A MONITORING AND DATA SECURITY MECHANISM FOR MULTIPLE CLOUD

[1]Samira Chandan, [2]Prof Vijay Shelake

[1]Student, [2]Professor

[1] Computer Engineering, SESGOIFOE, Mumbai University, India

[2] Computer Engineering, YTCEM, Mumbai University,

Abstract : ***Cloud computing is the combined solution for computation rather than a product, where software, resources, and information are shared to provided computational and other devices as a utility to consume this services over a network. Clouds can be classified as public, private or hybrid. Flexibility and portability are key services of Cloud Computing so that it can be accessed anytime from anywhere. By using redundant sites and backup storage, cloud service providers also provide greater reliability than local computing systems.***

Now-a-days the use of cloud computing has become very popular in many organisations. The reason for this is Cloud computing architecture provides user with computing services through internet on demand and pay per use access to shared resources. Cloud solutions and its resources are not only shared within multiple users but are also dynamically assigned on demand. However, this has created new challenge of security as data is stored and maintain on providers data centre leading minimum control of user on data.

Also, now-a-days use of single cloud is becoming less popular because of possibility of service availability failure and risk of malicious insiders in single cloud. So, use of multicloud environment is emerging due to the need of the application developer to combine the features exposed by different cloud providers

In clouds, it is essential to monitor the health of the system for its flawless operation. Cloud activities like resource planning, resource management, data centre management, SLA management, billing, troubleshooting, performance management, and security management essentially need monitoring to effective and smooth operations of the system. The aim and focus of this research is on the monitoring the system and providing solution on problem of data security. This research has built a common web platform cloud security and monitoring tool, which monitors cloud deployed entities such as Virtual machines (deployed on both Amazon web services and Microsoft Azure), Elastic Load Balancers, Amazon EBS volumes, Amazon RDS DB instances. This cross-platform solution also has alerting mechanism which triggers when user specific threshold is met and as a result Email is send to intended business head to notify about their abnormal state of cloud deployed entity. This also helps in monitoring and keeping track of critical cloud entities. Along with resource monitoring this tool also provides the security to data uploaded on the cloud regardless of client subscription to the encryption solution provided by the provider.

IndexTerms - — Cloud Computing, cross platform, monitoring, security, Client-side Encryption, AES

I. INTRODUCTION

In todays world one of the technology that is growing very fast is Cloud Computing. It is an extended form of distributed computing architecture which provides through internet computing services on demand and pay per use access to shared resources like networks, storage, software services and applications, servers without physically acquiring them.

Amazon Web Services (**AWS**) is a supplementry of Amazon.com that provides computing services to individuals, companies and governments, on a paid subscription basis with a free-tier option available for 12 months. AWS technology is implemented on cluster of servers throughout the world and is maintained by Amazon subsidiary. The user is charged depending on the usage and plan selected by him. As a part of agreement security is provided to subscribers system.

Microsoft Azure, (formerly Windows Azure before 25 March 2014) is a cloud computing platform and infrastructure, created by Microsoft, for building, deploying and managing applications and services through a global network of Microsoft-managed datacenters. All type of service models are provided by it and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems. Azure was released on 1 February 2010. [13]

A. Cost Saving

Cloud computing solves many problems of conventional computing like it reduces both running and installation costs of computers and software as there is no need to have any infrastructure. Users can access information from any corner of the world; all they need is to connect to a network (usually the Internet). Cloud computing offers companies cost saving option as the users need not have to worry about the storage space for huge data. Also the user need not have to hired highly skilled IT personnel for software updates as they are automated. The reason cloud computing technology gained trust was because of its performance, flexibility, availability and low cost.

B. Focus on Business

Cloud computing can provide full functioning platforms to organizations allowing them to build their own specific platform and share it with others with worrying about their communication as soon as they are subscribed to the cloud. Hence, cloud computing is being very popular and largely separated especially with the increase usage of internet connectively and virtualization techniques.

C. Increased Productivity

When multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed productivity may be increased and time can be saved.

