International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Data Privacy in Cloud Computing, An Implementation by Django, A Python-Based Free and Open-Source Web Framework

V Veeresh*[1], L Rama Parvathy[2]

Submitted: 18/09/2022 **Accepted:** 26/12/2022

Abstract: A feasible approach for transferring cyber risk is cyber insurance but, the network security may or may not be improved depending on the underlying environment features. A single profit-maximizing insurer (principal) together with client volunteers /insured volunteers was considered in this paper with a specific interest in two distinct cyber security features along with their impact on the contract design problem. Cyber security is interconnected, meaning that an entity's level of security is influenced by others' efforts within the same ecosystem in addition to its investment and effort (i.e. externalities). Secondly, the latest advancements made in internet measurement now permit an exact quantitative analysis of security posture at the form level when combined with machine learning techniques. Hence, the effective utilization of resources can be done possibly thereby reducing the cost of the manufacturers but, the only disadvantage of cloud providers is that the information will be safe and affordable in the cloud. So, the data must be encrypted before being transferred into the cloud. Secure private keys are made available to users of a collision protection information sharing system so they can add or remove customers. Via the certified authorities and safe channels, the new customers will receive the keys from the team managers. Therefore, a revoked customer won't be able to retrieve common data documents even if they are using the cloud. Hence, a revoked user will be prevented from data document retrieval even if they are utilizing the cloud.

Keywords:*Cloud Computing, Cloud Security, Cloud services, Crypto graphical storage, File-block keys, Native management System, Secure private keys, Un-trusted cloud.*

1. Introduction

The existing works examine the insurance’s impact on the security of agents' expenditures in competitive insurance marketplaces under mandatory insurance. A competitive market is considered by authors accounted with homogenous agents to demonstrate how the security state of the network has deteriorated by the insurance in comparison to the scenario of no insurance. The existing study considered a homogenous agent’s network to show that the network security state cannot be improved by the introduction of insurance. Also, it examines the effects of the degree of agent interdependence and demonstrates that as the level of interdependence rises, agent investments fall. Also, a competitive market in which agents participate voluntarily, both with and without moral hazard has been investigated.

The insurer can observe the investment of the agents in security without the moral hazard thus discriminating the premium depending upon the observed investments. This proves that this kind of market can offer agents incentives to increase their investment as self-protection. However, the agents will not be provided with incentives to improve their investment under moral hazard. In the current system, it has been investigated how insurance affects network security when there is a monopolistic insurer who maximizes welfare. As the aim of the insurer in these models is to improve social welfare, agents are provided with discrimination of premiums which means the agents with better-secured investments can pay lower premiums. Thus, these studies show that insurance can improve network security. By assuming voluntary participation, the existing work has examined an insurance market with a monopolistic profit-maximizing insurer which illustrates that the security state of the network cannot be improved with moral hazard when compared with the no-insurance.

2. Literature Review

By utilizing the resources from various locations like the cloud, a secured network has been framed to enhance the trust and confidence between the data owners and the service providers. By using the watermarking and data coloring method, authenticated data has been provided along with strong data control access both in public and private, and a single cloud depending upon the existing demand. Businesses are adapting the models to deliver Data Protection as a Service (DPaaS) and SECurity as a Service (SECaaS) owing to the rapid growth in cloud computing [1].

Security issues with cloud computing services are a topic of discussion since they put a lot of challenges on the data and storage layers. The Map Reduce in Hadoop security in processing massive data has been studied where the data are partitioned and presented along with independent tasks also covered. In the final section, the XACML application for Hadoop has been demonstrated by utilizing the trusted applications from non-trustworthy servers, to provide create the safest cloud computing with the finest data

[1] *Saveetha School of Engineering, Chennai, Tamilnadu, India.*
[2] *Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India.*
*Corresponding author Email: vaddeveeresh@gmail.com

access control [2].

The security of the data has been ensured with the RSA algorithm where the respective user along will get the access to data. The cloud service provider does the encryption whereas the cloud user does the decryption and thus, by implementing the RSA algorithm, data security will be provided [3].

By calculating the time of encryption, time of decryption, and the key generation time, the data will be encrypted right before cloud storage, by using a new encryption technique that will compare 3xAES with AES and T-DES algorithms. Based on the length of the key, data security will be high which means 3xAES will have a refined security level than AES and T-DES as it will be encrypting the data three times with a new key for every encryption and decryption [4].

Executing risk assessment, analysis, and mitigation, a framework has been implemented to cover all the models of cloud service and cloud deployment. Successful execution of secured information or the altering of data for a cloud computing environment is the justification for accepting this framework. It is utilized in logistics. The framework is examined with Platform as a Service (IaaS) whereas Software as a Service (SaaS) will be created and implemented in the locations of Infrastructure as a Service (IaaS) [5].

Due to main reasons like data storage and privacy safety measures, cloud computing services have been accepted by consumers. This was followed by an in-depth discussion on the safety issues of cloud computing that includes solutions to those issues. But the scope hasn’t met the expectations, and so, future research on security and privacy issues related to the cloud has been recommended [6].

Depending on the needs of the organizers, either a single-tier "Security as a Service" or a multi-tier coherent security system will be provided by a coherent system. Data security is assessed both at the macro level and micro level of the cloud. This gives users with similar objectives or needs and the cloud application an efficient option [7].

The user-provided three cryptographic constraints which are Availability (A), Confidentiality (C), and Integrity (I), and these form basis for the system’s actions and methods to present the data from beginning to end. SSL (Secure Socket Layer) 128-bit encryption is used for safeguarding the data storage in the cloud which can also be upgraded to 256-bit encryption when required. Also, data authenticity is verified using Message Authentication Code (MAC), along with searchable encryption which is followed by classifying the data into three segments on the cloud.

