IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Security For Cloud Computing Using V-Grt Methodology

Deepika A J[1], Dr.Savitha C K [2], Dr.Ujwal U J.[3], Dr.Smitha M L[4]

[1]Mtech, Computer Science Engineering ,KVGCE, Sullia D.K, Karnataka, India

[2] M.tech,Ph.D,CSE .Dept,KVGCE,Sullia,D.K,Karnataka,India

[3] M.tech,Ph.D,CSE .Dept,KVGCE,Sullia,D.K,Karnataka,India

[4]M.tech,CSE .Dept,KVGCE,Sullia,D.K,Karnataka,India

Abstract:

Distributed computing is turning into the design of another age of IT Undertaking. Not at all like customary arrangements, Distributed computing moves application programming and data sets to huge server farms, where information and administration the board may not be completely trusted. In any case, this extraordinary component presents numerous new security gives that poor person been surely known. In distributed computing, neither the information nor the product is completely contained on the client's PC; Information security concerns emerge in light of the fact that both client information and the program are situated on the supplier's premises. Mists normally have a solitary security design, however have numerous clients with various necessities. Each cloud supplier takes care of this issue by scrambling information utilizing encryption calculations. In any case, there is likewise an opportunity that the cloud administration isn't trusted to conquer this issue. This web application presents another model called the V-GRT approach that conquers the central issue of distributed computing information security. The creator introduced an information security model of distributed computing with a security seller, which kills the worry of information abuse by the cloud specialist co-op and subsequently increments information security.

Index Terms – IT Enterprise, Data security, Clouds ,V-GRT.

I. INTRODUCTION

What is distributed computing?

Distributed computing is the utilization of processing assets (equipment and programming) that are conveyed as a help over an organization (typically the Web). The name comes from the normal utilization of the cloud-molded image as a reflection for the perplexing framework it contains in framework charts. Distributed computing endows client information, programming and estimations to remote administrations. Distributed computing comprises of equipment and programming assets made accessible on the Web as outsider oversaw administrations. These administrations commonly give admittance to cutting edge programming applications and very good quality server PC organizations.

How Distributed computing Functions?

1. Cloud registering expects to utilize conventional supercomputers, or elite execution processing power usually utilized by military and examination offices, to perform several trillions of estimations each second in customer situated applications, for example, monetary portfolios to give customized data. to give information capacity or to control enormous, vivid PC games.

2. Cloud figuring utilizes organizations of enormous gatherings of servers, ordinarily running minimal expense customer PC innovation with devoted associations, to disseminate information handling work among them. This common IT framework contains huge gatherings of frameworks that are interconnected. Virtualization procedures are frequently used to amplify distributed computing execution.

Qualities and Administrations Models: The remarkable attributes of distributed computing in light of definitions given by the Public Establishment of Norms and Wording (NIST) are recorded beneath:

a. On-Request Self-Administration: The client can singularly arrangement registering capabilities, for example, server time and organization stockpiling depending on the situation, naturally without requiring human cooperation with the supplier of each assistance.

b. Broad network access: Abilities are accessible over the organization and are gotten to through standard systems that help use by heterogeneous slender or thick client stages (eg, cell phones, workstations, and PDAs).

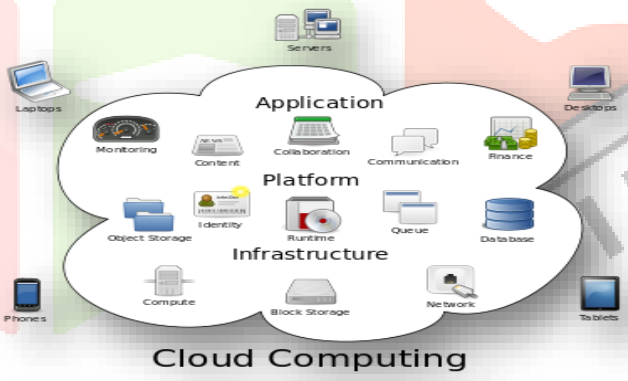


Fig1,. Structure of distributed computing

Administrations Models:

Distributed computing incorporates three different help models, specifically Framework as-a-Administration (IaaS), Stage as-a-Administration (PaaS), and Programming as-a-Administration (SaaS). These three assistance models or layer are supplemented toward the end-client layer, which embodies the end-client's perspective on cloud administrations. The model is displayed in the picture beneath. For instance, in the event that a cloud client gets to administrations at the framework layer, they can run their own applications on cloud foundation assets and stay liable for the help, upkeep, and security of those applications. In the

event that getting to the help at the application layer, these undertakings are normally taken care of by the cloud specialist co-op.