The advantages of cloud computing may be very appealing but nothing is perfect one can't ignore the different threats to user's data/file on multi-cloud storage. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy. Cloud providers must provide solutions to these data security issues. Also in clouds, monitoring is essential for the health of the system and is important for both providers and consumers. Cloud computing also need monitoring for effective and smooth operation of the system. In proposed system we are developing the concept of single monitoring tool and providing data security in multi-cloud environment using AES encryption techniques.

II. EXISTING SYSTEM

Towards a Cross Platform CLOUD API, was researched by Dana Petcu and Ciprian Craciun at Institute e-Austria & West University of Timis¸ Oara, Romania from Second University of Naples, Italy. This research paper introduces systematic development of platform where features of different cloud service providers will share a common stage to facilitate the consumer's needs. This can be achieved with the help of APIs that are exposed by CSPs, to consume such APIs from federation of clouds requires a certain knowledge of programming the infrastructure. APIs exposed by CSPs are gaining popularity, due to emerging need of dynamic marketing treads of businesses who uses multiple cloud computing platform and service for their business critical applications. Businesses like these are trying to bring multiple cloud platforms together by accessing APIs exposed by CSPs to one common platform. Author's expectation from this approach is that it will add vendor independence for cloud based applications with higher degree of portability. [11]

Chrysostomos Zeginis, Kyriakos Kritikos, Panagiotis Garefalakis, Konstantina Konsolaki, Kostas Magoutis, and Dimitris Plexousakis identified that Cloud computing is becoming a popular platform to deliver *service-based applications* (SBAs) based on service-oriented architecture (SOA) principles. Monitoring the performance and functionality of SBAs deployed on multiple Cloud providers (in what is also known as *Multi-Cloud* setups) and adapting them to variations/events produced by several layers (infrastructure, platform, application, service, etc.) in a coordinated manner are challenges for the research community. Their paper proposes a monitoring framework for Multi-Cloud SBAs with two main objectives: (a) perform cross-layer (Cloud and SOA) monitoring enabling concerted adaptation actions; (b) address new challenges raised in Multi-Cloud SBA deployment. The proposed framework is empirically evaluated on a real-world Multi-Cloud setup [14].

Monitoring of infrastructural resources in clouds plays a crucial role in providing application guarantees like performance, availability, and security. This paper "Resource Usage Monitoring in Clouds" also stated monitoring is important from two perspectives - the cloud-user and the service provider. The cloud user's need to monitor the resources to check if they are using the resources according to the service agreement signed by them and the cloud provider's needs monitoring to see if the demands made by user in the agreement are fulfilled or not . To support this, a monitoring framework is necessary particularly since cloud hosts are likely to be affected by varying load conditions

III. PROBLEMS IN EXISTING SYSTEM

Cloud computing has been proved beneficial and advantageous not only in IT industry but across a variety of industries for basic business support functions. So, Cloud computing is used as tool to be a successful in evolving marketplace. It's been also observed that both government and private organizations are adopting cloud technology to either improve their existing process of operation or to delegate their work so that they can focus on critical function of operation.

But while adopting cloud computing, industries have understood that despite best efforts, no vendor is perfect.

So now they have understood that by combining best quality of different vendors, organizations can maximize the cost, agility and security benefits of cloud computing.

But with this the new problem arise , that is of managing the data as organisation have stored their data, distributed their operations, storage and other means of cloud use across different platforms. Along with this the security of data also matters.

This problem become an opportunity for "Monitoring and Data Security Mechanism for Multiple Clouds" study. To bring different culture of different cloud service providers together on one single platform.

IV. PROPOSED SYSTEM

4.1 Proposed Architecture

In today's IT industry when cloud computing platforms are used at its best with lot of usage flexible cost effective plans are made available on different CSPs platforms for their end users. Everyone is searching for best possible solution to one common problem i.e. how they can monitor (CPU utilization, network usage, memory usage and many more) and receive notifications about cloud deployed entities like business application, virtual machines and other cloud instances (databases, servers etc.) from different cloud platforms and service models , how they can secure their data on multiple cloud platforms. Today's I.T. industries look at cloud platform as a tool which will help them in surviving and in growing up their businesses with rapidly changing market. Cross platform cloud resource monitoring and data security research work elaborates best possible solution, by combining features of different CSPs on a common platform for cloud consumers.