The data stored in the cloud is protected using methods such as SSL (Secure Socket Layer) 128-bit encryption, which can be increased to 256-bit encryption upon request. The authenticity of the data is also confirmed using MAC (Message Authentication Code), and searchable encryption and the data is divided into three segments in the cloud. In Section 1, Section 2, and Section 3, the consumer is given a login identity and password to access the data that has been safeguarded following data conversion [8]. So in Sections 1, 2, and 3, a login identity along with a password will be provided to the consumers to prevent data after the process of data conversion [8].

Several surveys have been conducted on data safety and privacy from hardware and software where the data is stored across various cloud locations. To get the highest cloud data security, several methods were recommended to create trust between the users and the cloud service provider [9].

Data security issues are the main concern now and the main reason behind this concern is data security and virtualization security. As a result, cloud computing is currently confronting security challenges. Users frequently move from one cloud to another while storing their data on the cloud, endangering the data's security. The elliptic curve cryptography technique is utilized to generate cryptographic keys faster and more efficiently thereby providing better privacy, data quality, and privacy [10].

The study conducted on the cloud architecture presented three solutions to enhance cloud computing's data security process. To boost cloud computing security, the software is used recently in the Amazon EC2 Micro instance [11].

The quality and functionality of data processing, data collection in IIoT, data processing, data recovery, and secured data storage were examined by conducting various studies. After studying cloud computing and fog computing, the structured framework has been introduced for storing data more efficiently and securely and also for recovering data from IIoT to provide solutions. The data will be transferred depending upon the latency need which will be stored on the edge server or the cloud server [12].

To ensure data security in the cloud, two algorithms as Blowfish Algorithm and Advanced Encryption Algorithm (AES) were examined to ensure safety against unauthorized data access. Only the early proposal and technical details were discussed in this research paper whereas the data analysis has not been briefed [13].

A productive and safe controllable environment has been built with Distributed Hash Table (DHT) networks, Identity-Based Timed Release Encryption, and Attribute-Based Encryption (ABE) for cloud computing (IDTRE). Depending upon the user's requirement, the data will be encrypted, separated, and compressed to obtain in the form of Ciphertext. The encryption of the decryption key is done by implementing the IDTRE technique. The compressed ciphertext is kept on cloud servers, and the ciphertext key and extracted ciphertext are combined to create ciphertext shares that are disseminated over the DHT network [14].

Depending upon a homomorphic authenticator with arbitrary camouflaging, the cloud data has been audited using a public key and it resulted in preserving cloud data privacy. This also focuses on several auditing along with a bilinear dividing method resulting in multiple user settings. Hence, TPA is applied for conducting numerous auditing tasks and found, this technique to be the most secure and effective [15].

For the users relying upon cloud services. A new method was introduced to store and delete data efficiently and safely. The introduced new method comprises of All-Or-Nothing data transformation thereby securely storing and classifying the resources for decentralizing the data finally in the network. This model is efficiently used by resource owners for controlling their settings securely [16].

Users are provided with several advantages with the recent evolving technology, cloud computing but, there are many challenges involved in the security issues. Hence, several solutions have been offered to enhance secured cloud services. To achieve secure data storage and recovery from the cloud, proper management solutions might be used coupled with inventive or supported encryption techniques. This would restrict access to the data to registered users only [17].

To describe data scopes at various levels, a classification technique has been presented that provides safety to the segregated and stored data at every stage and resulted in successful analysis with the sample cloud storage data [18].

A combo together with constructing access trees is collectively called CP-ABHE which is nothing but a Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme. This tree will rise and rise frequently by merging the smaller ones where each leaf will have a secret number that can be used for data encryption. This will end up enhancing the performance. According to Ciphertext storage capacity and safety issues, CP-ABHE expressed the work more efficiently. [19].

In a multi-authority cloud storage structure, control measures and privacy protection are ensured by the PMDAC-ABSC data access control system, which is based on Cipher text Policy ABSC. The sign Cryptor and de-sign Cryptor have characteristics that are known to the authorities and cloud servers. By providing privacy, unidentified validation, and public verification, this method is therefore demonstrated to be secure for normal models [20].

A combined attribute index and a multi-center attribute authorization structure are some of the features of a classified multi-authority attribute-based encryption. A dual-tree is structured by identifying its characteristics and presented to a larger group. The value of the parent node in an attribute access tree is determined based on the child node. In this work, attribute-based encryption reduces decryption volume while compressing unnecessary data in the ciphertext to a higher extent. There are implications found both theoretically and practically in the “large universe" constructions framework [21].

To get solutions for storage and deleting problems, a mediated revocation and Mediated Constant Ciphertext-Policy ABE (MCCP-ABE) were constructed, and to enable file transmission in semi-trusted patterns, a third-party server has been designed by utilizing these methods for better access control. Then, it was evaluated for its performance and it resulted in retaining a numeric ABE ciphertext with a fixed length and a time restriction for conducting selective and restricted revocation [22].

3. Types of Cloud Computing

3.1. A Private Cloud

A cloud infrastructure that is operated only for a single firm is known as a private cloud. A private cloud can be managed and hosted internally or externally by a third party. An organization must reevaluate its decisions on existing resources for virtualizing the business environment before undertaking a cloud project with a significant level of engagement. In general, self-run data will be intensive with a physical footprint which may need space allocation, environmental controls, and hardware allocation.

