of at compile-time. Superclasses reference

variables used to call an override method. The object being referred by the reference variable is used to find the method called. When a parent class or superclass variable refers to the object of its child class is known as upcasting.



Upcasting

The process of connecting a method body to the call made to invoke the method called Binding. Binding is Static (binding is done early) or Dynamic (binding is done late). Static binding at compile to determine the type of object at compile time. Methods like private, final or static defined in a class is an example of static binding. Type of object determined at runtime is Dynamic Binding. To determine if the object is an instance of class or subclass or interface, the Java instance of operator is used. It is also called as Comparator as used to compare the type of object with the instance of the object. The output of this operator is 0 'false' or 1 'true.' All null variables have the instance of operator output as False.

Logging Framework

AJSC6 is based on the EELF logging and Error Logging framework. It wraps a lot of the functionality for us hiding the configuration and complicated settings. MDC values already set by AJSCEelfManager. RemoteHost—The remote hostname/IP address making the request. ServerFQDN—Servers fully qualified domain name. ServerIPAddress—Server IP address. Hostname—hostname serviceName—service being called version—version (application jar version) PID—Process ID is provided by the system transaction Id—UUID (If not presented as a

header request param then it will generate its uuid) request timestamp—request time stamp
 responseTimestamp—response time stamp
 AJSCEelfManager initialize the MDC properties and returns an EELFManager it is a singleton. All customer-facing APIs should have a provision for providing the UUID in its header. If not provided, AJSC will auto-generate a UUID.

```

HelloWorld getQuickHello(
    @HeaderParam(ApplicationConstants.TRANSACTION_ID)
    String transactionId,
    @ApiParam( value = "Name", required = false )
    @QueryParam("name")
    String name);

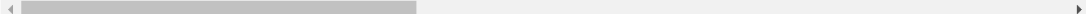
```

The logback configuration in each AJSC project defines the format of the logs

```

<property value="%d{yyyy-MM-dd HH:mm:ss.SSS} $ version: %X{version} threadId: {PID:- } %-5level namespace:${namespace} %logger{20} [
<property value="%date{ISO8601,UTC}|%thread|%. -5level|namespace:${namespace}|%logger{20}|%X{ServerIPAddress}|%X{ServerFQDN}|%X{service

```



These have the important MDC values already set. One can add additional ones from the preconfigured ones above. The AJSC6 archetypes provide us with to formats as samples but can create its format to suit its requirements. Attached is a sample logBack.XML extended to save the different loggers (audit, app, performance, metrics etc.) in different files.logback.xml. By default, the logs will all be application logs. To use the specific logger for different purposes, they must be invoked separately.

```

For ex: private static EELFLogger metricsLogger = AjsceelfManager.getInstance().getMetricsLogger();

```

```

metricsLogger.info(LogMessages.RESTSERVICE_HELLO);

```

It will add logs to the metrics specific logs. Also attached is the document provided by the AJSC team on EELF. Implementation of EELF.DOC. More samples are available at

<https://github.com/att/EELF/tree/master/EELF/src/test/java/com/att/eelf> Steps to add application

log messages. Define the log message in the resource files log

message.properties:

```
RESTSERVICE_HELLO_NAME=SERVICE0002I|Get a quick hello for {0} |No resolution needed|No action is required
```

Update the LogMessage.java Enum for the new message:

```
RESTSERVICE_HELLO_NAME, /** The sprinservice hello. */
```

Use the appropriate logger for logging the message:

```
log.debug(LogMessages.RESTSERVICE_HELLO_NAME, name);
```

Sample application log for a API call:

```
2017-06-19 16:54:00.255 $ version: 1.0.0-SNAPSHOT threadId:
{PID:\- }
INFO namespace:com-att-ajsc c.a.a.c.m.TransactionIdResponseFilter [ hostname: LP-507B9DA1D355.HCLT.CORP.HCL.IN serviceName: idp-ms-
```

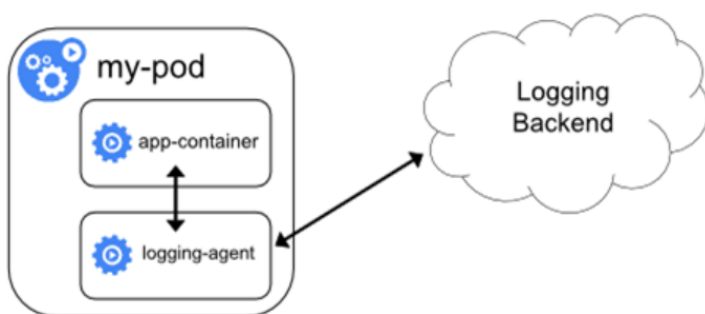
Performance Tracing—Use `@Tracable(message="<custom message>")`

It will call the tracing interceptors for the complete flow, including the sub-methods called during the process. Sample output—where `@Tracable` has been added to the Rest Service and the internal service implementation (Each ‘-‘ hyphen indicates the depth of the call)

```
AJSC60001I Trace log:
Transaction Id=2ac621b2-6e96-4272-ae73-eb2ac520b026
Start Time=1497871435499
End Time=1497871440248
Total Time=4749 millis
-5 millis for Invoking PreInterceptor
-34 millis for invoking quick hello
--8 millis for invoking quick hello service
-2 millis for Invoking PostInterceptor
```


While the execution time seems to be shown high (This is because of the `getHostName` API call, which works fine when executed within Kubernetes <15 ms).

Kubernetes based logging each microservice will be deployed inside a pod, and there will be multiple instances of the same running (based on the requirement). There will be a need to drain out the logs, index them for monitoring. It can be done via long spout or fluid. Fluentd is the recommended approach by the kubernetes community and is documented as well. There are multiple deployment modes for this. One is shown below where the fluentd based logging agent streams the logs out to the logging backend (ELK, Splunk, etc.). Kubernetes are logging via fluentd to ELK, Splunk <https://kubernetes.io/docs/concepts/cluster-administration/logging/>.



Logging Framework

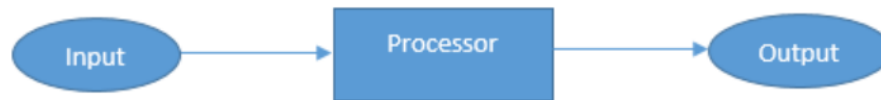
If desire is to introduce new MDC properties, they must be added as utilities in the foundation layer and then these can be used in the patterns as shown in #5.

For example `MDC.put("IDP_XXX", <value>)` Then use it in the logback format as `%X{IDP_XXX}`

Pipeline Framework

This Pipeline framework aims to replace pipeline framework available in ATG. To understand what is pipeline as per the name implies, it's a sequence or branches of the various unit of processing logic put-together serves for single common functionality. There are three

significant components Processor, Pipeline, and PipelineBuilder. The processor is a unit of business logic performed for given need or called as processing units.



Single Processor

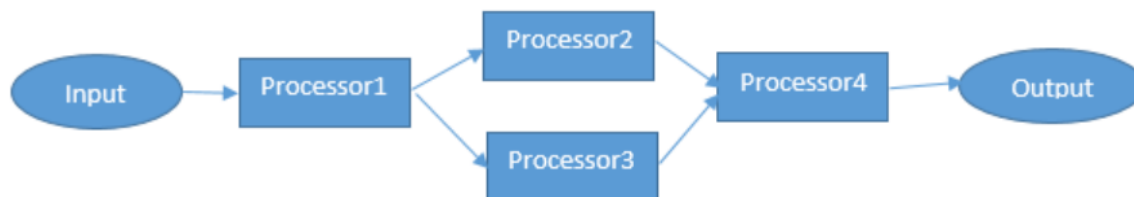
The pipeline is a collection of the processor, and it's built using pipeline builder. The various processing logic can be executed in simple sequence (or) could be based on some condition/predicates one after another.

Plain series of processing units:



Multiple/Pipeline Processors

Conditional based processing units:



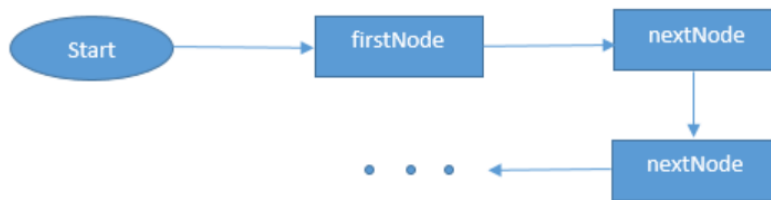
Multilevel Pipeline Processors

Pipeline Builder: Like it, names imply pipeline builder provides various provisional methods to build a pipeline with simple sequential processing, (or) conditional based processing, (or) complex based nested conditional based processing. The list of methods used to build the pipelines explained in detailed. First: It defines the very first processing units of pipeline called primary processor or initial node or merely first node.