Cross platform cloud resource monitoring and data security research is not only limited to Amazon web Services CSP and Microsoft Azure CSP for Monitoring, alerting and security , but also provides a common cross platform solution architected with such a dynamicity that it should easily accommodate more CSPs in near future. This research has built a common web platform monitoring and data security tool, which monitors cloud deployed entities such as Virtual machines (deployed on both AWS and Azure), Elastic Load Balancers, Amazon EBS volumes, Amazon RDS DB instances. This cross platform solution also has alerting mechanism which triggers when user specific threshold is met and as a result Email is send to intended business head to notify about their abnormal state of cloud deployed entity. This also helps in monitoring and keeping track of critical cloud entities. This solution also provides the security to the data uploaded on cloud by providing

client side encryption, which means before uploading the data on cloud it is encrypted first by using AES encryption technique regardless of client has subscribed to the data security mechanism provide by the CSP by paying extra charges.
This cross platform web application is architected such a way that once CSP account details are configured, many environments can be created and these environments can be configured for any cloud instance which is deployed on either AWS or Microsoft Azure. This platform also allows to configure environment for multiple account hosted on same CSP, this allows to have monitoring , alerting and data security feature for any cloud entity hosted on single or multiple account of same or different CSPs (AWS and Azure).

4.2 Implementation

Implementation of this vision is very effort taking since this will not just bring different culture of different cloud service provider together but it will also take maximum advantage of latest technology for betterment of future migration of cloud cultures, means developer should develop this vision such a way that this solution should be able to support more cloud service providers. This vision will be useful and efficient only when the system is ready for future migration, that's one of the reason why Domain Driven Design is selected for implementation.

The products that are analysed during requirements and design phase are implemented using appropriate technologies. Main focus is on Model–view–controller (MVC) and Domain driven design (DDD). MVC, a sophisticated software architectural pattern, this pattern separates responsibilities between Model, View and Controller. In this pattern Controller hold core business logic, it takes the input and provide it as a command to model or view, Model is used to manage data, logic and application rules and View provides the data to user in understandable format like charts, tables etc. Due to this simple segregated responsibility implementation has become very easy. This makes Monitoring scalable and robust even if architecture of different cloud service provider is unique.
REST APIs of Cloud providers are used to collect data points of instances. UI consist of views that are shown to users. It also includes graphical representation of data points of instances which is configured by cloud providers in this web application.