3.2. A Public Cloud

When cloud service rendered over a network is kept open for public use, it is said to be known as a "public cloud" and is free to be used as it will be available based on pay per usage model. Still, the security constraints will differ based on the services made available by a service provider like applications, storage, and other resources when it is open to public usage and also at the times of communication being disturbed by a non-trusted network. Access is typically made through the Internet and is typically owned and operated by public cloud service providers. Some of the public service providers are Microsoft, Amazon AWS, and Google. Both AWS and Microsoft provide direct connect services under the names "AWS Direct Connect" and "Azure Express Route," respectively. Customers that use these connections must buy or rent a private connection provided by the cloud provider.

3.3. Hybrid Cloud

An integrated cloud service that involves both the private and the public clouds is known as a hybrid cloud and is used for performing various functions under an organization. Based on the degrees, all cloud computing services must be efficient. When compared, public cloud services will be more scalable and efficient than that private clouds.

- Integrated services containing both private and public services will be offered by separate cloud service providers. A complete range of hybrid packages will be offered by individual cloud service providers.
- Private cloud management companies will subscribe to a public cloud service in which they can be incorporated into their infrastructure.
- Some of the characteristics of a hybrid cloud are cost efficiency, scalability, flexibility, and security.

3.4. Cloud Services

Though the cloud is a type of environment that can be accessed remotely, all IT resources within them cannot be remotely accessed. For example, the physical server and database inside a cloud can be accessed by the IT resources that are belonging to the same cloud. Hence, software with published API will be implemented to help remote clients get the right access.

The term "cloud" was coined by people who created and sold client-server software, hardware, and applications many years ago when we would link a PC to a network and a server to the network to create an image. We simply sketched a cloud and titled it "network" because none of us genuinely knew how the network operated. There are days when companies have built their networks on their own but currently, businesses and consumers were using network cloud services offered by Masergy, Verizon, AT&T, and Sprint.

Application Cloud Services

For the last ten years, all the business apps are being executed as cloud services whereas the focus was laid on consumer applications cloud services previously. As a result, 15 companies have turned out to be public companies since the year 1999 with acquisition targets. Out of 100, 40 companies have shown that they haven’t utilized any of such services. Currently, Oracle and JDA have started offering applications as a service traditionally.

Platform Cloud Services

Platform cloud services are the last type being used for developing new applications by various software developers. In addition, it can be used for various purposes like managing applications, computing, and storing cloud services.

Development can be speed up with flexible and specific horizontal platforms to reduce the new app development costs. The experts in operations management can also benefit from a variety of platform cloud services. Broadband Requirements You must assess bandwidth and the potential bandwidth constraint in your strategy if you plan to use the cloud framework.

Memory capacity, which virtualization implementers discovered to be the main impediment to virtual machine density. And this is addressed by a new wave of servers that have significantly bigger memory footprints, eliminating memory as a system limitation. By taking the problem of machine density out of the equation and giving the cloud provider control over it, cloud computing eliminates that constraint and relieves the cloud user of that concern.

The strongest barrier is the bandwidth from the providers to and from the cloud in cloud computing. A blade server is nothing but the optimized space to consume energy. Broadband speed enhancement is one of the major benefits of using a blade server for cloud computing. The IBM BladeCenter, for instance, was created to efficiently and swiftly accelerate high-performance computing tasks. The bandwidth restriction and limitation can be checked whether they are performing well or not with the service provider's capabilities to ease the high machine density problem.

Advantages of cloud computing

Cloud computing has numerous advantages and do you want them to occupy your personal computer with private emails, illegal MP3s, and unwanted files while you were leaving that responsibility to some other else? Using cloud computing, you can buy services whichever you want thereby avoiding the problems of equipment going out of date. This will ensure the reliability and security of the system and whenever needed, you can add some other services additionally as per your wish without waiting for a long time for the new computer.

Cloud computing has several clear advantages that are powerful. Do you want them to fill up your expensive PCs with their private emails, illegally downloaded MP3s, and unwanted YouTube movies when you could reassign that task to someone else? You can reduce the upfront capital expenditures of computers and accessories by using cloud computing to only pay for the services you need when you need them.

You prevent outdated equipment and other common IT issues like guaranteeing system security and dependability. As your company's needs evolve, you can add more services at a moment's notice. Without having to wait weeks or months for the new computer (and its software) to arrive, it is incredibly quick and simple to add new apps or services to your organization.

4. Problem Definition

The way that cloud service providers currently do things gives pay-as-you-go storage for hosting data files. The cloud is not trusted, though, as cloud service providers have a quick tendency to lose credibility as they can understand the information type. New user registration, revocation of an existing user, and processing of the system settings will be handed over and operated by the group manager. In light of this, the research assumes that everyone involved has complete faith in the group administration. Group members are a group of persons that have joined up to store and share their data in the cloud and the group membership can be dynamically adjusted depending upon the new user registration and existing user revocation.

However, this current method is unsafe due to the absence of effective commitment protection during the issue of identity tokens. To achieve secured key distribution, secured user rejection, and better access control in the cloud group that is dynamic, such a technique is not feasible since it does not require adjusting and updating the private keys of the other users.

5. Automatic Coding

5.1. Automatic coding via Bayesian classifier (Germany)

Bethmann et al. (from the Institute for Employment Market and Career Research) presented their research by using two different types of probabilistic supervised machine learning algorithms. The two types of algorithms are Naive Bayes (NB) and conjugate Bayesian analysis based on multinomial distributions (BMN). These two algorithms are used in German panel surveys for occupation coding automatically which was held at the 2014 International Methodology Symposium of Statistics Canada with a sizable amount of 300,000 manually coded occupation text strings from recent surveys. By utilizing the agreement rate between automatic coding and manual coding, both algorithms have been assessed. Authors reported that though the algorithms have performed with good agreement rates by common machine learning standards, they are not satisfying the higher range of accuracy needs.