Advantages of distributed computing:

1. Accomplish economies of scale - increment creation volume or efficiency with less individuals. Your expense per unit, venture or item will dive.

2. Decrease spending on innovative framework. Keep up with simple admittance to your data with insignificant forthright expenses. Pay persistently (week after week, quarterly or every year) in light of interest.

3. Globalize your labor force economically. Individuals all around the world can get to the cloud given they have a web association.

4. Smoothing out processes. Accomplish more quicker than expected with less individuals.

5. Diminish capital expenses. There is compelling reason need to burn through huge load of cash on equipment, programming or permit charges.

6. Further develop openness. You approach whenever, anyplace, making your life a lot simpler!

II. Related Work

1) A fully homomorphic encryption scheme, 2009.
AUTHORS: C. Gentry
He proposed the first completely homomorphic encryption conspire, tackling an old open issue [1]. Such a plan makes it conceivable to register erratic capabilities over the encoded information without an unscrambling key - i.e., with the given codes E(m1), ..., E(mt) from m1, ..., mt, a reduced ciphertext can be proficiently figured. which encodes f(m1, ..., m t) for any successfully processable capability f.Fully homomorphic encryption has various applications. For instance, it empowers scrambled web search tool inquiries - the web search tool can offer you a short encoded response to your (legitimate) inquiry without understanding what your question was. It likewise permits looking through in encoded information; you can store scrambled information on a distant server and later have the server recover just records that (when unscrambled) meet some boolean requirement, regardless of whether the server can't decode the actual documents. It works on the proficiency of secure multiparty registering all the more comprehensively.
In our answer, the creator begins by proposing a to some degree homomorphic "boostrappable" encryption conspire that works when the capability f is the plan's own decoding capability. The creator then, at that point, shows how, through recursive self-inserting, bootstrapable encryption gives completely homomorphic encryption.

2) Hybrid Encryption for Cloud Database Security, 2010.

AUTHORS: A. Kaur and M. Bhardwaj

In the distributed computing climate, another information the executives model is utilized today that empowers information reconciliation and admittance to enormous scope distributed computing as a help called Data set as-a-administration (DAAS) [3]. Through which the specialist organization offers client the executives highlights as well as costly equipment. Information protection is a significant security determinant in DAAS, as information will be imparted to an outsider; an untrusted server is risky and hazardous for clients. This article shows interest in the security component in the cloud climate. It proposes a procedure to expand the security of a cloud data set. This procedure gives adaptable staggered and half and half security. It utilizes RSA, Triple DES and an irregular number generator as an encryption device.

3) Lightweight and secure database encryption using the tsfs algorithm, 2010.

AUTHORS: D. Manivannan and R. Sujarani

Introduced, data set security is of prime significance in modern, common and administrative fields [5]. Associations store immense measures of information in a data set for information mining and different sorts of examination. A portion of this information is viewed as delicate and should be shielded from exposure. Information base security moves are expanding because of the tremendous prevalence of online business. As of late, insider assaults definitely stand out enough to be noticed than normal malware flare-ups. Data set frameworks are normally sent somewhere inside an's organization, so insiders have the least demanding an open door to assault and think twice about and consequently take information. So information should likewise be shielded from inside aggressors. Numerous regular data set security frameworks are intended to guarantee data set security, yet delicate information in the data set is helpless against assault in light of the fact that the information is put away just in plain text. Information base encryption is the main answer for keep away from the gamble presented by this danger. This article centers around a security answer for safeguard information very still, explicitly safeguarding delicate information put away in data sets utilizing a three-key TSFS calculation, hence giving greater security to the data set. This calculation increments proficiency while questioning the information base by encoding just delicate information.

4) Using in-memory encrypted databases in the cloud, 2011.

AUTHORS: F. Pagano and D. Pagano

Introduced, information capacity in the cloud presents various protection issues. The method for taking care of them is to help information replication and dissemination in the cloud through nearby, halfway synchronized stockpiling [6]. The article makes sense of the utilization of an in-memory RDBMS with column level information encryption to allow and disavow access freedoms to dispersed information. This sort of arrangement is seldom utilized in traditional RDBMS in light of the fact that it requires a few complex advances. Commitment of the execution and benchmarking of the test framework, which shows that our straightforward yet viable arrangement beats most issues.

