A Flow Control Approach Using Tag Based Filtration for Cloud Computing and Its Statistical Performance Analysis

Neha Joshi
Department of Computer Science & Engineering
Jawaharlal Institute of Technology, Borawan

Abstract— Cloud computing technology is the integration of various computing models for serving the goals of tenant computation. It provides various operations as a service to the end users or the provider. Mainly the system deals with various internal components from which the flow of data is organized and depends on each other. Information flow control over cloud is one of the recent domains which require more effort to solve its issues related with security and robustness. The model counts the behavior of user access towards various services, complexity of flow, consumption and security measures. But as of now the users is getting exponentially increased with cloud and hence generates the issues related with isolation of data on interconnected devices. It makes more surface area for security attacks. Information flow control (FC) also assures confidentiality and integrity between the users interaction with the system. Primarily the flow control approaches use tagging or labeling mechanism. All it needs to clearly identify the traffic with cost effective categorization. For applying the categorization or class formation the data flow is analyzed and classified into several group of having communication similarities known as subjects. Traditional flow control is having certain issues regarding with clear separation of user's interaction, classification of flow information, categorizing the traffic classes, self contained tagging, labeling with over and under level process. This work suggests a novel flow control based on tag filtration for cloud computing. So many provisions are generated for guiding the information flow and achieves clear classification with improved accuracy. The result is been evaluated at analytical level is serving all the needs of effective flow control mechanism.

Key words: Software System, Cloud Computing, Security, Flow Control (FC), Labeling, Classification, Rule, Tag filtration, Encryption, Integrity, and Isolation

I. INTRODUCTION

Software based system is a group of multiple instruction for performing the desired task. During this execution, the information flows between various modules of software and the hardware installed with it. This information based data flow should be controlled for securing the exchanges of software system. Securities of such flows have to perform two major tasks: first is to make the information secure from the outsider or attacker and second is to protect the distributional flow of information. Form the above objectives only the prior one gets resolve effectively using some authentication and confidentiality mechanism. Models of secure data access are often classified into Mandatory Access Control (MAC) or Discretionary Access Control (DAC) systems [1]. They only prevent the information updates and outcomes but does not control the information flows between the systems.

Now a days, the software systems advancements lets their support for distributed and parallel systems for supporting the market based requirements. One of such requirements is cloud computing which provides the various computing paradigms as a service to the users by provisioning and sharing. Here the information flows through various heterogeneous systems rather than a single system. Now for cloud based system must require some modification in traditional flow control mechanism which only supports the formal access control. This access control is not sufficient for complete security. While the information flows handles how the information gets propagated during the complete operations of the system.

A. Information Flows Control (FC):

Propagation model for information must follows two basic requirements: Confidentiality using cryptosystem and access control and integrity which protects the reading or writing of information. It aims towards making the information flow secure using public output dependence, non interference and secret input processing. One of the important objectives of information flow integrity is to prevent its declassification from unintended user. Some of the outlines for getting a complete inner view of information flow some of the outlines are given with [2] are as follows:

- It controls the information dissemination using the propagation models from different heterogeneous objects.
- It frequently partitions the information into various classes to get the separate handling of objects and subjects for improving the flow security.
- The boundaries and conditions of security classes cannot be changed once created and hence the entity places respectively do not change their class.
- All the information flowing through the internal systems gets unambiguous paths which follows the security rules.

Both confidentiality and integrity policies can be staged into two parts. The policy language describing the possible classifications of information and how the different classifications relate, i.e., how information from one classification may flow with respect to the other and the semantic characterization describing the meaning of the policy language in terms of the semantics of the programming language. The former is predominantly described using a lattice model for information classification.

Keeping in mind the above requirements or rules, an attacker's model is required form which the comparison for attack confirmation has to be made. Traditionally such attacker model is program centric which have the control of the program completely and performs the operation to destroy or affects normal working of the system. But as the web based computing and operation gets on operating between distant locations through cloud, these attacker models is inadequate

for achieving the security goals. Some of the common model which works with the security improvements is:

- Access Control Lists (ACLs)
- Capability Systems and Role-Based Access Control (RBAC) are DAC systems

In later one (DAC) the owner of the data can modify access permissions. DAC systems achieve protection by controlling access to resources. Their implementations often focus on where access control checks are performed in the code of an application. Data is protected as a function of access control checks in the APIs provided to interact with that data. There are some problems also which the above models specially the DAC faces are:

- It may be possible to bypass access control checks, especially in web-based systems.
- Data can propagate or influence system behavior indirectly in ways that are disclosive, but which access control barriers at discrete points in code do not detect.