First Node

Next: This method defines what could be the next processing units that follows first node.



Next Node

Branch and join: Branch defines pipeline execution to choose the path between different path. Branch end-point could be a processor or could be another pipeline. Join methods wait for all branch execution completed and go head to next node or end-point.

Code Snippet:

```

public void test() {
    final PipelineBuilder<PurchaseRequest> approvalBranchPipeline = PipelineBuilder.<PurchaseRequest>builder()
        // lambda expressions can also be used
        .first(p -> System.out.println("Asking for approval amount=" + p.amount)).next(new GrantApprovalProcessor());

    final PipelineBuilder<PurchaseRequest> silverCardBranchPipeline = PipelineBuilder.<PurchaseRequest>builder()
        .first(new MakeSilverCard()).branch(approvalBranchPipeline).join().next(new SendSilverCard());

    final PipelineBuilder<PurchaseRequest> goldCardBranchPipeline = PipelineBuilder.<PurchaseRequest>builder()
        .first(new MakeGoldCard()).branch(approvalBranchPipeline).join().next(new SendGoldCard());

    final PipelineBuilder<PurchaseRequest> defaultCardBranchPipeline = PipelineBuilder.<PurchaseRequest>builder()
        .first(new MakeDefaultCard()).branch(approvalBranchPipeline).join().next(new SendDefaultCard());

    final PipelineBuilder<PurchaseRequest> mainPipeline = PipelineBuilder.<PurchaseRequest>builder()
        .first(new InitialProcessor()).next(new AddAmountProcessor())
        .branch(goldCardBranchPipeline, p -> p.amount > 3000)
        .branch(silverCardBranchPipeline, p -> p.amount > 2000 && p.amount <= 3000)
        // if none of above condition matches the execute default branch
        .branch(defaultCardBranchPipeline).join()
        // After join continue the pipeline chain
        .next(new NotifyCustomer()).next(new UpdateCustomerRecord()).build();

    mainPipeline.execute(new PurchaseRequest(3000));
    mainPipeline.execute(new PurchaseRequest(2000));
    mainPipeline.execute(new PurchaseRequest(1000));
}
  
```

Chapter V: Methodology

Introduction

In this chapter, the design incorporated for the study data collection, analysis to get the required data for the project. Details on budget and timeline are included in this chapter.

System Design

DATA FLOW DIAGRAM / USE CASE DIAGRAM / FLOW DIAGRAM

The DFD is also called a bubble chart. It's far natural graphical formalism that may be used to symbolize a system about the input data the system, different processing executed on these data, and the output data is generated via the system.

Data flow diagram. Figure 1 illustrates the flow of data: On user, action the data is first **UPLOADED** by the authenticated DATA OWNER in cloud database via the application and then the attribute-based encryption algorithm triggered to encrypt the data. After the first stage of encryption again identity-based attribute encryption algorithm triggered to bind the encrypted data with the user identity resulting in re-encrypting the data and is stored as is in the cloud cache database. For an unauthenticated user, the application flows through the '**no**' flow.

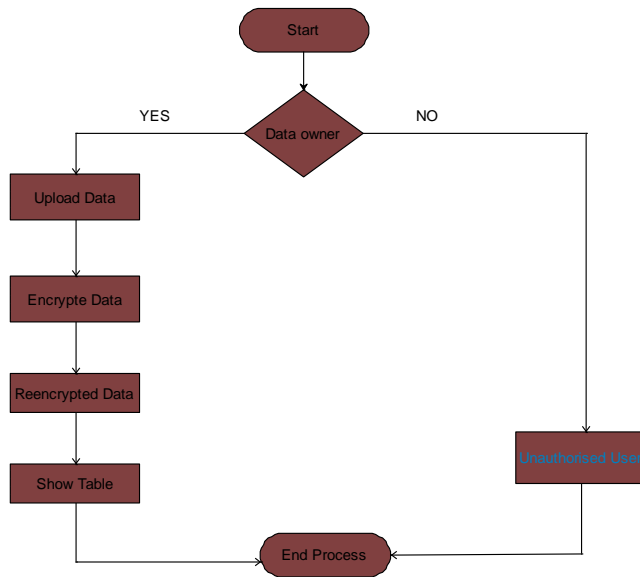


Figure 1. No Flow

Use case diagram. In Figure 2, only if the user is authenticated by the application at the time of LOGIN then the data owner can perform actions such as upload data, encrypt data, re-encrypt data and show table where the re-encrypted data is stored in the cloud database.

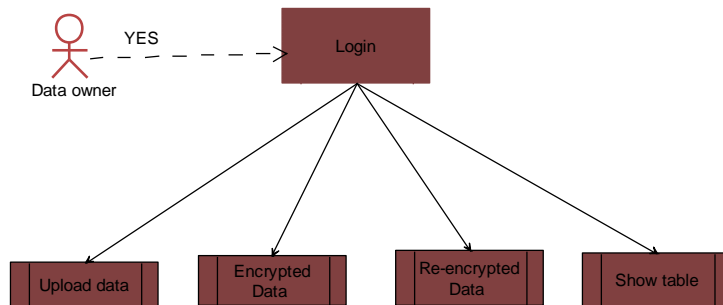


Figure 2. Data Encrypted Flow

Sequence diagram. Figure 3 illustrates the sequence flow from the time the data owner logs in into the application as an authenticated user till the time the re-encrypted is stored in the cloud database.

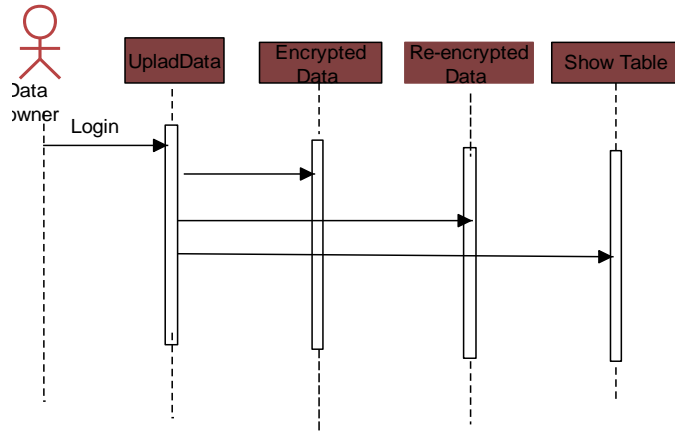


Figure 3. Sequence Flow

Activity diagram. Figure 4 highlights the activities that an authenticated data owner can do when he logs into the application.

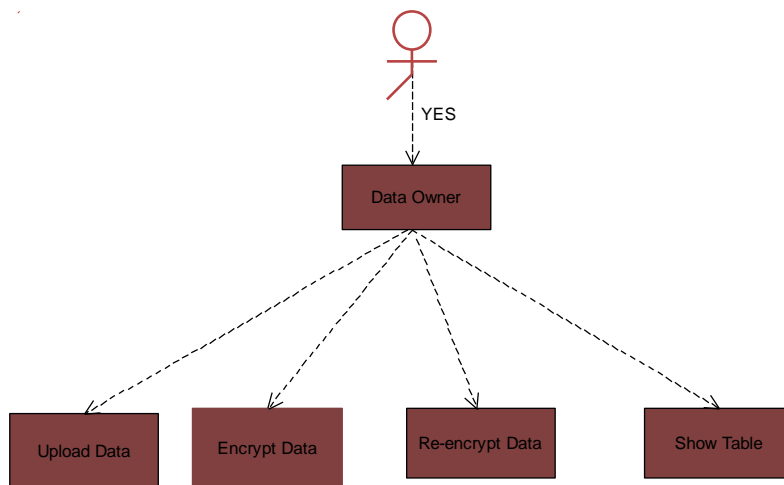


Figure 4. Authentication Flow

Data Flow Diagram

Data consumer. Figure 5 illustrates the data consumer actions from the time he logs in to the application as an authenticated user till he downloads the data.