5) Commutative encryption scheme based on ElGamal encryption, 2012.

AUTHORS: K. Huang and R. Tso

The introduced commutative encryption is a sort of encryption framework that permits plaintext to be encoded at least a couple of times utilizing the public keys of various clients [7]. In this framework, decoding isn't expected before encryption/re-encryption processes. Moreover, the subsequent ciphertext can be decoded by assigned decryptors no matter what the request for the public keys utilized in the encryption/unscrambling processes. As such, the request for the keys utilized in encryption and decoding doesn't influence the consequence of the computation. The commutative encryption plot is valuable in some genuine applications like mystery sharing, data set mix, and so forth. Nonetheless, regardless of its value, scarcely any papers tell the best way to develop such a sort of commutative encryption. The paper makes sense of another commutative encryption plot in light of the ElGamel figure and gives a security confirmation in an irregular prophet model..

III. Problem Statement

a) Information privacy happens in light of the fact that clients have little to no faith in cloud suppliers and it is essentially unimaginable for distributed storage suppliers to wipe out potential insider danger, it is exceptionally perilous for clients to store their delicate information straightforwardly in distributed storage. Straightforward encryption deals with the issue of key administration and can't uphold complex prerequisites like inquiry, equal change, and fine-grained approval.

b) One of the fundamental weaknesses of the cloud is that the cloud specialist organization has such a large number of potential outcomes to abuse the information put away in its server farm by the client. Along these lines, a techniques that are proposed don't straightforwardly affect lessening this issue. Distributed computing issues will go on until the cloud specialist organization's information on the information is debilitated. Distributed computing strategies likewise over and again utilize the OTP strategy, which makes this framework wasteful

IV. .Proposed System

1) Username and secret key given by the client to the cloud specialist co-op. The secret phrase is encoded with a Crossover Encryption strategy, for example, RSA, Caeser figure, and alphabetic encryption.

2) The Cloud Specialist co-op (CSP) validates the client by checking the username and secret key by decoding and sends with the login key for the security seller.

3) The client space in the CSP and the memory address distributed to the client is given by the cloud specialist co-op to the security merchant.

4) Security merchant login key

5) Client validated by the key given by the cloud specialist co-op

6) Client chooses encryption strategy for different choices obscure to CSP and saves information

7) The security merchant sends the scrambled information to the cloud specialist co-op

BENEFIT OF PROPOSED SYSTEM

1.A safer Framework

2.The outcomes show a superior presentation rating contrasted with the current framework.

V. SYSTEM DESIGN

MODULES:

1. Cloud Service Provider
2. Data Users Module
3. Security Vendor's Module (Auditor)
4. RSA, Caeser Cipher, 3DES Algorithm

MODULES DESCRIPTION:

Cloud Service Provider

In this module we foster Cloud Specialist co-op module. This is a substance that gives an information stockpiling administration in the public cloud. S-CSP gives an information reevaluating administration and stores information for clients. To decrease capacity costs, S-CSP takes out repetitive information stockpiling through de_duplication and keeps just remarkable information.

The paper makes sense of that we expect that the S-CSP is consistently on the web and has enormous capacity limit and figuring power. Java code to send key to security seller and client utilizing Shishi. Gets encoded information sent by the provider. It can show the data set of all clients in an encoded design.

Data Users Module:

Plan the code for three encryption calculations in Java. Plan a front-end utilizing Java. A client is an element that needs to reevaluate the S-CSP information store and access the information later.In a capacity framework supporting deduplication, the client just transfers remarkable information, yet transfers no copy information to save transfer data transmission, which might be claimed by a similar client or different users.In an approved deduplication framework, every client is relegated a bunch of consents in the framework settings. Each record is safeguarded by a joined encryption key and approval keys to carry out approved deduplication with differential approvals.

Security Vendor's Module:

In this module, the security merchant chooses the encryption calculation to be utilized to store the information. Utilize the keys got from the cloud specialist organization to sign in. On the off chance that the confirmation is effective, the administrations can be utilized.

Triple DES, Caeser Cipher, RSA Algorithm:

The critical size of the first DES code of 56 pieces was by and large adequate when this calculation was planned, however the accessibility of expanding figuring power made animal power assaults conceivable. Triple DES gives a somewhat straightforward strategy for expanding the DES key size to safeguard against such goes after without planning a completely new block figure calculation.