B. Flow Control With Cloud:

Cloud is the recent technology which aims to provide the applications and other resources using a computing paradigm through a service model to the user or intermediate provider with reduced managerial loads. It lets the provider and user the rapid adoption of application and other services using an online mechanism. As the number of users, their types, and requirements gets increased with the cloud their security controlling requirements also gets complex. Thus, achieving the confidentiality in cloud specifically with the data flow through tracking of boundaries for data is the recent field of work for researchers.

It aims towards making the data of flow viewer which categorizes the data according to their privileges and authenticity ad forwards them accordingly to their destinations. Here the data is first classified into various security classes with different access rights and flows the isolation rules using flow provisioning. For maintain the complete security boundary, the flow control will maintains the registry for each flow and give the categorization for protecting the sensitive data. Thus, here the information and its flow get security transited by isolating the data itself with low information. Users have to trust the efforts of both the third-party service provider and the cloud infrastructure provider for properly handling their private data as intended.

This works aims towards making the information flow control a complete a secure system using some of the novel filtering and label reading mechanism. Also the suggested models will help in acquiring the filtering schemes as per the system requirements. Traditionally, the information flow is working for only the static situations where the same types of software system is at both the end but with this work, dynamic and heterogeneous supports for secure information flow with clear isolation is achieved in near future.

II. BACKGROUND

Cloud computing is the recent area of advancements where the user are provided with their application in an effective service based delivery models. The ongoing shift of user in such technology giving rise to the significant concerns about security options over here. All it needs to increased the trust which should be more than traditional computing. Most of the companies are now working towards making their sensitive information secure form the attackers or must follows the access control according to their information visibility levels. Also, large scale companies are now moving towards integrating their solution with cloud computing which satisfies their business needs. But, the third party based access and data storage and exchanges always involves vulnerabilities related to their privacy and confidentiality constraints.

To add this objective with traditional developments of clouds lots of work had been done by the researchers. Most common situation faced by these organizations is multi-tenancy. It is problems here the users accessing their common or shared records form the different locations to some shared servers or data centers. It involves the risk of information dissemination. Here the attacker or some unintended user might disrupt their communication or might affects their data. It causes the compromises and gets reduction in trust towards cloud based applications.

Many security fears associated with cloud computing therefore revolve around incomplete isolation of these myriad users. Large category of cloud security research has therefore concerned the enforcement of various forms of data access control in clouds. The standard way to protect confidential data is (discretionary) access control: some privilege is required in order to access files or objects containing the confidential data [4]. Access control checks place restrictions on the release of information but not its propagation. Once the information access of contents gets open for attacker than some other changed information or denial request can be flowed in later communication causes assets damages for organizations. Thus the objective with the work is:

"To ensure that information is used only in accordance with the relevant confidentiality policies, it is necessary to analyze how information flows within the using program."

Most the traditional security generators beliefs that the system is secure if the data is get converted to some encrypted content for achieving the confidentiality. But its flow towards various system modules and zones of information access should also be considered. Confidentiality policies must be enforced to data as well as their information flow path also. The security analyst must control the flow of information through some confidentiality and integrity policies and should restrict their movements towards location which violates their rules or provisions.

It is the best way to achieve the system design principle of end to end construct. Some of the researchers had made the secure programming languages which restricts the motion or flow of data according to strongly typed methodologies. Mainly, they have some policy based annotations which can be readout by the compilers and termed as security type checking for internal information flow to achieve complete isolation of data and their users. It provides a suitable tracking data flows across different services offers the cloud provider a way to log sensitive operations on tenant data rigorously, thus improving accountability.

A. Labeling [5]:

Information flow control is a data oriented approach works towards achieving protection of internal flowing information

through security labels which tracks and limits the data flow and transitions. Here the labels are associated with the primary functionality of the developed system. It defines the provisions for permitting the secure exchanges of information based on some trust relationship between the labeled data and their requesters. That is, data protection policy checking can be based on comparing the labels associated with the data with the labels held by principals. Example: permitting unprivileged users to pass information to privileged users, but not read privileged information (so-called no read up, a write down") with matching restrictions on the privileged users.

It can be further extended to forcefully apply the general provisions of security through appropriate labeling and verification schemes. All its aims are to providing stronger defense than the formal once applied with DAC. Labels are mainly used to classify the data units flowing between the multiple system modules to identify the flow which is following the constraints of security towards integrity and confidentiality. Here the integrity provides the quality of data and confidentiality serves the security. Secrecy concerns where data is permitted to flow to, and integrity where it is allowed to come from. FC implementations must ensure that labels can be allocated to principals but not be forged by them, can be allocated and "stuck" to data, and that label checking enforces security policy regarding all aspects of information flow.

B. Labeling With Privileges:

A system of privileges operates to introduce carefully controlled additional components into the Trusted Computing Base that can modify labeling contrary to the default restrictions. The privilege to override "secrecy" FC restrictions is known as the declassification privilege. In this case, FC labels such as public, secret and top-secret would be associated with data items and principals and used to enforce the required security policy.