However, findings suggested that both methods produced noticeably better results if the objective variable was changed either to "social-economic status" or to "occupational prestige". Specifically, both the ISEI-08 and SIOPS-08 scores are obtained from occupation codes. It was concluded by the authors that existing versions are enough for forecasting occupational prestige and socioeconomic status.

Still, to develop trustworthy occupation coding, a few more advancements are required. By including a preprocessing phase, it is possible to make improvements to clean input text strings and by utilizing alternative machine learning techniques like random forests or support vector machines minimizing the noise in the training data can be achieved which will be then incorporated into a specific distance metric into the current models.

5.2. Automatic occupation coding via CASCOT (United Kingdom).

The University of Warwick's Institute for Employment Research, a collaborator on the Eur-Occupations project, produced the automated occupation coding software application known as Computed-assisted Structured Coding Tool. The project's goal is to create a freely accessible database of the most common occupations to make it easier to collect data from multiple countries. Since 2009, CASCOT will execute automatic coding in any of the 7 languages that are spoken in eight Eur-Occupations partner nations. It will execute it into the ISCO'08 classification of occupational literature. If high-volume processing is required, a desktop version of CASCOT is available for purchase and is free to use online. However, the underlying methodology behind CASCOT has not been made public.

5.3. Open-source indexing software with automatic coding (Ireland)

It was reported that an automatic coding system was developed by the Central Statistics Office of Ireland for the classification of Individual Consumption by Purpose (COICOP) assignments for their Household Budget Survey which will be utilizing the data that are previously recorded during the training phase. This method is solely dependent on the open-source indexing and searching tool Apache Lucene (http://lucene.apache.org).

5.4. Utilizing Support Vector Machines, automatic coding of census variables

The potential of utilizing the support vector machines has been examined by Statistics New Zealand to enhance the item response coding in Census. By utilizing the two disjoint observation sets, support vector machines are used to code the occupation and post-school qualification of the variables. The two disjoint sets of observations measure 10,000 each in size, according to Census 2013 for testing and training. A 50% correctness rate was reported for both variables. It was reported that further investigations are required for the evaluation of support vector machines (SVM) as an automatic coding technology.

6. DJANGO

Django is an open-source framework and is Python-based following the MTV architectural pattern which is the Model Template Views pattern. A non-profit American independent organization, Django Software Foundation (DSF) is maintaining it. The main goal of Django is to simplify the process of creating intricate, database-driven webpages. The framework is made with pluggability and reusability components like low coupling, lesser codes, fastest development, and the principle of don't repeat yourself [11]. Python is used throughout the process including the settings, data models, and files and it also provides the optional read, create, update, and deleting interfaces which can be dynamically generated and configured by the admin models with the method of introspection.

Ridiculously fast -Django was framed for helping developers in developing an application right from the beginning to end.

Reassuringly secure – As Django considers security seriously, it aids developers in avoiding the security mistakes that are arising frequently.

Exceedingly scalable - Django offers greater flexibility and scalability to several busy websites available on the web.

Web applications may be developed with Django and launched in a matter of hours. Hurdles regarding web development will be efficiently handled by Django as it helps develop the app with no need of inventing the wheel and this will be open and free source available. Django has numerous features for handling all the chores of web development like the authentication process of users, content management activity, RSS feeds, site mapping, and some other host functions. Django was created to speed up and simplify routine Web development chores because it was developed in a hectic newspaper setting. Here is a quick introduction to how to create a Django-based database-driven Web application.

Although we have both a tutorial and a reference, the purpose of this document is to provide you with enough technical details to enable you to grasp how Django functions. When you are ready, you may begin the project either with a tutorial or can dive into a detailed informative document. Though Django can be used without a database, it includes an object-relational mapper in which you can define the database structure by writing Python code. The data-model syntax provides a variety of rich ways to represent your models; thus far, it has been successful in resolving years' worth of database-scheme issues.

The model layers

An abstraction layer is provided by Django to structure and manipulate the web application data. The details are as follows:

- **Models:** Introduction to models | Model class | Field types | Indexes | Meta Options
- **Query Sets:** Lookup expressions| Query Set method reference | Making queries
- **Model instances:** Accessing related objects |Instance methods
- **Migrations:** Migrations' Introduction | Migrations Writing | Schema Editor | Reference to the operations
- **Advanced:** Conditional Expressions | Transactions | Searches |Managers | Aggregation |Customized lookups | Query Expressions |Multiple databases | Custom fields |Database Functions | Raw SQL
- **Other:** PostgreSQL specific features | Providing the initial data | The view layers | Supported databases | Legacy databases | Optimizing the database access |

The view layers

To encapsulate the logic responsible for responding to a user's request, Django has an idea of views and information related to view layers are:

- **Reference:** Template | Custom storage | Built-in Views | Response objects |Request objects or response objects
- **Basics:** Shortcuts | View functions |Asynchronous Support | Asynchronous Support |URLconfs | Decorators |
- **Middleware:** Overview of Middleware | Built-in middleware classes
- **Uploading Files:** Overviewing Files |Managing files | API Storage | File objects | custom storage
- **Class-based views:** Overviewing Views | Built-in display views | Using mixins | Built-in editing views | Flattened index | API reference |
- **Advanced Views:** Generating a PDF | Generating a CSV

Forms

To initiate form creation and manipulate the form data, a framework is provided by Django to make the processes easier.