In cryptography, the Caesar figure, otherwise called the Caesar figure, shift figure, Caesar code, or Caesar shift, is one of the least complex and most popular encryption strategies. It is a sort of replacement figure in which each letter in the plaintext is supplanted by a letter a specific fixed number of positions in the letter set. For instance, on the off chance that moved left by 3, D would be supplanted by A, E would become B, and so on. The technique is named after Julius Caesar, who involved it in his confidential correspondence.

SYSTEM ARCHITECTURE:

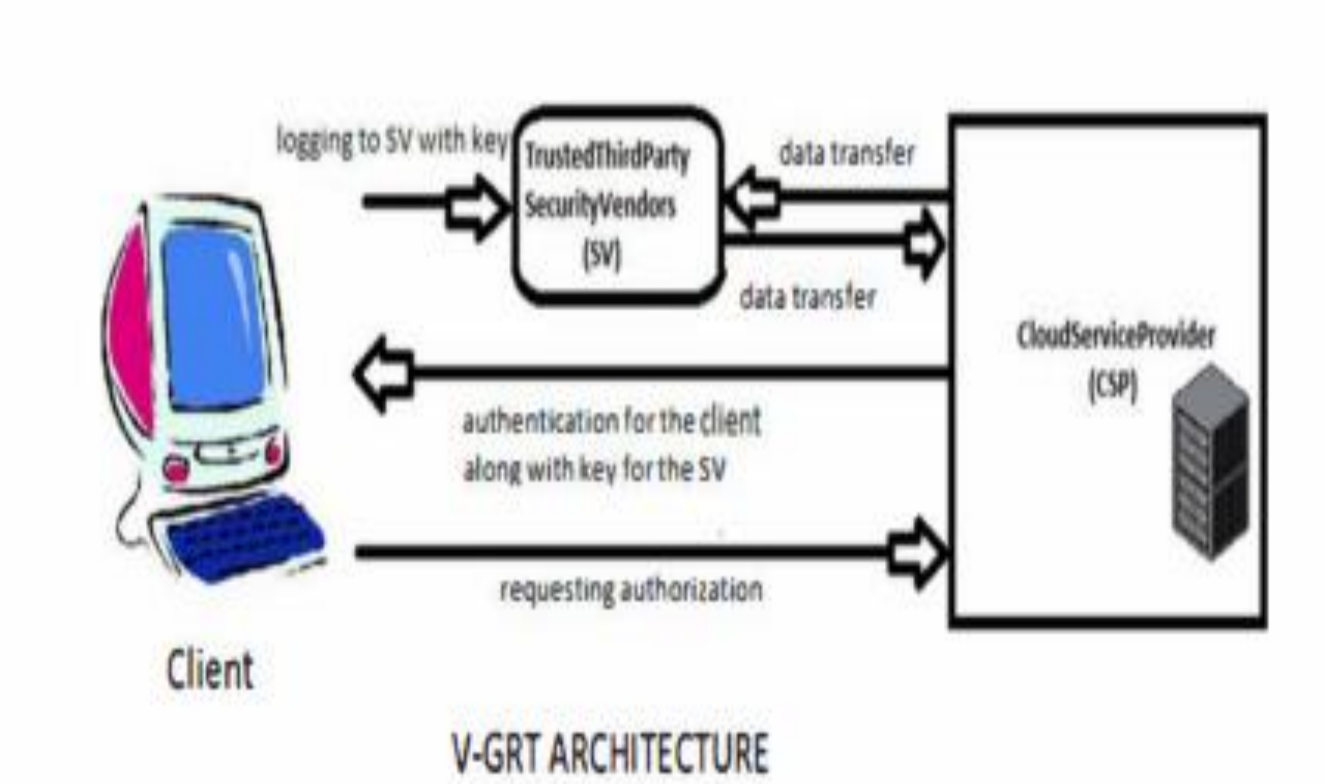


Fig2,System Architecture

VI. IMPLEMENTATION

Framework examination is the most common way of social occasion and deciphering realities, diagnosing issues, and data about the Property The board Framework to prescribe upgrades to the framework. A critical thinking action requires concentrated correspondence between framework clients and framework designers. Framework examination or study is a significant period of any framework advancement process. The framework is considered to the littlest detail and examined. A frameworks investigator assumes the part of a questioner and stays profound into the operations of the ongoing framework. The framework is seen overall and the contributions to the framework are distinguished. Yields from associations are followed to different cycles. Framework examination manages issue mindfulness, ID of pertinent and dynamic factors, investigation and amalgamation of different elements, and assurance of the ideal or if nothing else good arrangement or program of activity. An itemized investigation of the cycle should be finished through different procedures like meetings, surveys, and so forth. The information gathered by these sources should be inspected to come to an end result. The primary concern is understanding the way that the framework works.