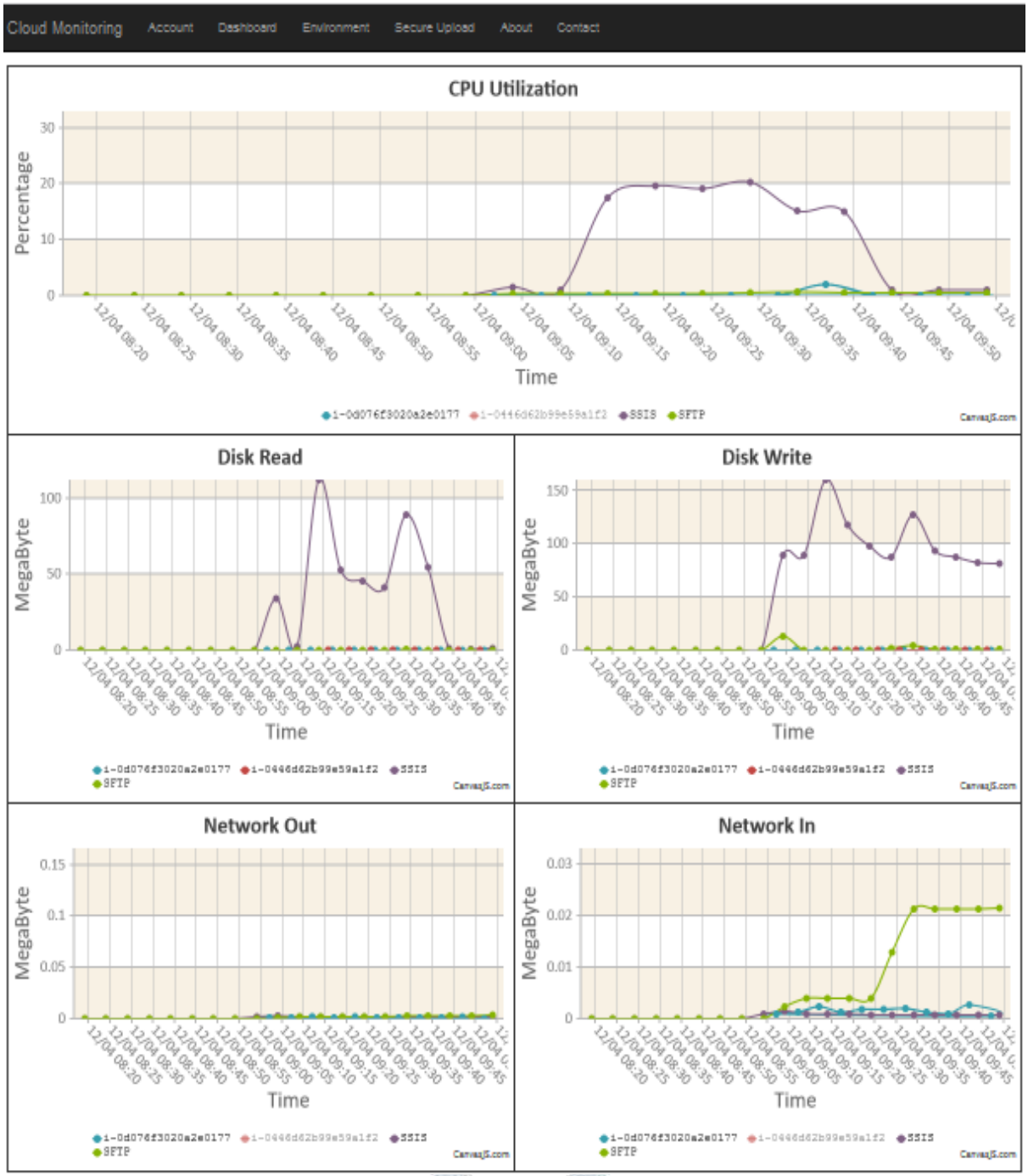
For client side data security in multiple cloud, AES algorithm is used. So that data is encrypted before uploading it to different cloud providers in this web application.

V. RESULT AND DISCUSSION

Result section is distributed in three main segments which are monitoring of a cloud resources using charts , ensuring data security and testing. In price comparison segment, different pricing models from different CSPs in this case (AWS and Microsoft Azure) are compared. This explains why consumers will choose different CSPs platform to fit in business budget. In next segment i.e. cloud resource monitoring, different parameters under which cloud deployed entities are monitored is explained. To represent cloud resource consumption in graphical format JavaScript libraries like Chart JS is used. Consumers also needs to provide their cloud account and resource related data before starting with the monitoring and notification.
In data security segment it will show what will happen if an illegitimate user tries to open a file. Last and final segment mentions steps carried out to test environment against functionality, usability and security.

5.1 Monitoring Cloud Resources with charts:

Chart JS is open source java script library used to display graph for cloud resource Monitoring. This charts will have inputs as data point which will be received through an API call to cloud service provider's REST API services. CSP's API services will be called and it will respond with data points to Monitoring platform, which are nothing but the representation of a cloud resource utilization, which will again represented in form of graphs to the user. If it is a Virtual machine or EC2 instance in case of AWS system will call for CPU utilization, Data In, Data Out, Network In and Network Out.