- **Advanced:** Integrating media | Forms for models | Customizing validation | Form sets
- **The basics:** Overview | Built-in widgets | Built-in fields | Form API

The development processes

Know more about the components and tools used to develop and test Django applications.

- **Settings:** An Overview | Full list of settings
- **Applications:** An Overview
- **Testing:** Introduction | Writing & running tests | Included testing tools | Advanced topics
- **Exceptions:** An Overview
- **Django-admin & manage.py:** An Overview | Adding custom commands
- **Deployment:** An Overview | Deployment checklist | ASGI servers | WSGI servers | Tracking code errors by email | Deploying static files |

Template layers

For rendering the data that will be displayed to the user, a designer-friendly syntax is offered by the template layer. Learn how designers can utilize this syntax and how programmers can expand it:

- **The basics:** An Overview
- **For programmers:** Custom template backend | Custom tags | Template API | Custom Filters
- **For designers:** Built-in tags | Built-in Filters | Language overview| Humanization

The admin

One of the most popular Django features, the admin interface details are listed below:

- Admin actions
- Admin site
- Admin documentation generator

Performance and optimization

Several methods and technologies may be used to make your code run more quickly and with a lesser amount of resources.

- Performance Overview
- Optimization Overview

Security

When creating Web applications, security is a key concern, and Django offers several tools and procedures for protection:

- Disclosed security issues in Django
- Security Middleware
- Cross-Site Request Forgery protection
- An overview of security
- Cryptographic signing
- Clickjacking protection

Internationalization and localization

To help you create applications for many languages and geographical areas around the world, Django provides a strong international and localization framework:

- Time Zones
- Overview | Localization | Internationalization | Formatting Localized Web User Interface and form input

Common Web application tools

Several tools frequently used in Web application development provided by Django are:

- **Authentication:** An Overview | Password management | Using the authentication system | API Reference |Customizing authentication |
- Log In
- Caching
- Syndication feeds (RSS/Atom)
- Emailing
- Messages framework
- Sessions
- Serialization
- Sitemaps
- Pagination
- Managing Static files
- Validating the data

Geographic framework

A top-notch geographic Web framework is what GeoDjango aims to be. Making the creation of GIS Web applications as simple as feasible is intended to maximize the potential of spatially enabled data.

The Django open-source project

Study the Django project's development methodology and discover ways to become involved.

- **Over time of Django:** Release notes | Upgrading instructions | Deprecation Timeline | API stability |
- **Documentation:** About this documentation
- **Community:** The process of Releasing | Getting Involved | Organizing the Team | Repositing Django source code | Mailing lists | Security policies
- **Design philosophies:** An Overview of design philosophies
- **Third-party distributions:** An Overview of third-party distributions

Other core functionalities

Several other functionalities of the Django framework are as listed below:

- Types of content and generic relations
- Conditional content processing
- Redirecting
- System check framework
- Flat pages
- Signals
- The sites framework
- Django Unicode

7. DJANGO Environment

Django is a high-level, open-source, and free Python Web framework this will provide the fastest cleaning and develop the pragmatic design and this will handle all the difficulties associated with web development. Hence, the users focus on writing apps with no need for wheel reinvention.

The main objective of Django is to develop intricate, database-driven websites simpler. Rapid development, "pluggability," and don't repeat yourself philosophy are all emphasized by Django. Everywhere, including in the configuration files and data models, Python is used.

Furthermore, Django supports creating, reading processes, updating processes, and deleting interface processes that are dynamically generated throughout introspection and configured admin models.

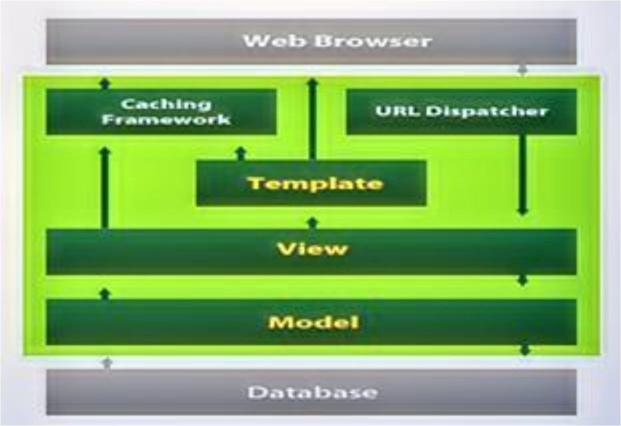

Fig.1 Django environment

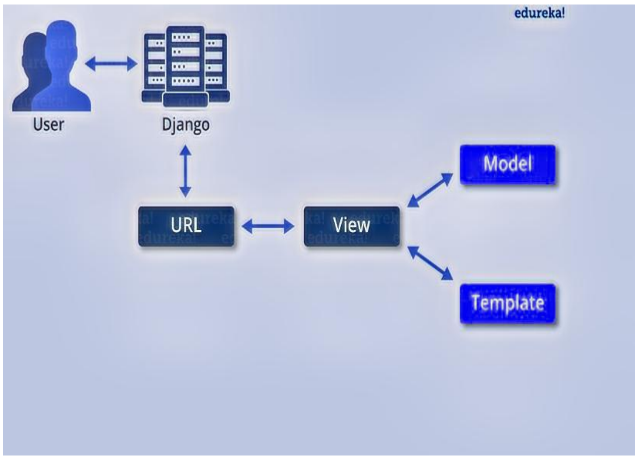

Fig. 2 Existing System

8. Existing system

- Various techniques like proxy re-encryption, key policy attribute-based encryption, and lazy re-encryption are combined for achieving the finest data access control with no need of disclosing the data contents.
- A cryptographic storage system was established by Kallahalla et al to enable safe data sharing over untrustworthy servers. This will be performed depending on the techniques that divide files into file groups and encrypts every file with a file-block key.