This framework is known as the current framework. Presently the current framework is exposed to a point by point study and trouble spots are recognized. The creator currently goes about as an issue solver, attempting to take care of the issues the business is confronting. Arrangements are given as ideas. The proposition is then scientifically weighed against the current framework and the best one is chosen; the plan is submitted to the client for client endorsement. The plan is investigated at the client's solicitation and proper changes are made. This is a circle that closes once the client is happy with the plan. A starter study is the most common way of get-together and deciphering realities involving the data for additional investigations of the framework. Primer review is a critical thinking movement that requires escalated correspondence between framework clients and framework engineers. He is doing different possibility studies. In these examinations, an unpleasant sign of the framework exercises can be gotten, based on which choices can be made about the methodologies to be followed for compelling review and examination of the framework.

BLOCK DIAGRAM:

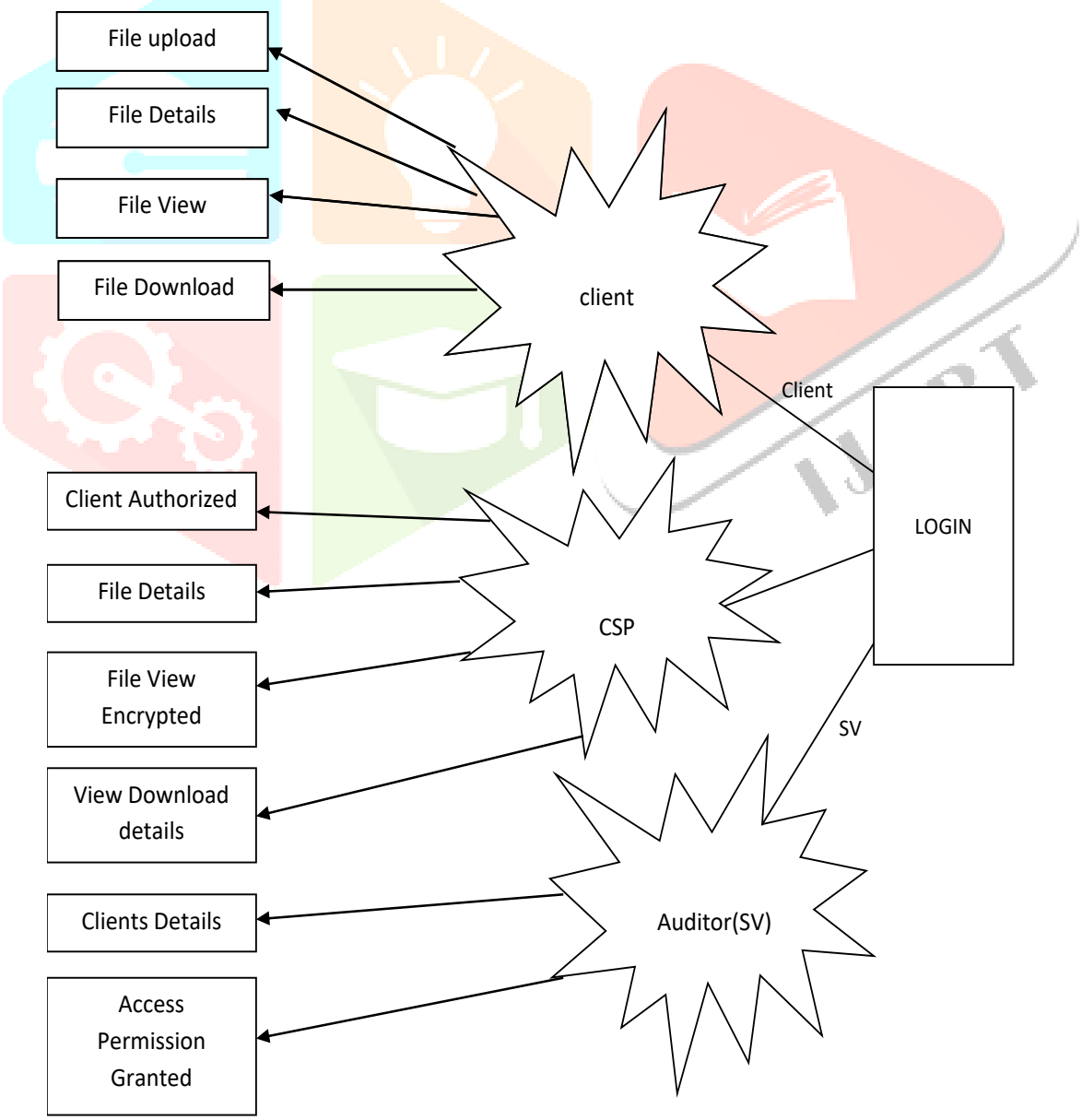


Fig3,Block diagram

DATA FLOW DIAGRAM:

1. A DFD is likewise called an air pocket diagram. A straightforward graphical formalism can be utilized to address a framework concerning input information to the framework, different handling with that information, and result information created by the framework.

2. Information Stream Graph (DFD) is one of the main displaying instruments. Displaying framework components is utilized. These parts are the framework cycle, the information utilized by the interaction, the outside element that collaborates with the framework, and the data streams in the framework.

3. The DFD shows how data travels through the framework and the way things are changed through a progression of changes. A graphical method shows the progression of data and the changes that are applied while moving information from contribution to yield.

4. A DFD is otherwise called an air pocket diagram. DFDs can be utilized to address a framework at any degree of reflection. DFDs can be isolated into levels that address expanding data stream and utilitarian detail.

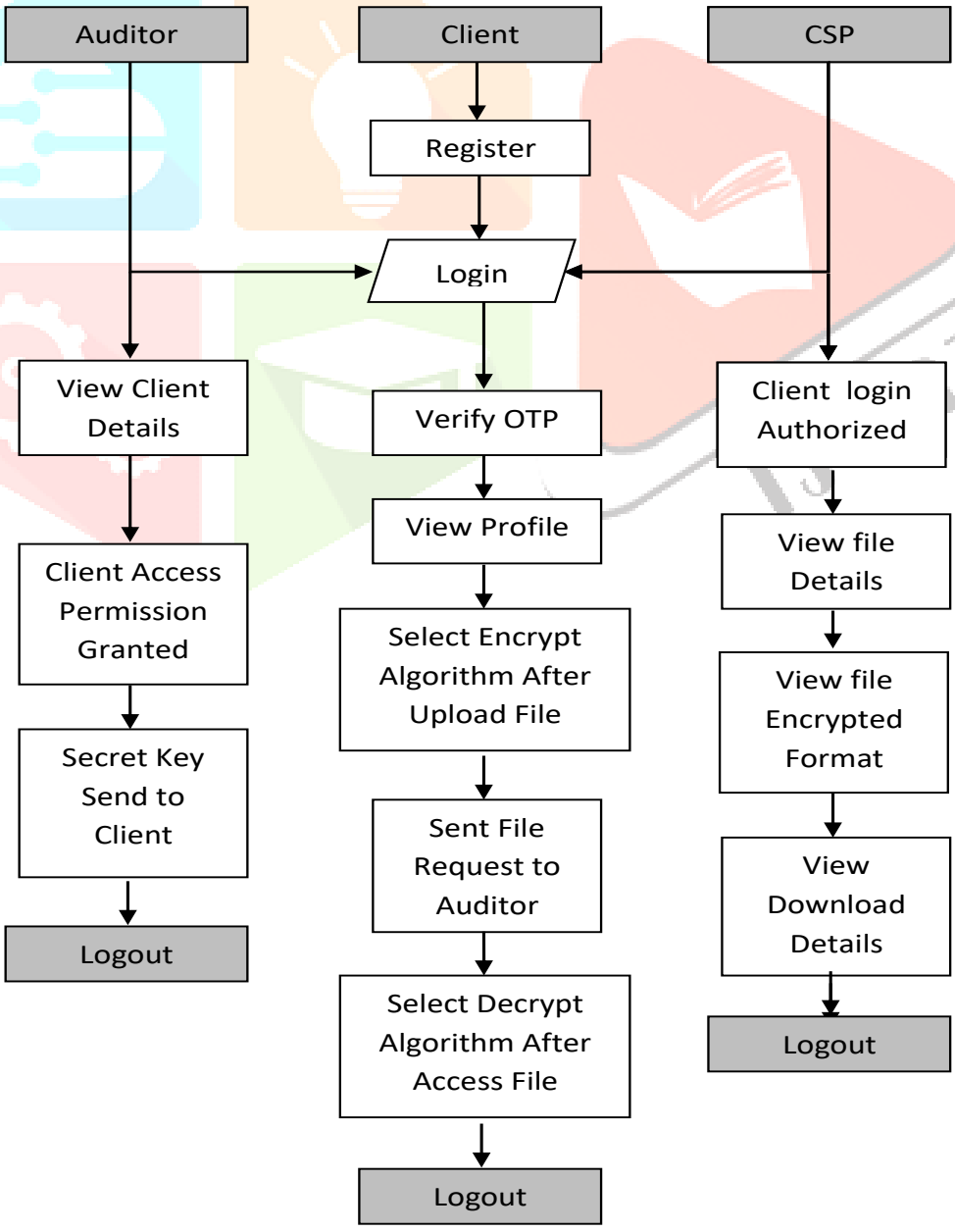
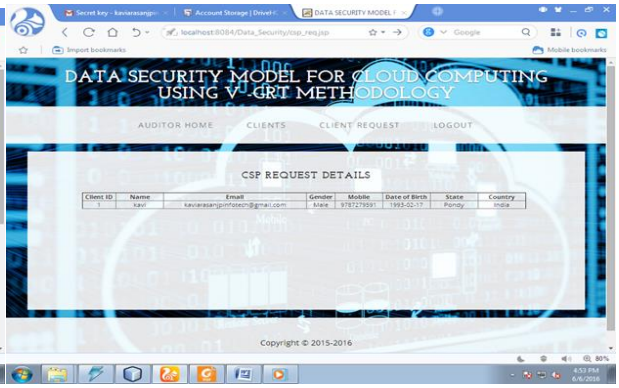