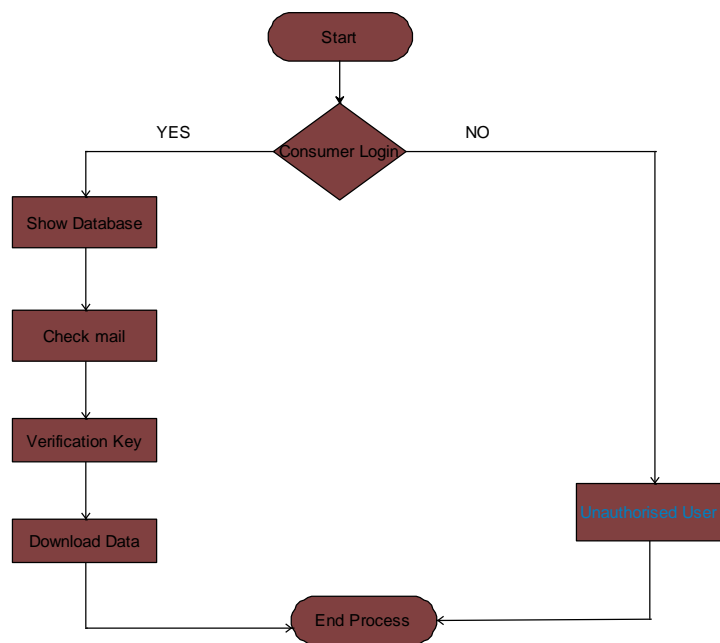


Figure 5. Data Consumption Flow

Sequence diagram. Figure 6 illustrates the sequence of consumer actions after login into the application and when he tries to query the database a mail sent to his Gmail id with the verification key which enables him to download and decrypt the data.

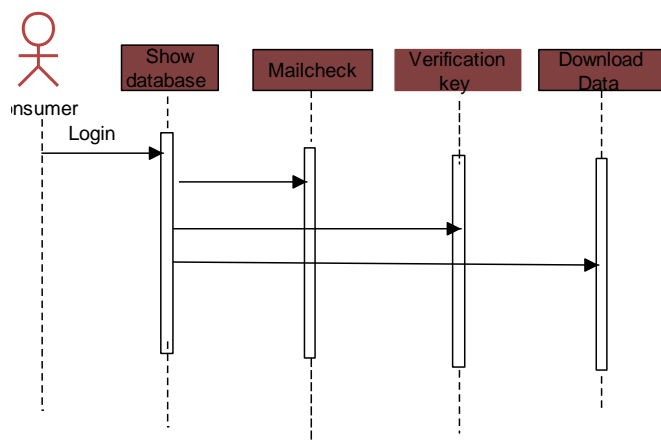


Figure 6. Verification Flow

Use case diagram. Figure 7 illustrates the use cases that consumer can do when he is successfully authenticated in the application and goes through the 'yes' flow.

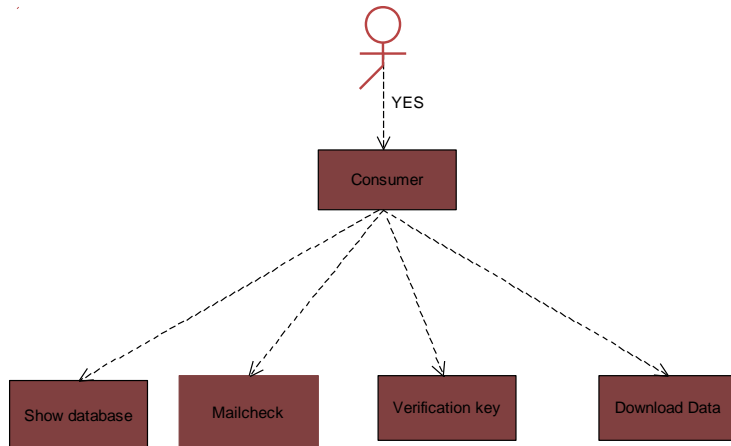


Figure 7. Yes Flow

Activity diagram. Figure 8 illustrates the various actions that an authenticated data Consumer can do in the application. From the start process, he can view the database to see what data he needs to get the required authenticated keys to decrypt the data in the readable form.

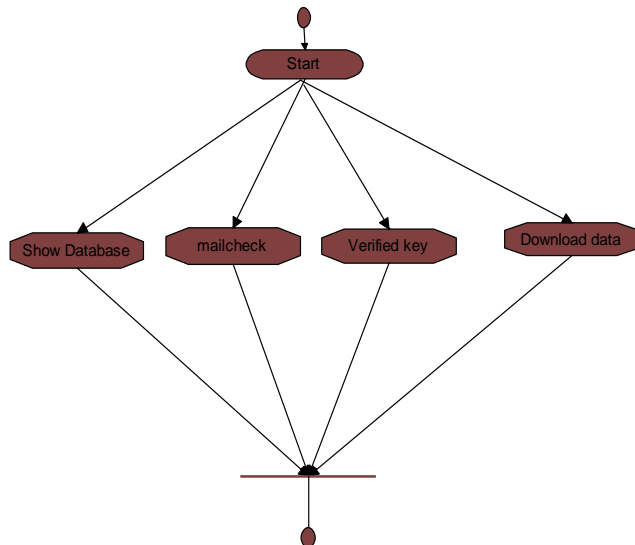


Figure 8. Decryption Flow

Cloud Admin

Use case diagram. Figures 9 and 10 are the use cases for a Cloud Admin. Once the authentication for the Admin is successful, the ‘yes’ flow invoked and the Admin can then do the operation like health checks of the database, make sure the encryption/decryption algorithms are all in place and the graph generated does not have unstable spikes.

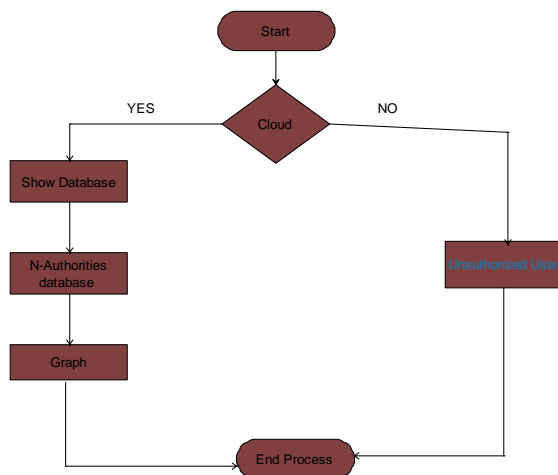


Figure 9. Cloud Admin

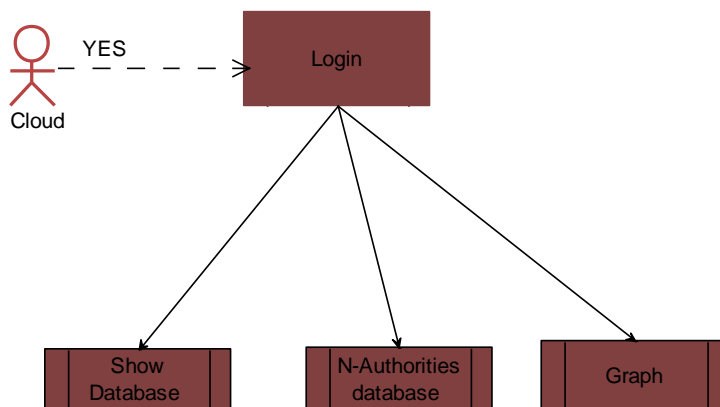


Figure 10. Yes Flow

Sequence diagram. Figure 11 details the sequence in which each operation is executed by a cloud admin after he is authenticated for log in into the application.

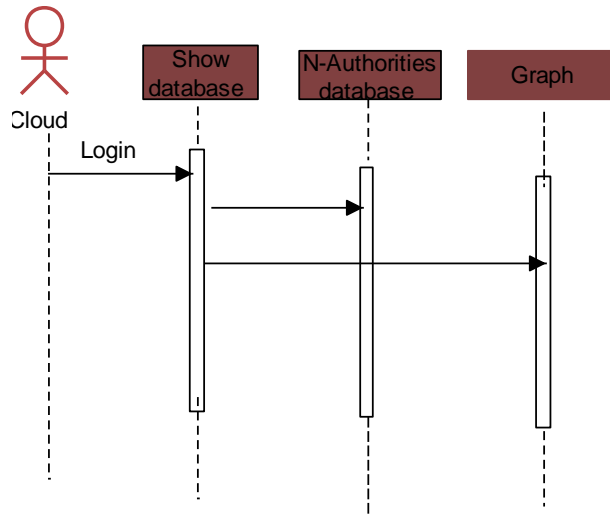


Figure 11. Authentication Flow

Activity diagram. Figure 12 illustrates all the actions that a cloud admin can do after getting authenticated into the application. From the activity start (login) and then check the database and the graph spikes till the end process.