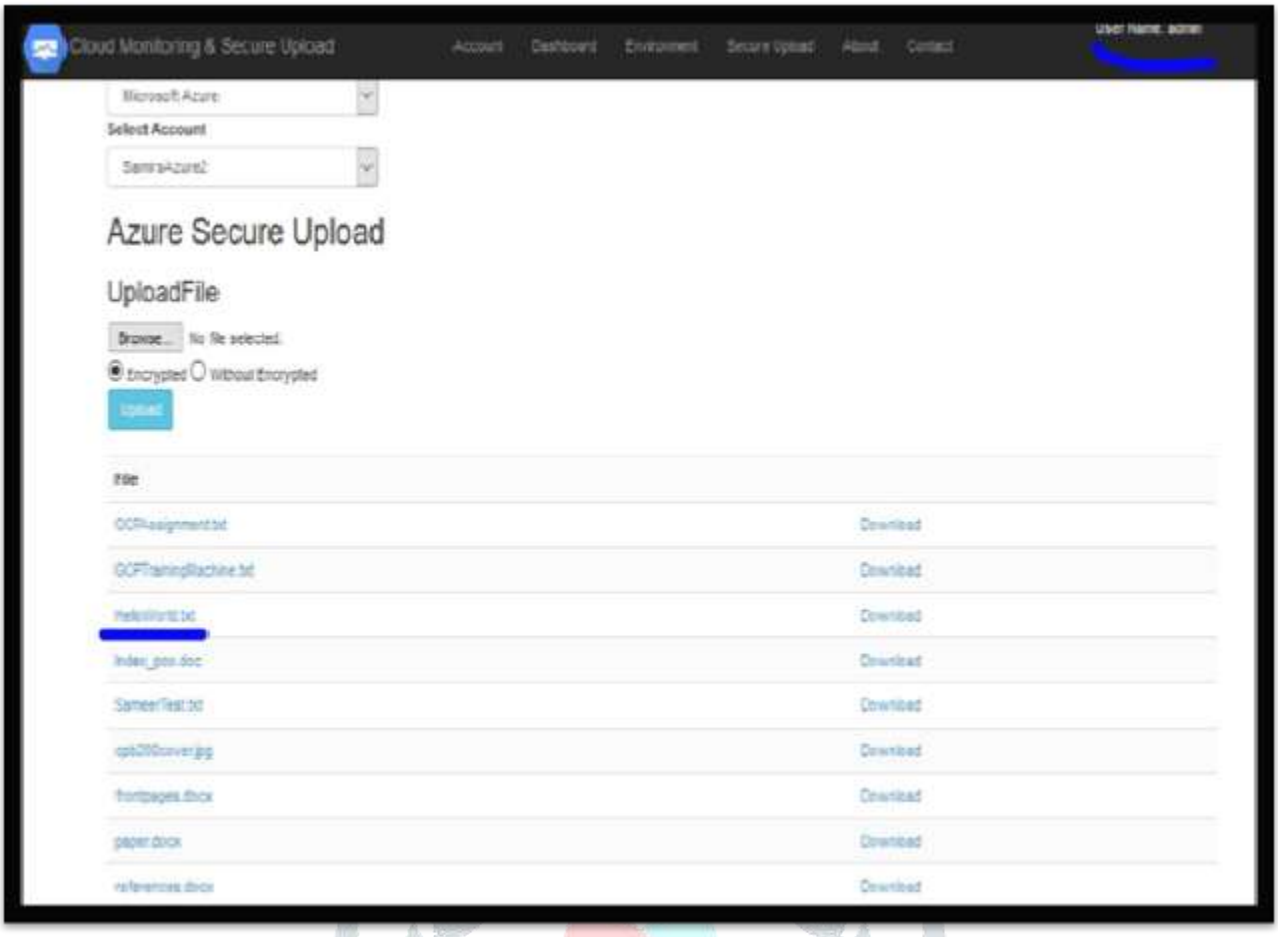


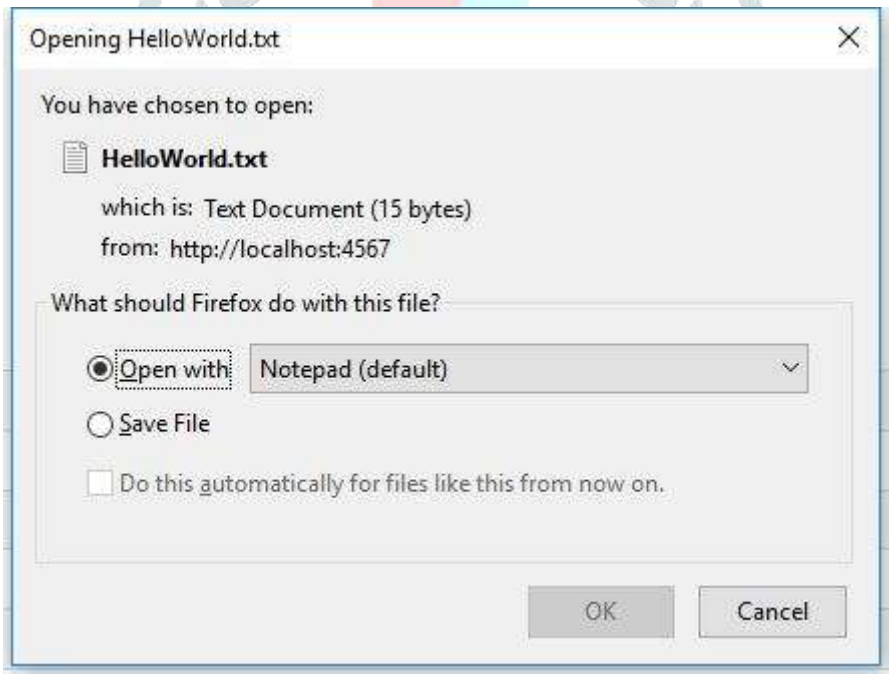
5.2 Ensuring Data Security

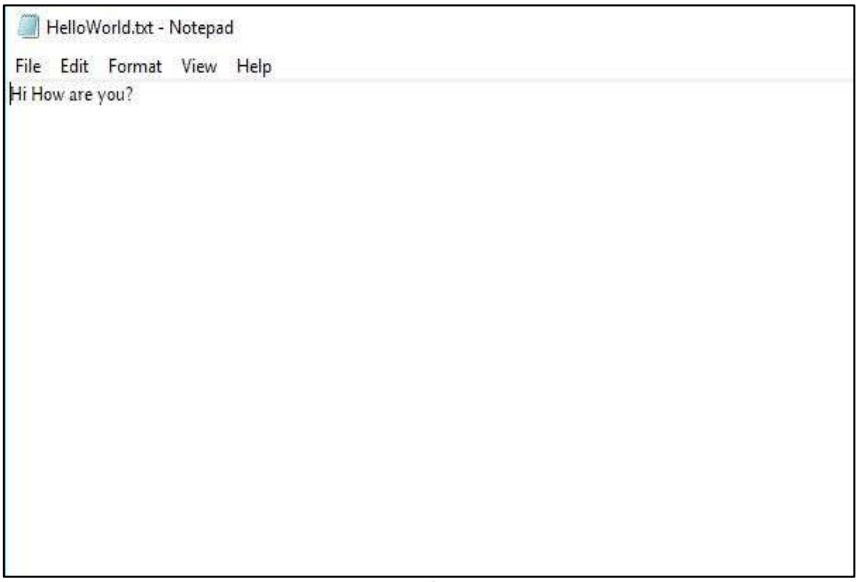
In cloud computing ensuring data security to client is most important as there are many ways through which an illegal user can breach the data security and data may be lost or used for an illegal purpose without the knowledge of an user. So in this automation tool we are providing data security by using AES encryption. So when any unauthorised user tries to access the data he will see the encrypted data.