Fig4,Data Flow diagram

VII. RESULT AND DISCUSSION

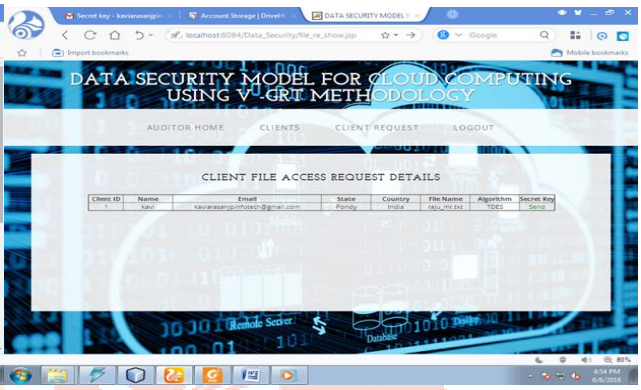
HOME PAGE

AUDITOR- CLIENT REQUEST

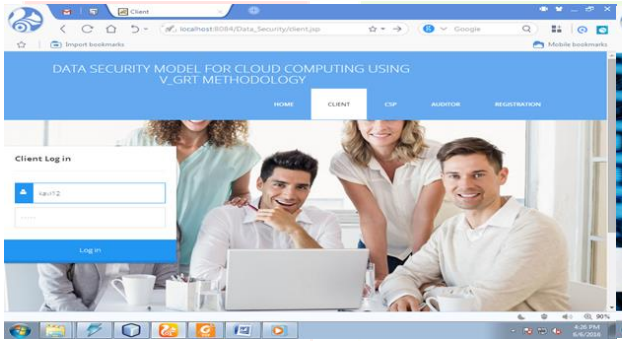


REGISTRATION PAGE

CLIENT FILE ACCESS REQUEST



CLIENT LOGIN PAGE

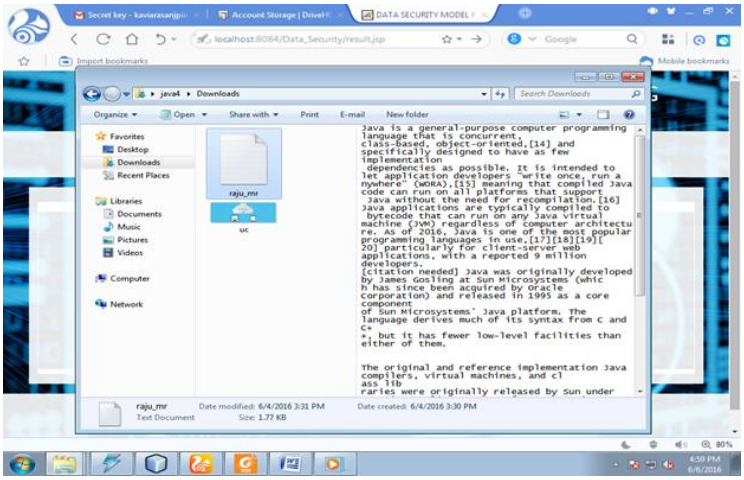


ENCRYPTED FILE VIEW

AUDITOR LOGIN PAGE

DECRYPTED FILE VIEW

FILE DOWNLOAD PAGE



VIII. CONCLUSION

Data and privacy protection are the primary problems that need to be solved in cloud computing. Data Security and privacy issues exist in all levels in cloud service. The above-mentioned model is fruitful in getting the user to trust the cloud computing so that the user can able to store confidential data over the cloud computing. The Encryption Algorithm applicability provides the flexibility in range and sequence to the user's choice because of the various Methods a user can apply all or omit any in any order. Even if the user does not select any encryption technique, then random number algorithm will be implemented by default thus providing at least a single level security. The opted sequence will also be stored in the database so that the decryption may be possible. The negative effect of this scheme is that it creates an overhead on the query performance due to multilevel of encryption and decryption but for the sake of security the performance issue can be overlooked as we are concerned with only a small amount of data like that of passwords and not the large files. In this way we can conclude that security vendor enhances security with the help of multilevel hybrid encryption.

REFERENCES

[1]. C. Gentry, "A fully homomorphic encryption scheme [Ph.D. thesis]", International Journal of Distributed Sensor Networks, Stanford University, 2009.

[2]. D. Boneh, "The decision Diffie-Hellman problem", Algorithmic NumberTheory. 2008.

[3]. A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security", Journal of Engineering Science Technology, 2010.

[4]. R. Arora, A. Parashar, and C. C. T. Transforming, "Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, June 2013.

[5]. D. Manivannan and R. Sujarani, "Light weight and secure database encryption using tsfs algorithm", Proceedings of the International Conference on Computing Communication and Networking Technologies ICCCNT '10.

[6]. F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud", Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (TWSSC '11).