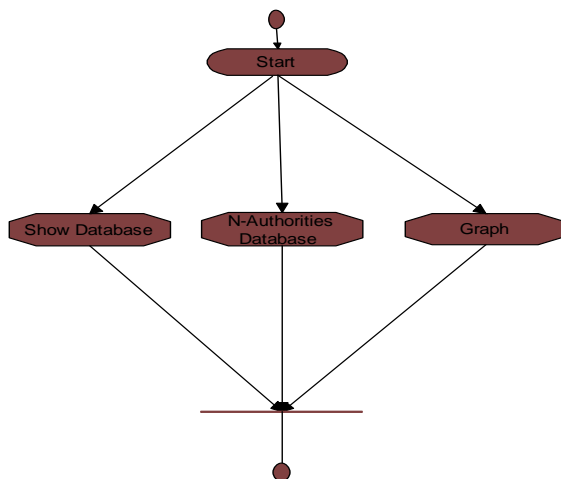


Figure 12. Login Flow

Summary

This chapter helps in understanding the various phases of operations that a Data Owner, Data Consumer and Cloud Admin can perform in the application, represented as part of the data flow diagrams. These diagrams are the base to develop the operations that are presented in the application. It is the base for the architectural design as it illustrates the various aspects of user operations. In the next coming chapter, the architecture, algorithm and the feasibility study done which are the critical factors for implementation.

Chapter VI: Feasibility Study and Implementation

Introduction

This chapter gives a brief explanation of the architectural design, feasibility study, algorithm and the technical implementation. In the Chapter II Methodology, the various use cases and data flow diagrams help in understanding the operational aspects of the application and give a clear understanding of how the operations built in the application.

Feasibility Study

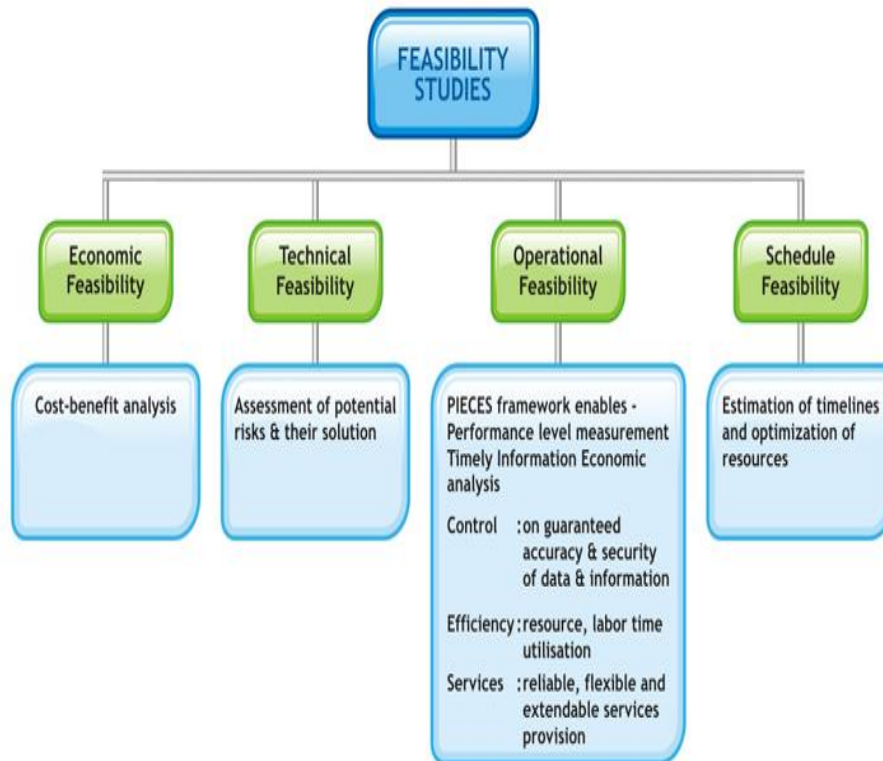


Figure 13. Feasibility Study

Economic feasibility. The reason for the monetary achievability appraisal is to focus the definite financial advantages to the association that the proposed framework will give. It

incorporates evaluation and ID of every one of advantages anticipated. This assessment regularly includes a cost/ advantages investigation.

Technical feasibility. The Technical Feasibility evaluation centered on picking up comprehension of the present specialized assets of the association and their relevance to the reasonable needs of the proposed framework. It is an assessment of the equipment and programming and how it addresses the issue of the draft framework.

Operational feasibility. Operational feasibility is a valuation of how well a proposed framework tackles the problems and exploits the opportunities distinguished amid degree definition and how it fulfills the prerequisites recognized in the necessities examination period of framework improvement. The operational unattainability evaluation concentrates on the extent to which the proposed improvement ventures fit in with the current business environment and destinations advancement plan, conveyance date, corporate culture, and existing business forms.

To guarantee achievement, sought operational results granted amid outline and advancement. These incorporate such outline subordinate parameters, such as dependability, viability, supportability, convenience, productivity, abundance, manageability, moderates, and others. These parameters obliged are considered in the early phases of configuration if fancied operational practices are figured out. A framework setup and advancement requires proper and opportune utilization of designing and administration endeavors to meet the already said parameters. A framework may fill its proposed need most adequately when its specific and working qualities are built into the outline. Subsequently, operational plausibility is an essential part of frameworks building that needs to be a necessary piece of the early plan stages.

Schedule feasibility. A task will fizzle on the chance that it takes too long finished before it is helpful. Usually, this implies evaluating to what extent the framework will seek to create, and if it is completed in each period utilizing a few systems like payback period. Plan achievability is a measure of how reasonable the task timetable is. Given our specific ability, are the due task dates sensible? A few ventures are launched with due dates. It is essential to figure out if the due dates are obligatory or attractive.

Architecture Diagram and Main Modules

Usage was the stage of the undertaking when the possible configuration transformed out into a working framework. Accordingly, it is the most basic stage in accomplishing a fruitful new structure and in giving the client, the certainty that the new framework will work and be compelling. The execution stage includes proper arranging, examination of the current framework and its limitations on usage, planning of techniques to accomplish changeover and assessment of change over strategies.

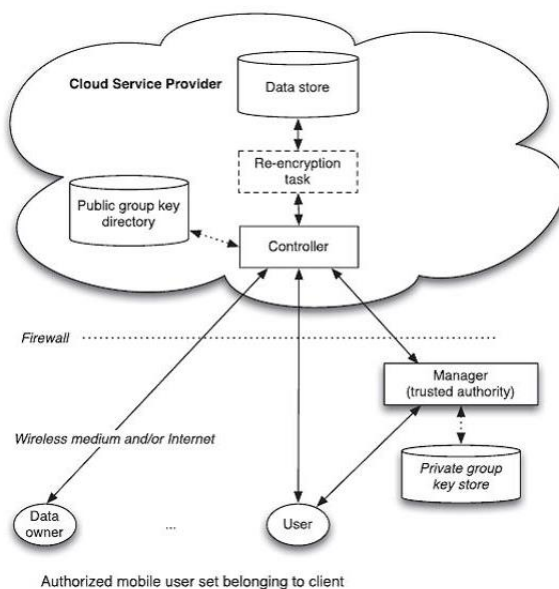


Figure 14. System Architecture

Registration-based social authentication module. The framework gets ready trustees for a client Alice at this stage. Alice originally confirmed with her key authenticator (i.e., password), and then a few (e.g., 5) companions, who additionally have accounts in the framework, chosen by either Alice herself or the administration supplier from Alice's companion list and are designated as Alice's Registration.

Security module. Validation is vital for securing records and keeping caricature messages from harming online notoriety. Envision a phishing email being sent from Gmail since somebody had produced data. Irate beneficiaries and spam grumblings coming about because of it turn into chaos to tidy up, with a specific end goal to repair notoriety. Trustee-Based social confirmation frameworks request that clients select their trustees with no requirement. In our investigations (i.e., Section VII), demonstration of administration supplier can oblige trustee determinations using forcing that no clients chose as trustees by an excess of different customers, which can accomplish better security ensures.