Disadvantages Of Existing System:

The system had a significant cost associated with key distribution. This is due to the reason that it is a must to update the file-block keys and then, distribute them widely for a user revocation.

- There is an increase in the difficulties associated with user participation and user revocation. The increase is due to the increase in the count of revoked users and data owners.
- Applications are hindered from implementation by the single owner in which the user can share their files with other group members by utilizing the cloud service.

9. Proposed System

- A secured methodology for data sharing and key distribution has been proposed in this paper that is suitable for dynamic groups.
- Due to the public key of the user, without any secured communication channels, a secured key distribution will be provided where the users can obtain their private keys from the managers without any certificate authorities.
- A secured method for distributing the keys has been offered with no secured communication channels. Users can obtain the keys from the managers securely with no need for any certificate authorities as the public keys are verified.
- To prevent collision attacks, the safest data-sharing methodology has been introduced. In this method, the revoked user conspires with a non-safety cloud and hence, they cannot access any original data after they have been revoked.
- The introduced methodology achieves safe user revocation by utilizing the polynomial function.
- Our methodology helps in supporting the groups efficiently whenever a new user enters the group. Private keys need not be updated or recomputed whenever a user is revoked from the group.
- The security of this methodology has been proved with the security analysis.

ADVANTAGES OF THE PROPOSED SYSTEM:

- The cost of computation is not based on the number of users in the RABC scheme as there is no limitation for several users revoked whereas the functions to decrypt data files will be remaining the same.
- Computational cost is not related to the users whose access has been revoked. The primary reason is that, in our architecture, the two signature verifications that account for computational cost don't depend on the revoked users whose access has been prohibited. The fact that the RBAC system does not take into account communication entity verifications is the cause of the low cloud computing cost during the file upload phase.
- The users can get their private keys either from their group manager Certificate Authorities or from the secured communication channels, under this scheme which will support the groups dynamically. Also, Private keys need not be updated or recomputed whenever a user is revoked from the group or entering the group.

10. implementation status Modules

I. Member or User Module
II. Manager Module
III. Cloud or Admin Module

I. Member or User Module:

1. To obtain access permission via a signature key, each user must register with the appropriate group.
2. The vendor list and the list of users whose access has been revoked are both included in the group admin.
3. The customer approaches the admin with a request to join the group. They can upload files to the cloud after receiving access permission. Members of the same group can download and simultaneously view the contents of the file.

II. Manager Module:

1. Accountable for giving or refusing access permission to members of different groups.

2. The primary access permission for managing the files on the cloud belongs to the manager. A manager is also able to move about the group.
3. The manager has access to the activity log information of cloud file storage.
4. Whenever a user is entering or revoked from the group, the manager can support them dynamically. Private keys need not be updated or recomputed whenever a user is revoked from the group.

III. Cloud or Admin Module:

liable for manager module and user module-related access-granting and access-denying activities.

2. The admin is authorized to manage all permissions.

3. Admin may efficiently revoke users using a public list of revoked users without having to change the remaining users' private keys, and new users can decrypt data without having to first encrypt it.

11. Proposed System Architecture

The private keys can be distributed using this approach in a very secure manner without the use of secure communication channels. Users can obtain their private after the process of verifying their public key from their group manager with no need for certified authorities. There are three actors in the architecture, namely the group user, group manager, and group administrator, as indicated in the aforementioned fig. 1. The list of revoked users and the vendor list are both included in the group admin. The customer approaches the admin with a request to join the group. Following registration, the administrator emails its mail address to the admin secret key. The customer can then upload or download the data after the verification.

- The files that are kept in the group are broken up into blocks, which are subsequently encrypted and kept in the cloud. The data were not fragmented before and were fully encrypted. Data security is improved by this block encryption. When a file is uploaded, this procedure takes place. The blocks of the files are merged and decrypted during the process of downloading the data file before being made available to the user. OTP is used for two levels of security. The first level's security system just requires a text-based password, and the second level's security system will produce a one-time password after level 1 has been completed. The OTP will notify the legitimate user on its email address. The system supports active groups effectively; however Private keys need to be updated or recomputed whenever a user is added or revoked from the group.

PROPOSED MODULES:

The proposed modules are as follows:

1. **PRESCREENING**
2. **THREAT DETECTION**
3. **LIMIT RESOURCES**
4. **ANALYSIS**

1. PRESCREENING

Normally, a login system can be used to screen a system, however, with this system, a username and password are not sufficient to authenticate the system. To verify whether the correct user has signed in or not, the security questions will be individually defined for each user. It restricts user access to protect them from dangers. While enrolling, the administrator can limit the class, and only the administrator can approve a user's admission into the system.

2. THREAT DETECTION

With the aid of prescreening approach, the threat can be found. Threats include unauthorized access to the system by performing a separate act on a specific account more than five times. Different users may have their insurance coverage configured. Users may access, as permitted by the policies. If a specific number of tries are unsuccessful, the user may be blocked and must ask the administrator to unblock them again.

3. LIMIT RESOURCES

The administrator is in charge of monitoring policy and rule violations. According to the policy, the administrator may prevent unauthorized access to a specific document after a predetermined period and be notified of any violations. The resources that have been uploaded by the admin or user can thereafter be blocked or unblocked by requests made by the admin to the user.