[7]. K.Huang and R. Tso, "A commutative encryption scheme based on ElGamal encryption", Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC '12), August 2012.

[8]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data", IEEE Transactions on Parallel and Distributed Systems, 2012.

[9]. M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multiclouds to ensure security in cloud computing", Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11).

[10]. C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data". Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10).

[11]. M. Asad Arfeen, K. Pawlikowski, and A. Willig, "A framework for resource allocation strategies in cloud computing environmen", Proceedings of the 14th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW'II).

[12]. P. Victer Paul, D. Rajaguru, N. Saravanan, R. Baskaran and P. Dhavachelvan, "Efficient service cache management in mobile P2P networks", Future Generation Computer Systems, Elsevier, Volume 29, Issue 6, August 2013 , Pages 1505-1521.

[13]. E. M.Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing" , Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12).

[14]. S. Biedermann and S. Katzenbeisser, "POSTER: event-based isolation of critical data in the cloud", Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2012.

[15]. C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, security and data concealmen", Proceedings of the 16th IEEE Symposium on Computers and Communications (lSCC '11).

[16]. Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Fade: secure overlay cloud storage with file assured deletion", Security and Privacy in Communication Networks, 2011.

[17]. P. Victer Paul, N. Saravanan, S.K.V. Jayakumar, P. Dhavachelvan and R. Baskaran, "QoS enhancements for global replication management in peer to peer networks", Future Generation Computer Systems, Elsevier, Volume 28, Issue 3, March 2012, Pages 573 -582.

[18]. A. Rao, "Centralized database security in cloud", International Journal of Advanced Research in Computer and Communication Engineering, 2011

[19]. P. Victer Paul, T. Vengattaraman, P. Dhavachelvan, "Improving efficiency of Peer Network Applications by formulating Distributed Spanning Tree", Third International Conference on Emerging Trends in Engineering & Technology (lCETET-201O), IEEE, India, May 2010. pp. 813-818.