Attribute-based encryption module. The property-based encryption module is utilizing for every hub scramble information store. After encoded information and again the re-scrambled the same information is employing for a fine-grain idea using client information transferred. The trait based encryption proposed to secure the distributed storage. Characteristic Based Encryption (ABE). In such encryption plot, a person is an arrangement of stable traits, and decoding is understandable if a decrypter's character has a few covers with the one determined in the ciphertext.

Multi-authority module. A multi-power framework displayed in which every client has an id, and they can associate with every key generator (power) utilizing several nom de plumes.

To probably accomplish a multi-power CP-ABE which achieves the security characterized above; insurances the privacy of Data Consumers' personality data; and ensures bargain assaults on the powers or the conspiracy assaults by the forces. It is the first execution of a multi-power quality based encryption plan.

Algorithm

Anony control and anony control-f. In this system, there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers (refer Figure 14) (Li et al., 2010). Authorities have powerful computation abilities because some attributes partially contain users' personally identifiable information. Multiple N disjoint sets combined to form a complete authority and each N disjoint set are controlled by each authority. Therefore, each authority is aware of only part of attributes. A Data Owner outsources encrypted data file to the Cloud Servers. The Cloud Server has adequate storage capacity, does nothing but store them. New Data Consumers request private keys from all the authorities and are unaware of which attributes are controlled by which authorities. When Data Consumers request their private keys from the authorities, authorities create a composite private key and send it to the consumer. All Data Consumers can download any of the encrypted data files if their private keys satisfy the privilege tree T_p and can execute the operation associated with privilege p . The server executes an operation p if and only if the user's credentials are authenticated via the privilege tree T_p .

Partial information disclosed in AnonyControl and no information disclosed in AnonyControl-F. To formally define the security of our AnonyControl, first, give the following definitions should be known.

Setup \rightarrow AK, HKk : This algorithm input is just the security parameters. Attributes based authorities execute this algorithm to compute a system-wide public parameter AK as well as an authority full public parameter ok, and to compute a master key HKk individually.

key generated (AK, HKk, Au) \rightarrow SKU: This algorithm enables a user to interact with every attribute authority, and obtains a private key SKU corresponding to the input attribute set Au.

Encrypt (AK, M, $\{Tp\}_{p \in \{0, \dots, r-1\}}$) \rightarrow (CT, VR): This algorithm takes as input the public key AK, a message M, and a set of privilege trees $\{Tp\}_{p \in \{0, \dots, r-1\}}$, Where r is determined by the encrypted. It will encrypt the message M and returns a ciphertext CT and verification set VR so that a user can execute a specific operation on the ciphertext if and only if his attributes satisfy the corresponding privilege tree Tp. As defined, T0 stands for the privilege to read the file.

Decrypt (AK, SKU, CT) \rightarrow M or verification parameter: This algorithm will be used at file controlling (e.g., reading, modification, deletion). It takes as input the public key AK, a ciphertext CT, and a private key SKU, which has a set of attributes Au and corresponds to its holder's GIDu. If the set Au satisfies any tree in the set $\{Tp\}_{p \in \{0, \dots, r-1\}}$, the algorithm returns a message M or a verification parameter. If the verification parameter is successfully verified by Cloud Servers, who use VR to verify it, the operation request will be processed.

Step 1: The application not only provides data content privacy but also includes identity privacy by using AnonyControl. AnonyControl decentralizes the central authority to hide

the identity of origin and semi-anonymity is achieved with this. Subsequently, the AnonyControl-F, which entirely hides the identity helps in attaining full anonymity.

Step 2: System uses Attribute Encryption Standard (AES) algorithm. The algorithm is used to protect classified information and is used by the entire world to encrypt and decrypt sensitive data. AES consists of three block ciphers. AES-128, AES-192, AES-256 and this each cipher uses 128 bits of blocks using cryptographic keys 128,192 and 256 bits to encrypt and decrypt delicate data. The ciphers installed in this algorithm uses the same secret key for encrypting and decrypting. The different rounds of keys that is executed. Each series consists of steps that include substitution, transposition, and mixing of plain text. Then the plain text is transformed into ciphertext.

Step 3: There are four types of systems: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and Data Consumer in one session. Data owner encrypts and uploads the files to the cloud server. Data consumer decrypts and downloads the files from the cloud server.

Step 4: To perform any operations on files and to have unlimited access to such records, the data owner and data consumer should first register in the application. When they registered at a time password, and unique id will send to their registered mail id.

Step 5: To upload and download files by the user. The user data owner/data consumer requests authority for permission. The authority provides public key to data owner and private key to the consumer. Issuing keys to authority and authentication in our system is succeeding using attribute-based encryption.

Step 6: Attribute-based encryption is a type of public-key encryption in which the secret user key and the ciphertext are dependent upon (e.g., the country he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is conceivable only if the set of attributes of the user key matches the attributes of the ciphertext. A critical security aspect of Attribute-Based Encryption is collusion-resistance. An adversary that holds multiple keys should be able to access data if at least one individual key grants access.

Step 7: The keys provided by the authority to the users (data owner and data consumer) can be used to perform operations and to have access to files in and out from the cloud server.

Summary

The above chapter detailed the feasibility study of the application and measured on the different feasibility study methods. The section also includes the algorithm used for implementation and the steps that are followed by different users of the application like the Data Owner, Data Consumer and Cloud Admin. The next chapter details the pages built into the app and the operations done by the user that logs in to the application.

Chapter VII: System Configurations

Software Requirements

Operating System	Windows
Technology	Java and J2EE
Web Technologies	Html, JavaScript, CSS
IDE	My Eclipse
Web Server	Tomcat
Database	My SQL
Java Version	J2SDK1.5

Hardware Requirements

Hardware	Pentium
Speed	1.1 GHz
RAM	1GB
Hard Disk	20 GB
Floppy Drive	1.44 MB
Key Board	Standard Windows Keyboard
Mouse	Two or Three Button Mouse
Monitor	SVGA

Chapter VIII: Pages Designed

Introduction

This chapter is to give an idea of the operations performed by the user in the applications and the various pages of the application that user traverses to perform operations. Depending on the user intent in the application depending on his privileges of activities.

Home Page

The initial landing page is the home page where the different tabs are displayed and are to be select based on the user privileges available for operation in the application. Depending on his role and intent he is posed with three options: Admin, Private Cloud, and Client.

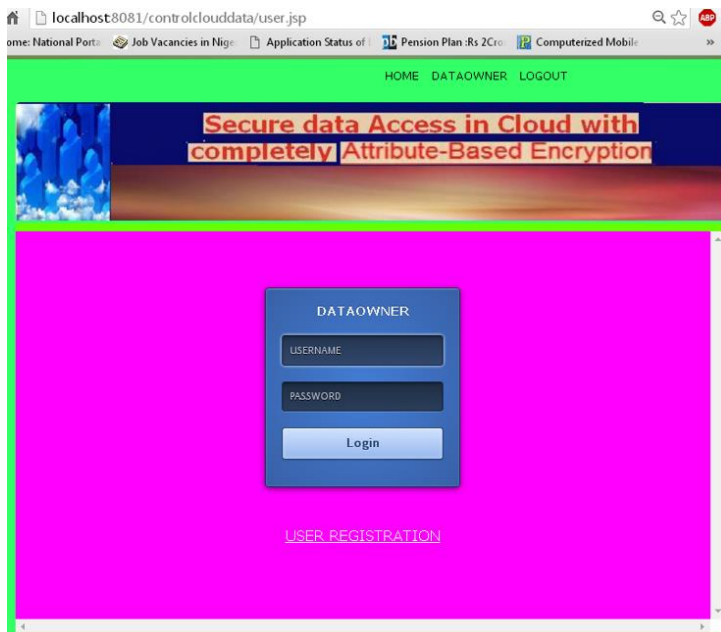


Figure 15. Home Page

Registration Page

For accessing the operations provided by the application first the user must register into the application. For this, he must fill in the required field of the registration page. Authentication

is essential for securing account and preventing spoofed messages from damaging online reputation.

Figure 16. Registration Page

Successful registration will shoot a popup as registered and then only the login ID and password are sent to user's email id after the cloud admin approves of his registration.