4. ANALYSIS

In this module, the system analysis will be performed to calculate the accuracy of the proposed algorithm. It might be useful to compute and display the comparison of several factors using graphs like pie charts, bar charts, and line charts. The system is used to gather the data needed to plot the graph.

DESIGN OF INPUT

The link between user and system information is called input design and is comprised of specifications of development and procedures for preparing data that are a must for transforming the data into a reusable form for processing. It will occur by directly entering the data into the system by inspecting the computer to read the data. The input design will be focused on the required format of the input, avoiding delays, avoiding the extra steps available thereby keeping the process more simple and easier with privacy retaining. It considers the following things:

- What is the data given as input?
- Validation methods for preparing inputs
- Steps to execute when the errors are occurring
- How the data must be arranged?
- How to code the data?
- What is the dialogue to guide and provide inputs?

OBJECTIVES

1. Input design is to convert the user-oriented description of the input into a computer-based system and is also vital for avoiding errors while processing the inputs. This helps in getting the correct information in the correct direction from the computerized system.
2. This is executed by creating user-friendly data entry screens for handling larger data volumes to make data entry easier with a zero percent error rate. The data entry screen will be designed such that all the data manipulations can be performed along with providing record viewing facilities.
3. The validity of the data is checked while it is entered in with the help of screens. To prevent users from maize of instance, accurate messages will be provided. Thus, an easy layout for input is designed with these objectives.

OUTPUT DESIGN

The output will be quality one if it meets the requirements of both the end user thereby presenting clear information. The processing results are communicated to users and another system through outputs. Output design is used to determine how the information can be displaced for urgent needs. This is the most vital and direct source of information to the users whereas system relationships can be improved with efficient and intelligent outputs to help users in the process of decision making.

1. Output computer designing must be well organized and the right output must be developed. Also, it is a must to ensure every output such that it helps users to find the system more easily and efficiently while they are searching and they should identify the correct output that is required to meet the requirements.
2. Creates documents, and reports in other formats including the information produced by the system.
3. Choosing the appropriate method for presenting the information.
4. One or more of the following goals should be achieved by an information system's output form and they are:
   - Triggering the actions
   - Confirming the actions
   - Conveying details about both the past and present status of the activities
   - Conveying information about the future projection
   - Signaling opportunities, warnings, important events, and other problems

RESULTS

Unit testing

The design of test cases is evaluated under this unit testing which will validate the functionality of internal program logic that they are producing proper outputs. It is a must to validate the decision branches and internal code flow. This testing will be performed between the stages of individual unit completion and right before integration. As this is relying upon its construction knowledge, this is also called structural testing and this is invasive and performed at the component level. This test ensures unique business paths and is operating accurately thereby clearly defining the inputs and expected results.

Integration testing

To ensure that the integrated software components are running as a single program or not, integration testing will be done and is concerned with basic output or screens or fields. This type of testing is done to ensure that the combinations of components are correctly made or not and also to check their consistency level. To address the problems arising out of components combination, integration testing will be conducted.

Functional test

A functional test is done to ensure that all the demonstrating functionalities are available as specified by the technical and business requirements, user manuals, and system documentation.

The focus of functional testing is on the following areas:

- **Valid Input:** Recognized valid input classes must be accepted.
- **Invalid Input:** Recognized categories of invalid input must be discarded.
- **Functions:** It is necessary to use the listed functions.
- **Output:** Specific application output classes must be put to use.
- **Systems/Procedures:** It is necessary to call interacting systems or processes.

Depending upon the key functions, requirements, and special test cases, functional tests are organized and executed. Also, the facts like the identification process of business process flow, predefined processes, successive processes, along with data fields are accounted for testing. Before ending, additional testing is found and the value of the current test will be evaluated.

System Test

The system will be conducted to ensure that all the requirements have been met by an integrated software system. To assure known and predictable results, it checks a configuration. System testing examples include the configuration-oriented system integration test. Depending upon the process flows and descriptions system test will be conducted to emphasize the integration points and process links that are pre-driven.

White Box Testing

The testing process of software along with inner workings, structures, and model languages is called white box testing and this type of testing is used to test areas that cannot be visible under or cannot be reached from the black box level.

Black Box Testing

The testing process of software without inner workings, structures, and model languages is called black box testing and this will be written from a source document like a requirement document or specification document. Under this testing, the software is considered a black box that is not visible. Without accounting for the working methodology of software, this testing will provide input and responds to output properly.

Unit Testing

Though it is unusual to perform unit testing and coding in two different stages, this unit testing will be performed as a part of the combined code and unit test phase of the software lifecycle.

Test strategy and approach

Manual field testing will be performed whereas the functional tests are written in detail.

Test objectives

- All the entries made must work properly and accurately
- There should not be any delay in messages, entry screen, and response times.
- Identified links must activate the pages

Features to be tested

- Ensure that the entries are entered correctly in the prescribed format.
- All the links must redirect users to the correct page.
- None of the fake entries should be made

Integration Testing

Integration testing of the software is the testing done on two or more integrated components of the software. The integration will be done on a single platform to protect their failures and faults. An integration test is performed to check whether the components and software are interacting without any error or not.

Result of the integration testing: All the above-mentioned test cases are successful as there are no defects found.

Acceptance Testing

The critical phase of any project is the user acceptance testing and this testing will be requiring the end user's participation to ensure that the system has met the functional requirement.

Result of the acceptance testing: All the above-mentioned test cases are passed successfully and no defects have been encountered.