Below screens show that what happens when both aythorised and unauthorised user try to access the file **"HelloWorld.txt"** uploaded by user **"admin"**

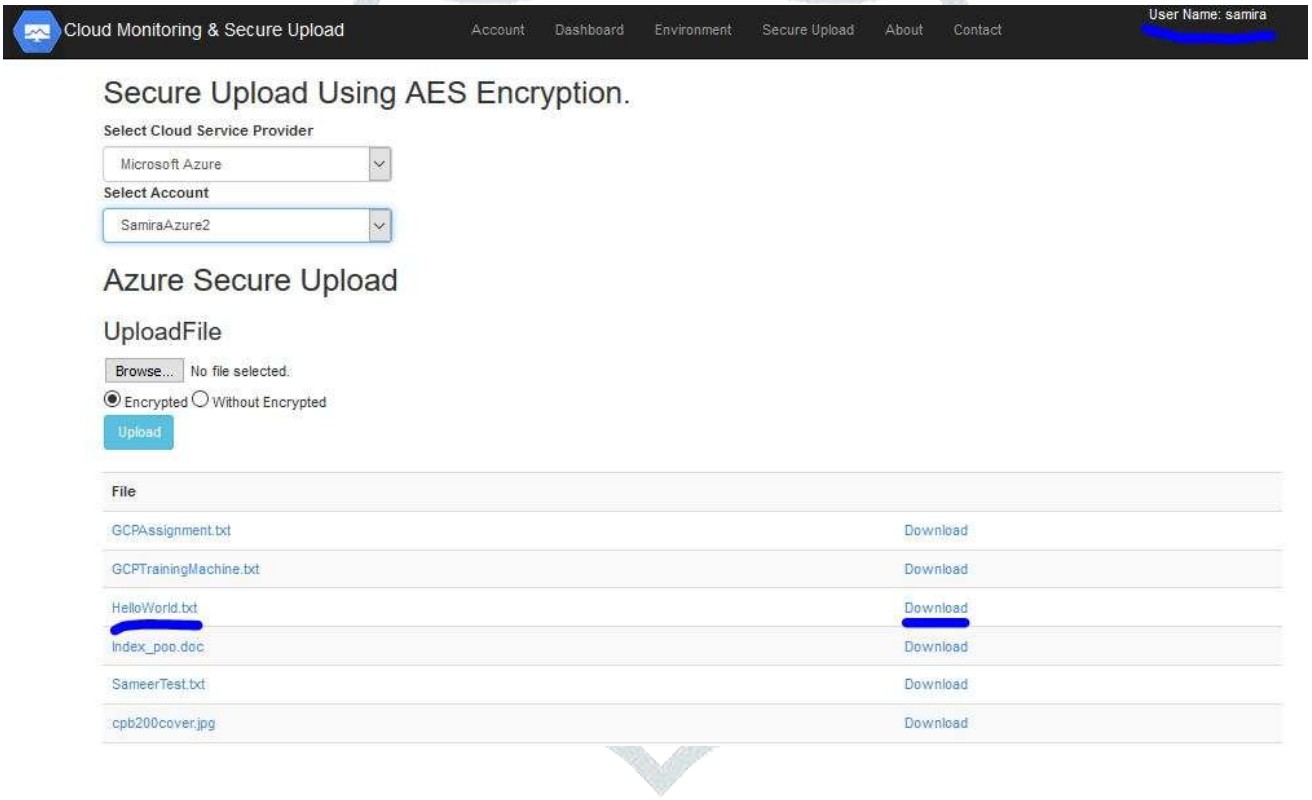
When "admin" tries to access the file


Cloud Monitoring & Secure Upload
Account
Dashboard
Environment
Secure Upload
About
Contact
Select Account
Azure Secure Upload
UploadFile
Browse...
No file selected.
Encrypted
Without Encrypted
Upload
File
Download


Opening HelloWorld.txt
You have chosen to open:
HelloWorld.txt
which is: Text Document (15 bytes)
from: http://localhost:4567
What should Firefox do with this file?
Open with
Notepad (default)
Save File
Do this automatically for files like this from now on.
OK
Cancel



Now see what happens when an unauthorised user try to access the same file



5.3 Testing in monitoring and security

- Functional Testing
- Reliability Testing
- Integration Testing
- Security Testing: This is very much important testing than any other because user are going to provide access keys to access their cloud specific data by our system.
- Authorization – Content uploaded to cloud will be accessible to only authorized user.
- Authentication

VI. CONCLUSION

MuliCloud Monitoring and Data Security application will allow organizations to intensively not just monitor but also provide alerts about the health and performance of their important cloud hosted resources on AWS as well as Microsoft Azure. It will also provide the data security to the client by encrypting the data before uploading it on cloud.