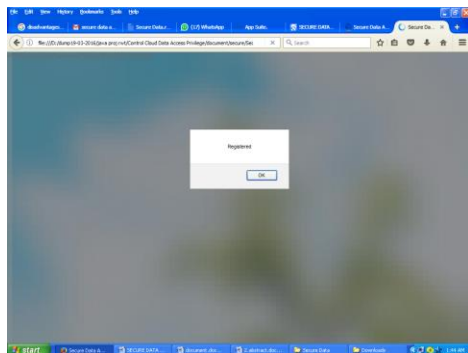


Figure 17. Success Full Registration

Login Page

After successfully registered, the password and unique id will be sent to the users registered mail ID. Using this id and password, they should log in. Depending on the role and the

privileged access provided by the application to the user ID, their different login pages in the application.

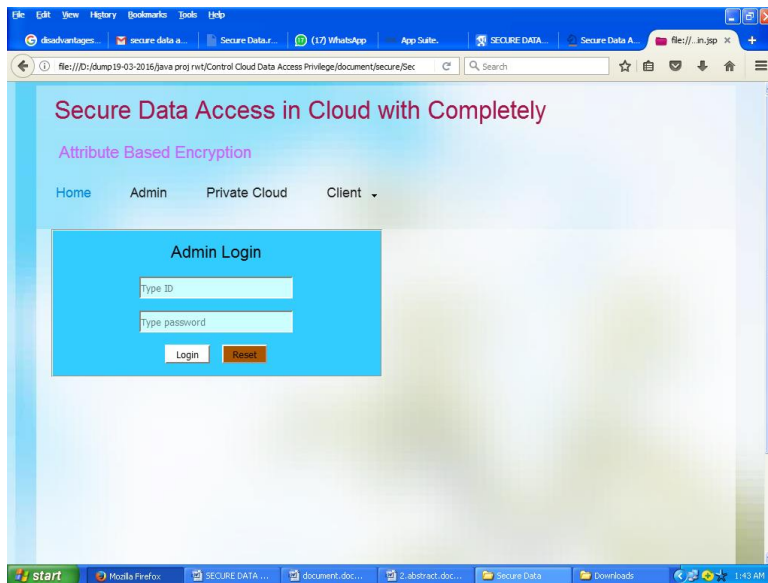


Figure 18. Admin Login

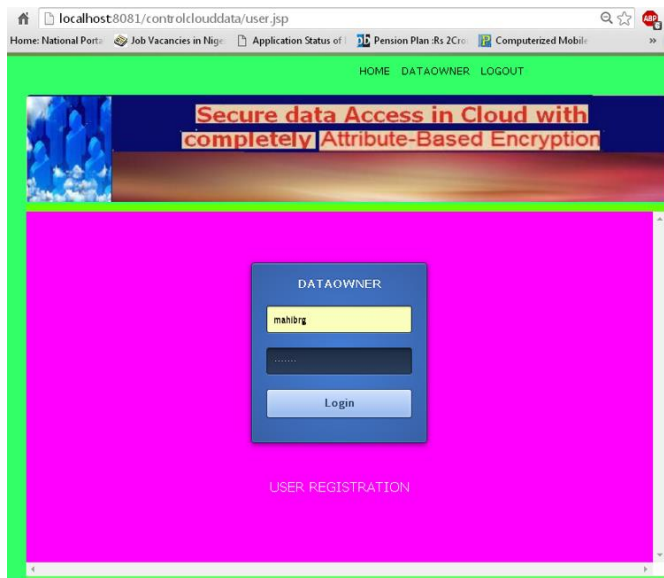


Figure 19. Private Cloud Login

localhost:8081/controlclouddata/details.jsp

Home: National Port Job Vacancies in Hig Application Status of Pension Plan :Rs 2Cro Computerized Mobil

CHANGE PASSWORD REQUEST OUTSOURCE LOGOUT

Secure data Access in Cloud with completely Attribute-Based Encryption

OWNER DETAILS

FIRSTNAME: mahib

LASTNAME: babu

EMAILID: burugupallibabuster@

MOBILE NO: 9949823490

GENDER: Male

Figure 20. Data Owner Login

Request Data Ownership

After successful login to the application, data owners can view the availability of the files uploaded by the data owner and request for authentication to operate on files like download.

Unique ID	Email	Owner Key	Status	Action
3394#	gouthami222@gmail.com	Waiting	Waiting	Request

Figure 21. Request Data Ownership

Providing Ownership

The application algorithm, after success full data consumer authentication, N-Authorities algorithm is then invoked to provide a public key, authority key for the owner and private key,

authority key for the consumer to perform operations on files. The cloud admin can only invoke this method.



The screenshot shows a web application with a navigation bar containing 'Home', 'Response', and 'Logout'. Below the navigation bar is a table with the following data:

Owner ID	Owner Key	N-Authority Key	Status	Action
1ecgch	Waiting	Waiting	Waiting	Response
3394ff	Pending	Pending	Pending	Response

Figure 22. Providing Ownership

Data Owner Operations

After successful authentication, the access privileges provided to the data owned by the Cloud Admin, the data owner using the public key the data owner performs encryption and uploads files to the cloud server.



The screenshot shows a web application with a navigation bar containing 'Home', 'Change Password', 'Request', 'File Upload', 'File Details', and 'Logout'. Below the navigation bar is a table with the following data:

Unique ID	Email	Owner Key	Status	Action
3394ff	gouthami222@gmail.com	4efg26	Granted	Request

Figure 23. Data Owner Operations

Data Owner Uploads File

After having access to all the operation in the application, the data owner now uploads files to the application, and during the upload, all the encryption methods are invoked, and the resulted encrypted data is then uploaded in the cloud database.

localhost:8081/controlclouddata/fileupload.jsp

Home: National Port | Job Vacancies in Nige | Application Status of | Pension Plan -Rs 2Cro | Computerized Mobil

OWNERDETAIL OUTSOURCE OWNERDBAS LOGOUT

Secure data Access in Cloud with completely Attribute-Based Encryption

OUTSOURCE DATA UPLOAD

FILEID: 810

FILENAME: admin

USERDATA: Choose File | admin.jsp

N-KEY: XU0op3=ae&F

UPLOAD

Figure 24. File Upload

On selecting the choose file option, the user can browse files on his system and upload it to the cloud DB. After he selects the file, there is another popup triggered wherein the user must enter the file id and file name.

localhost:8081/controlclouddata/viewencrypt2.jsp

Home: National Port | Job Vacancies in Nige | Application Status of | Pension Plan -Rs 2Cro | Computerized Mobil

OWNERDETAILS OUTSOURCE OWNERDBAS LOGOUT

Secure data Access in Cloud with completely Attribute-Based Encryption

VIEW OWNERDATABASE

FILE ID	FILE NAME	USERDATA	KEY	AGAIN ENCRYPT DATA
810	JS84yDEOKU3	7C???? ???e_70?>d ?? D???	(7s94.00r-7 cyECSA6 u(Ji, A	Start Again

Figure 25. File Details

In the above screenshot apart from file upload, the data owner can also perform a different operation like changing his account password. If he chooses to change password, then he is redirected to change password page where he must enter the old password and give the new password and a session authenticated id is sent to his registered email id which he must register to change the password successfully.

Data Consumer

After the data owner has performed the above operations and makes data available for the data consumer in the cloud, now the data consumer after following the same process as Data Owner like registering into the application, getting authenticated login credentials, he can then use the data in the application. Using private key, the data consumer performs decryption and downloads files from the cloud server. Figure 26 details the different kinds of files that the data consumer can access in the cloud made available by various data owners.



FILE ID	OWNERKEY	N_KEY	STATUS	RESPONSE
32	UoD6?EAYeA6? U/A7	?N& O& 4Z.6eP? C	approved	Response
33	-Qv?F&M? Ou2pA,	?7? 0g6G?? AgB	approved	Response
34	null	?M?y?IC %??	approved	Response
35	T?6O_?p zs:Ej??	?a&cl?n[s? aF5	approved	Response
36	?7&?-?Xl? %a_u'n	?u?4?+?ab?6e? e	approved	Response
37	null	?U1- A&UMO? br?k?-?y?BUA %s]	null	Response
38	XJOp5-?aF		PublicKey Requested	Response

Figure 26. Data Consumer Accessing Data from Cloud

Attribute Authority Login

The authority login keeps a time track of all the requests that are being made in the application of requests from data owners and data consumers. Then with the response, both data owner and data consumers are emailed based on the acceptance criteria of the data owners as for whom they want to provide access to their data made available via application.