12. Conclusion

Thus, this paper studied the problem of cyber insurance policies designed for risk-neutral agents and risk-averse by a single profit-maximizing insurer. Though adding insurance to independent agents' networks will reduce the safety of the network, it was proven that the outcome will be different in a network of interdependent agents. In particular, the insurer can get the profit opportunity owing to the security interdependency leads that are created by inefficient levels that are exerted by free-riding agents in the absence of insurance but in the presence of interdependency. This may increase the risk transfer that an insurer will get profit from.

With the right contracts formed, insurers can get the advantage of getting additional profit when allowed by security prescreening. This will help agents to maximize their effort levels by incentivizing them to increase their commitments to selling to interdependent agents. Hence, it was shown that this kind of contract leads under that condition may not only lead to increased profit for both the agent's principal and utility but also improve the state of security for the network. Various alternative schemes have been utilized for sharing information over the un-trusted servers, but there are several limitations existing for the revocation and the user involvement in such schemes as there is a progressive increase in the information on the users and the revoked users.

From the secured communication channels and the certified personnel, secured private keys were obtained for the users by the cloud with an Anti-Collusion Information Sharing Scheme from the team managers. By providing the secured private keys, the scheme will support powerful companies when there enters a new registering user or a user is revoking from a group. These secured private keys will not be required to be recomputed or updated. When a revoked user cannot retrieve the data, the data will be safeguarded by this scheme even though they are attempting to process with an untrusted cloud. Hence, this scheme will handle the revoked users more efficiently at an ease.

Author contributions

V Veeresh 1: Conceptualization, Methodology, Investigation, Visualization, Software, Writing-Reviewing and Editing, Field study **L. Rama Parvathy 2:** Data curation, Writing-Original draft preparation, Software, Validation., Field study

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput*., vol. 14, no. 5, pp. 14–22, 2010.

[2] E. Bacis et al., "Securing resources in decentralized cloud storage," IEEE Trans. Inf. Forensics Sec., vol. 15, pp. 286-298, 2019 [doi:10.1109/TIFS.2019.2916673].

[3] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing" in International Conference on Computer Science and Electronics Engineering, vol. 1. IEEE, 2012, pp. 647-651.

[4] K. G. Figueroa and S. Pancho-Festin, "An access control framework for semi-trusted storage using attribute-based encryption with short ciphertext and mediated revocation" in Second International Symposium on Computing and Networking. IEEE, 2014, pp. 507-513.

[5] J. Fu and N. Wang, "A practical attribute-based document collection hierarchical encryption scheme in cloud computing," IEEE Access, vol. 7, pp. 36218-36232, 2019 [doi:10.1109/ACCESS.2019.2905346].

[6] J. Fu et al., "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," IEEE Trans. Ind. Inform., vol. 14, no. 10, pp. 4519-4528, 2018 [doi:10.1109/TII.2018.2793350].

[7] Gampala et al., "Data security in cloud computing with elliptic curve cryptography," Int. J. Soft Comput. Eng. (IJSCE), vol. 2, no. 3, pp. 138-141, 2012.

[8] U. Gupta et al., Enhancement of Cloud Security and Removal of Anti-patterns Using Multi Level Encryption Algorithms, 2018.

[9] K. Hamlen et al., "Security issues for cloud computing," Int. J. Inf. Sec. Privacy, vol. 4, no. 2, pp. 36-48, 2010 [doi:10.4018/jisp.2010040103].

[10] Q. Z. Journal, "Ahmed, Farah Qasim, and lect Dr. Amin Salih Mohammed. Enhancing the Data Security in Cloud Computing by Using New Encryption Method," vol. 3, no. 1, 2018.

[11] P. Kalpana and S. Singaraju, "Data security in cloud computing using RSA algorithm", International Journal of research in computer and communication technology, vol. 5841, p. 2278, 2012.

[12] E. M. Mohamed et al., "'Enhanced data security model for cloud computing.' in 2012" 8th International Conference on Informatics and Systems (INFOS). IEEE, 2012, p. CC-12.

[13] S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," Concurrency Comput. Pract. Experience, vol. 31, no. 3, p. e4364, 2019 [doi:10.1002/cpe.4364].

[14] R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing" Procedia Comput. Sci., vol. 48, pp. 204-209, 2015 [doi:10.1016/j.procs.2015.04.171].

[15] R. Shaikh and M. Sasikumar, "Data Classification for achieving Security in cloud computing," Procedia Comput. Sci., vol. 45, no. C, pp. 493-498, 2015 [doi:10.1016/j.procs.2015.03.087].

[16] S. K. Sood, “A combined approach to ensure data security in cloud computing,” J. Netw. Comput. Appl., vol. 35, no. 6, pp. 1831-1838, 2012 [doi:10.1016/j.jnca.2012.07.007].

[17] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, 2011 [doi:10.1016/j.jnca.2010.07.006].

[18] Y. Sun et al., “Data security and privacy in cloud computing,” Int. J. Distrib. Sens. Netw., vol. 10, no. 7, p. 190903, 2014 [doi:10.1155/2014/190903].

[19] C. Wang et al., “Privacy-preserving public auditing for data storage security in cloud computing” in 2010, Proc. IEEE Infocom. IEEE, 2010, pp. 1-9.

[20] Q. Xu et al., “Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption,” IEEE Access, vol. 6, pp. 34051-34074, 2018 [doi:10.1109/ACCESS.2018.2844829].

[21] X. Zhang et al., “Information security risk management framework for the cloud computing environments” in 10th IEEE international conference on computer and information technology. IEEE, 2010, pp. 1328-1334.

[22] Z. Zhang et al., “Brij B. Gupta, and Danmei Niu,” IEEE Access, vol. 6, pp. 38273-38284, 2018 [doi:10.1109/ACCESS.2018.2854600].