While development cycle we followed waterfall and agile implementation which provide great support. The agile approach is a method to develop a software where developer follows planning, designs, evolutionary development, early delivery and continuous improvement until whole application is developed. It involves both phase's implementation and maintenance. A application is developed in Sprints and deliver in phases. The agile design is a design methodology based on sprint wise delivery where application delivered in sprints involves process of prioritizing, testing, analysing, and refactoring application development process. Sprint Testing issues needs to be fixed in next sprint along with new developement, changes and refinements to the system. This process helps in improving the quality and functionality of a application design. In the agile design, sprints are used to carry implementation further and hand it over to testing team for new results this process continues till final phase. [13]

REFERENCES

[1] Amazon Website, "Amazon Documentation" All actions and API related information, Available: http://aws. Amazon.com/ documentation/.
[2] Amazon Website, "Amazon basic training", Training related data for Amazon API handlers Available: http://aws.amazon.com/training/.
[3] Amazon Website, "Amazon Tools" All available tools for development related documentation Available: https://aws.amazon.com/tools/.
[4] Amazon Website, "Amazon Services", all service related information for developer Available: https://developer. amazonservices.com/
[5] Velte, A.T, Velte, T.J. and Elsenpeter, R. (2009). Cloud Computing, A Practical Approach. McGraw-Hill.
[6] "Iterative and incremental methodology for development cycle of Automation in cloud", Available: http://en.wikipedia.org/wiki/Iterative_and_incremental_development
[7] Difference between incremental and iterative development of project "Computing", Available: http://programmers.stackexchange.com/questions/231770/difference-betweenincremental-and-iterative-approach
[8] Development training for Microsoft azure cloud API consumers, "Microsoft Azure" Available: http://en.wikipedia.org/wiki/Microsoft_Azure
[9] Amazon Simple Storage Services documentation for developers to understand coding, "Amazon S3", Available: http://en.wikipedia.org/wiki/Amazon_S3
[10] Amazon Elastic computation cloud related basic information "Amazon EC2", Available: http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud
[11] Baixing Quan; Coll. of Comput. Sci., Zhejiang Univ., Hangzhou, China; Tian-zhou Chen ; Hongjun Dai ;Bin Peng cross platform application development environment, IEEE Conference.
[12] Microsoft Azure services related documentation from, "Azure Services", Available: http://en.wikipedia.org/wiki/Microsoft_Azure
[13] Methodology meaning and information, "Methodology", Available: http://www.merriam-webster.com/dictionary/ methodology
[14] De Chaves, S.A.; Post Graduation Program in Comput. Sci., Fed. Univ. of Santa Catarina, Florianopolis, Brazil; Uriarte, R.B.; Westphall, C.B., toward an architecture for monitoring private cloud. IEEE Magazine, 29(12), pp. 130-137
[15] Shicong Meng ; Coll. of Comput., Georgia Inst. of Technol., Atlanta, GA, USA ; Ling Liu ; Ting Wang ,State Monitoring in Cloud Datacenters, IEEE Trans., 23(9), pp. 1328-1344
[16] Amazon EBS (SSD) pricing Available: https://aws.amazon.com/ebs/pricing/
[17] Amazon EC2 pricing Available: https://aws.amazon.com/ec2/pricing/ Microsoft Azure pricing Available: https://azure.microsoft.com/enin/pricing/details/virtual-machines/
[18 Introduction to Amazon cloud service provider Available: https://en.wikipedia.org/wiki/Amazon_Web_Services
[19] Introduction to Microsoft Azure Available: https://en.wikipedia.org/wiki/Microsoft_Azure
[20] V. A. Bharadi and N M Saswade, "Virtual machine monitoring in cloud computing" in 2016 Procedia Computer Science, pp. 135-142