The attribute-based encryption module is using for each node encrypt data store. After encrypted data and again the re-encrypted the same data is using the fine-grain concept using user data uploaded. In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext. A multi-authority system is presented in which each user has an id, and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above guarantees the confidentiality of Data Consumers' identity information.

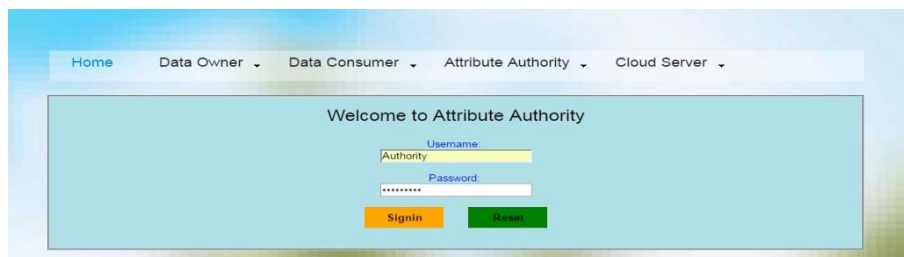


Figure 27. Attribute Authority Login

Figure 28 details the view of all the data made available in an application with an action tab available for responding the requests.

OWNER DETAILS FILEUPLOAD LOGOUT

Secure data Access in Cloud with completely Attribute-Based Encryption

ENCRYPTED DATA CONVERT TO BINARY DATA

FILEID:

FILENAME:

USERDATA:

ENCRYPT KEY:

Figure 28. Data Available in Application

Cloud Server Login

At the cloud server, all the data is in encrypted form the cloud server is unable to see the details and data. This provides not only data privacy but also user identity privacy by anonymity with entirely anonymous attribute-based encryption.

Home Data Owner Data Consumer Attribute Authority Cloud Server

Welcome to Cloud Server

Username:

Password:

Figure 29. Cloud Server Login

After successful login to the cloud database, different files can be viewed by the cloud admin with details such as the file id, file name, file size, file owner, and upload date.



File ID	File Name	File Size	File Owner	Upload Date
null	rSU5yyPhcZi49JEXW4a8ng==	1pUX2lqQk6o=	1x+8vcq3v1w=	null
null	rSU5yyPhcZi49JEXW4a8ng==	Bs2ZqYCnKlw=	1x+8vcq3v1w=	null
9018	rSU5yyPhcZi49JEXW4a8ng==	AZ1/TiHdUg=	tVvYZVOWUpYEEJqTxBWXlbeSMmd4vu0	!ajvK8sZfoembF874ssgBg=
null	rSU5yyPhcZi49JEXW4a8ng==	ZbcjrQswwJw=	1x+8vcq3v1w=	null

Figure 30. View File Details

Summary

This chapter details all the operations that the different users of cloud can perform in the application. All the privileges that are assigned to a user role are detailed. The various pages and the flow activity is detailed in this chapter. The next chapter describes the different methods used for testing the application.

Chapter IX: System Testing

Introduction

The motive of system testing is to find out errors. Testing is the procedure of seeking to find out every manageable fault or weak point in a work product. It offers a way to test the capability of components, sub-assemblies, assemblies and a completed product. It's far the technique of exercising software with the motive of ensuring that the software system meets its necessities and user expectations and does not fail in an unacceptable way. There are many varieties of the test. Each test type addresses a particular testing need.

Types of Tests

Unit testing. Unit testing involves the layout of test cases that check the internal program logic is operating well, and that program inputs produce reasonable outputs. All decision branches and inner code flow have demonstrated. It is the testing of personal software units of the application is accomplished after the final touch of an individual unit before integration. This is a structural testing that based on information of its production and is invasive. Unit tests carry out fundamental tests at the component stage and test a particular business technique, application, and system configuration. Unit tests make sure that every specific direction of a business process performs appropriately to the documented specs and includes described inputs and predicted outcomes.

Integration testing. Integration tests designed to test integrated software components to find if they run as one program. Testing is event-driven and is more concerned with the primary outcome of screens or fields. Integration tests show that although the components were individually satisfaction, as demonstrated by successfully unit testing, elements are correct and

consistent. Integration testing is specifically for exposing the problems that arise from the combination of elements.

Functional testing. Functional tests give systematic demonstrations that function tested be available as specified by the business and technical requirements, system documentation, and user manuals. Functional testing centered on the following items:

- Valid Input: Identified classes of valid inputs accepted.
- Invalid Input: Identified categories of invalid input rejected.
- Functions: Identified functions exercised.
- Output: Identified classes of application outputs exercised.
- Systems/Procedures: Interfacing systems or ways invoked.

Business enterprise and preparation of functional tests targeted on necessities, key capabilities, or unique test instances. Also, systematic coverage about identifies enterprise procedure flows; data fields, predefined strategies, and successive techniques ought to be taken into consideration for testing. Before functional testing is entire, extra tests described, and the useful value of current tests decided.

System testing. System testing guarantees that whole integrated software system meets necessities. It tests a configuration to make sure recognized and predictable outcomes. An example of system testing is the configuration oriented system integration test. System testing based on technique descriptions and flows, emphasizing pre-driven procedure links and integration factors.

White box testing. White box testing is a testing wherein the software tester has the know-how of the internal workings, structure, and language of the software, or at least its purpose. It is the goal. It is to test areas that cannot be reached from a black box stage.

Black box testing. Black box testing is testing the software without any earlier ability of the internal workings, structure or language of the module being tested. Black box tests, like most different forms of tests, have written from a definitive source document, such as specification or requirements record, including specification or necessities document. It is a testing wherein the software under test is dealt with, as a black box. Cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

Unit testing. Unit testing is usually conducted as part of a joint code and unit test phase of the software life-cycle, although it is not uncommon for coding and unit testing conducted as two distinct phases.

Test Strategy and Approach

Field testing will be performed manually, and functional tests will be written in detail.

Test Objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages, and responses must not be delayed.

Features to be Tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

Integration Testing

Software integration testing is the incremental integration testing of two or more conjoined software components on a single platform to produce faults caused by interface defects. The task of the integration test is to check that components or software applications, e.g., elements in a software system or—one step up—software applications at the company level—interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing

User Acceptance Testing is a critical stage of an ongoing project and requires significant participation by the end-user. It also ensures that the system has in place all the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects met.

Summary

The chapter on testing is to highlight the test cases methods ran to check the sanity, performance of the application. These tests help to find the successful implementation of the project.

Chapter X: Results, Conclusion, and Future Work

Introduction

As part of this chapter, a brief overview of the result of the application built is detailed. The conclusions and recommendations are also added to give a clear understanding of final result and the answers to the questions for which the project implemented.

Results

The following paramters are used to illustrate how privacy and controlled access of Data in Cloud is achieved, also addressing how the integrity and privacy of the User is achieved in the project.

- **Public Key:** The module generates a public key for authentication for the user to offer the user specification logging.
- **File Storage:** The File Storage module holds the file stored for usage by the data consumer and the files can be viewed and downloaded based on periodic time keys.
Encryption: Files encrypted to give content security.
- **Data Access Control:** The Data Access control enables limited access to the cloud for the performance and usage of the cloud by the user.
- **Data Access:** The Data accessed by viewing the content of the file or downloaded for the further usage. Attribute-based encryption is using data uploaded. Every node od data stored is encrypted data. Fine-Grain concept using encrypted data convert into binary value fully secure for the database.

Conclusion

This paper presents a semi-mysterious property based benefit control plot AnonyControl, and an entirely anonymous characteristic based benefit control conspires AnonyControl-F address the client protection issue in a computing storage server. By utilizing the many experts in the computing system, our proposed plans do not just fine-grained benefit control additionally character obscurity while controlling benefit control given clients' character data. More vitally, our system can acknowledge up to N-22 expert bargain, which is exceedingly ideal particularly in Internet-based computing condition. Likewise, immediate point-by-point security and execution investigation which demonstrates that AnonyControl both proficient and secure for cloud capacity system. One of the up and coming future works is to present the proficient client denial instrument on top of our mysterious ABE. Supporting client renouncement is an essential issue in the original application, and this is an impressive test the application of ABE plans (Yu et al., 2010). Making our plans versatile with existing ABE plans bolster proficient client denial is one of our future works.