C. Criteria for Implementing FC:

Cloud computing has particular needs in terms of information flow security. Here possible requirements for two cloud-hosted, interacting applications. Data isolation must be provided between compartments of the applications, and data flows tracked and/or enforced on input, output and inter-compartment and application communication [6]. It can be achieved by using following four criteria:

1) When the system operates, (static, runtime, hybrid)
2) How the system isolates data, (e.g. hardware-assisted OS and virtualization mechanisms, programming language and library mechanisms)
3) How the system tracks data flow across isolated data, (e.g. domain level, process level, variable level, message level) and
4) How the system uses the output of data flow tracking to enforce data flow (how policy is specified, the structure of label metadata, and the declassification of security data)

Security engineering involves tradeoffs between security and efficiency. The designers of FC systems will select their threat models to inform any compromises they need to make within the FC design space.

III. LITERATURE REVIEWS

During the last few years various authors had suggested several modifications in traditional information flow control models. Out of those soma had worked towards achieving it a specific way to improve its performance factors and reduces overheads would be taken here as literature survey.

In the paper [7], information flow control for objects and subjects are used to prevent the data dissemination of data using conflicts of interest (COI) phenomenon. Here the developed mechanism will improve the prior existing Chinese Wall Security Policy through levels wise separation of the industrial usable data. The highest level consists of conflict of interest classes which group all company datasets whose companies are in the competition together. All the subjects are allowed to access their data according to their interest. The paper resolves the specific issues of side channel vulnerability by its constrained regulations. Although efficient prevention of side channels is difficult within a single node, there is a unique opportunity within a cloud. This paper proposes a low-overhead approach to cloud wide information flow policy enforcement through CloudFlow information flow controlling tool. The approach identifies the side channels which could potentially be used to violate a security policy through run-time introspection, and reactively migrating virtual machines to eliminate node-level side-channels.

In the paper [8], a decentralized information flow control (DFC) is suggested for improving the programmable writing of security controls. Here the DFC runs on shared hardware and categorizes into language level and operating system. Traditionally the language level DFC does not guarantees the security flows violations. Similarly the operating system based approaches are sometimes do not gives effective security in case of shared resource and fine grained access. This paper gives an approach Laminar for flow control using set of abstraction for operating system and heap allocation policy based other objects. Here the programmers are defining these security labels which cover the aspects of both confidentiality and integrity both. Laminar enforces the security policies specified by the labels at runtime and limits dynamic security checks using the DFC. It also supports the multithreaded monitoring model using heterogeneous labeling process.

Some of the papers also showed the cloud based flow control using some virtual machine monitoring and controlling functions. In a way to do so, the paper [9] gives a administrative approach using the hypervisor process controlling and named as H-One. It is a new auditing mechanism which uses information flow tracking for effective privacy preserving solutions in cloud environments. The tool aims towards recoding all the types of flow starting or goes with the installed VM. Currently the H-One is working with the Xen hypervisors which will be extended for others also. The administrator has root privileges on the management stack and thus has the ability to use all privileges conferred on the administrative VM.

Some of the authors first led the basic understanding of all the cloud security controls which helps in further modification with traditional solutions. Once the clear and separated security requirement gets finalized the solution developments can be performed. The paper [10] provides a concise but all-round analysis on data security and privacy

protection issues associated with cloud computing across all stages of data life cycle. It also addresses the major problem with cloud security handling is multi-tenancy. Now for achieving the complete isolation between its multiple users and applications various factors are analyzed such as scalability, massive processing, service delivery model, sensitive information, virtual resource sharing etc.

In the paper [11], a distributed model for fine grained information flow control is presented which allows dynamic delegation and the revocation rights. The paper uses the defined Haskell libraries for such integrations for decentralized label allotments with individual integrity and confidentiality policies. It is a language based model which includes first-class references, higher-order functions, declassification and endorsement of policies, and user authority in the presence of global unrestricted delegation. The DLM allows each resource or collection of resources to be managed by a different principal. This principal owns the resources: it specifies the security requirements via a set of policies and is responsible for enforcing them. Here the policies use a label consists of exactly two policies: a confidentiality policy R and an integrity policy W. Integrity policy express which principals "trust" the data. Thus, dual to the ordering on confidentiality policies, an integrity policy that states that everyone must trust the data is the most restrictive, and an integrity policy that requires no one to trust the data is the least restrictive.

In the paper [12] a information flow model based on Chinese Wall policy is used to protect the sensitive information. It is a kind of information disclosure policy with effective processing of information belongings to various organizations. Here the companies are gets separated according to their conflicts of interest classes based on their service types. The major components of the approach are query processing in cloud having CQL based executions. The paper suggests following functionality like multiuser server with specialized authentication, replicated query processing, trusted schedulers and operators, security level aware window and other options, unauthenticated flow categorization and blocking etc.