Future Work

The proposed system is efficient in identity-based user revocation in multi-authority CP-ABE. In the future, work continued in several directions. First is great comparisons needed between revocation schemes proposed for attribute-based encryption to understand better and improve the performance in various circumstances. The secure way of forwarding the revocation related computations to the CSP (or even to the user), allows immediate banning of a user, reverting decryption of all previously (and later) encrypted ciphertexts. Steps in this direction, without assuming trusted CSP, would be useful. The method of identity-based user revocation

will form a base that enables non-monotonic access structures in the multi-authority setting. The proposed scheme cannot be applied directly for this purpose; it may be used to develop ideas in this field. Security of this application is proved in the generic bilinear group model, another possible way to achieve full security is by adapting the dual system encryption methodology, which was also used by Lewko and Waters (2009) in their composite order group construction. This type of work would be impressive even if it resulted in a moderate loss of efficiency from our existing system.

References

- Bethencourt, J., Sahai, A., & Waters, B. (2013). Ciphertext-policy attribute based encryption. *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321-334.
- Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk. In *Proceedings of the 2001 Workshop on New Security Paradigms*, Cloudcroft. New Mexico.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Buyya, R., Yeo, C. S., Venugopal, S., Brogerg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the fifth utility. *Future Generation Computer Systems*, 25, 5999-616.
- Chase, M. (2013). Multi-authority attribute based encryption. In S. Vadhan (Ed.), *Theory of Cryptography* (pp. 515-534). Berlin, Germany: Springer Vahlag.
- Chase, M., & Chow, S. (2009). Improving privacy and security in multi-authority attribute based encryption (pp. 121-130). In *Proceedings on Conference on Computer and Communications Security*.
- Infosecurity. (2010). *Google, Microsoft seek new approaches to security disclosure*. Retrieved from <https://www.infosecurity-magazine.com/news/google-microsoft-seek-new-approaches-to-security/>
- Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2), 125-143.

- Jung, T., Li, X-Y, Wan, Z., & Wan, M. (2015). *Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption*. Berlin, Germany: Springer-Verlag.
- Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers and Security*, 24(2), 147-159.
- Lewko, A., & Waters, B. (2009). *New techniques for dual system encryption and fully secure HIBE with short ciphertexts*. Retrieved from <https://eprint.iacr.org/2009/482.pdf>
- Li, M., Schucheng, Y., Ren, K., & Lou W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. *International Conference on Security and Privacy in Communication Systems*. Heidelberg, Germany: Springer Publications.
- Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *International Conference on Security and Privacy in Communication Systems* (pp. 89-106). Berlin, Germany: Springer Verlag.
- Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, 24(1), 131-143.
- Mishra, D. P., Mishra, R., & Tripathy, A. (2011). A privacy preserving repository for securing data across the cloud. In *Proceedings of the third International Conference on Electronic Computer Technology* (pp. 6-10).

- Park, N. (2011). Secure data access control scheme using type-based re-encryption in a cloud environment. In R. Katarzyniak, T-F Chiu, C-F Hong, & N-T Nguyen (Eds.) *Semantic methods for knowledge management and communication* (pp. 319-327). Heidelberg, Germany: Springer Verlag.
- Rees, J., Bandyopadhyay, S. & Spafford, E. H. (2003). PFIREs: A policy framework for information security. *Communications of the ACM*, 46(7), 101-106.
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems*. Gaithersburg, MD: National Institute of Standards and Technology.
- Vormetric. (2011). *Vormetric data security for Amazon web services extends leading encryption solution to the cloud*. Retrieved from <https://www.thalesecurity.com/about-us/newsroom/news-releases/vormetric-data-security-amazon-web-services-extends-leading>
- Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W. (2009). Enabling public verifiability and data dynamics for storage security in cloud computing. In M. Backes & P. Ning (Eds.), *Computer Security – ESORICS 2009* (pp. 355-370). Berlin, Heidelberg: Springer Verlag.
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security* (4th ed.). Boston, MA: Cengage Publications.
- Yang, K., & Ziaohua, J. (2014). DAC-MACS: Effective data access control for multi-authority cloud storage systems. *Security for Cloud Storage Systems*, 59-83. New York, NY: Springer Publications.

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *Proceedings of the 29th IEEE International Conference on Computer Communications* (pp. 534-542).

Appendix

Code:

```
<!DOCTYPE HTML>
<html>
<head>
<title>Secure Data Access</title>
<meta name="description" content="website description" />
<meta name="keywords" content="website keywords, website keywords" />
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<link rel="shortcut icon" type="image/x-icon" href="images/brainstorming_alternative.png"/>
<link rel="stylesheet" type="text/css" href="css/style.css" />
<!-- modernizr enables HTML5 elements and feature detects -->
<script type="text/javascript" src="js/modernizr-1.5.min.js"></script>
</head>
<body>
<div id="main">
<header>
<div id="logo">
<div id="logo_text">
<!-- class="logo_colour", allows to change the colour of the text -->
<pre> <h1><a href="index.html">Secure Data Access in Cloud with Completely </a></h1>
<h2 style="font-size: 22px"> Attribute Based Encryption</h2></pre>
</div>
</div>
<nav>
<ul class="sf-menu" id="nav">
<li class="selected"><a href="index.html">Home</a></li>
<li><a href="admin.jsp">Admin</a></li>
<li><a href="p_cloud.jsp">Private Cloud</a></li>

<li><a href="#">Client</a>
<ul>
<li><a href="user.jsp">Signin</a></li>
<li><a href="register.jsp">Register</a></li>

</ul>
</li>
</ul>
```

```

</nav>
</header>
<div id="site_content">
<div id="sidebar_container">
<div class="gallery">
<ul class="images">
<li class="show">
<!--img width="450" height="450" src="images/c1.jpg" alt="photo_one" /></li>
<li></li-->
<li></li>
<!--li></li>
<li></li-->
</ul>
</div>
</div>
<div id="content">


</div>
</div>
<footer>
</footer>
</div>
<p>&nbsp;</p>
<!-- javascript at the bottom for fast page loading -->
<script type="text/javascript" src="js/jquery.js"></script>
<script type="text/javascript" src="js/jquery.easing-sooper.js"></script>
<script type="text/javascript" src="js/jquery.sooperfish.js"></script>
<script type="text/javascript" src="js/image_fade.js"></script>
<script type="text/javascript">
$(document).ready(function() {
$('ul.sf-menu').sooperfish();
});
</script>
</body>
</html>

```

Cloud Code:

```

<!DOCTYPE HTML>
<html>
<head>
<title></title>
<meta name="description" content="website description" />
<meta name="keywords" content="website keywords, website keywords" />
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<link rel="shortcut icon" type="image/x-icon" href="images/brainstorming_alternative.png"/>
<link rel="stylesheet" type="text/css" href="css/style.css" />
<!-- modernizr enables HTML5 elements and feature detects -->
<script type="text/javascript" src="js/modernizr-1.5.min.js"></script>
<style>
#id{
width: 200px;
height: 25px;
background-color: #D3F2F7;
}
#but{
width: 60px;
height: 25px;
}
</style>
<script>
function validation(){
var uname=document.ulongin.username.value;
var pass=document.ulongin.password.value;

if(uname==0){
alert("Enter ID");
document.ulongin.username.focus();
return false;
}
if(pass==0){
alert("Enter password");
document.ulongin.password.focus();
return false;
}
}

```

```

}
</script>
</head>

<body>
<div id="main">
<header>
<div id="logo">
<div id="logo_text">
<!-- class="logo_colour", allows to change the colour of the text -->
<pre> <h1><a href="index.html">Secure Data Access in Cloud with Completely </a></h1>
<h2 style="font-size: 22px"> Attribute Based Encryption</h2></pre>
</div>
</div>
<nav>
<ul class="sf-menu" id="nav">
<li class="selected"><a href="index.html">Home</a></li>
<li><a href="admin.jsp">Admin</a></li>
<li><a href="p_cloud.jsp">Private Cloud</a></li>

<li><a href="#">Client</a>
<ul>
<li><a href="user.jsp">Signin</a></li>
<li><a href="register.jsp">Register</a></li>

</ul>
</li>
</ul>
</nav>
</header>
<div id="site_content">
<div id="sidebar_container">
<div class="gallery">
<ul class="images">
<li class="show"></li>
</ul>
</div>
</div>
<div id="content">

```