The paper [13] presents IFDB based database managements system which provides security to the decentralized flow control using query label monitoring. It uses a novel abstraction of relational query based handling of flows. As the labeling and tagging is the first step for traffic and flow type detection. In this step an identifier is attached with the flow which defines the sensitivity of the data flowing between the systems modules. Here the labels are the set of tags that summarize the sensitivity of the information contained in the data. Controlling Information Flow IFDB ensures that the label of each object reflects the tags of all the data that produced it, and the label of each process reflects the tags of all the data the process read. It does this by enforcing the following standard rule. The Principle of Least Privilege Delegation of authority makes it possible to define who can declassify, but it doesn't constrain how that authority may be used. At the evaluation points of view it is found that the IFDB reduces authority closures and calls. It gives good throughput for complex systems based applications when tested.

In the paper [14], a traffic classification technique is well studied with some state of art modification is suggested for further improvements. It aims towards improving the current flow structure with statistical feature analysis using machine learning techniques. In this the classification performed is affected by the limited supervised flow of the system information. For effective classification a new method of handling and tagging the unknown application data is given with the paper also. The suggested method uses supervised information training the superior capability of detecting unknown flows generated by unknown applications and utilizing the correlation information among real-world network traffic to boost the classification performance.

IV. PROBLEM IDENTIFICATION

Information flow is the behavior analysis process for flowing data between the various system components or between other systems. Currently there is various solution of this effective flow analysis is suggested for both single and distributed systems. Also the market oriented computing with cloud deployments will face the isolation issues majorly with shared resources. In this situation, categorizing the data from different sources according to their sensitivity of information is a quite complex task. Here the user outsources their data to any third party provider far apart from their trusted zones. Now if some user intentionally tries to fabricate this information at provider's location, trust on the system gets reduced and losses occur. In this situation various flow based labeling and tagging approaches suggested over the last few years are used for isolating the traffic. But in case of cloud the similar types of virtual machine will generate same traffic and it is very tedious task to separate such traffic. Even though some of the problems which remain unaddressed is found out during the survey. These problems are given as:

1) Simultaneous multiple virtual machine access to the same system might not be separated because the labels assigned with that will be same and hence isolation violates.
2) Information flow security policy for infrastructure based outsourced environment is not yet achieved effectively.
3) The decentralized solution of flow analysis and distributed approaches suffers from over labeling and under labeling. There is no such process which gives the exact labeling requires. If the information flow transits from multiple level of VM's and physical machines and then through network, the single data is gets overloaded with multiple labels and makes the degradation in systems performances.

Apart from the other issues which this work had identified there are various direction available in the literature for improving the classification of flow and their filtering mechanism. But somehow, it's a wide area and the work needs to restrict itself to achieve the time based goals. Hence to works aims towards improvements in distributed information flow control (DFC) for cloud computing.

V. OBJECTIVES OF WORK

This works aims towards developing some new security controls for information flow in cloud based environments. It verifies the requirements first to serve the dynamic information flow control both at the pipelines and programming level of system. The process first categorizes the data and later on by effective labeling and partitioning of

data into various classes the information isolation can be achieved. Some of the defined direction of work is given here are:

- Before applying the information flow model for cloud first the service models where the flow analysis is required needs to be indentified first. Normally the infrastructure is analyzed first then platform and later on software.
- Policy formation must be clearly defined along with the entities of the system and their privileges for accessing the flow.
- Policy enforcements and flow analysis using labeling does not affects other process of the system by which degradation in performance can be avoided.

VI. PROPOSED SOLUTION

This work proposes a novel mechanism for getting the better performance and flow security for cloud computing. Mainly the cloud is having the services offered by third party locations to the users as per their requirements and the systems. Information flow control (IFC) will handle the sensitivity of the information along with the protection of its Meta data with a secure flow pipeline between the subject and the object. Flow is the order and the path of information for maintaining the communication between the various entities of the cloud service provider and the requester.

Apart from the flow control the suggested mechanism is capable of achieving the isolation and robustness against the various security primitives. Flow of information in some authentication mechanism will further provides the access control and maintains the security with similar groups. The sharing of data and other resources must be managed effectively maintaining the confidentiality and integrity of the data. This secure information flow model follows the set of guiding rules for monitoring the traffic flows. The traditional concept of Chinese wall security is completely followed here with some more rules for further improvements.

Cloud is the medium which provides various computation and system processes as services to end users through remote medium. With increase in number of interacting devices, components, entities and the users are large in case of outsourced cloud computing, thus the flow of information is not controlled with security point of view. Such heavily flowed traffic generates the problem associated with isolation and sensitivity of intermediate data. The system starts operation with registering the user as tenant with the providers. Each user access its services for a different span of interacting time span for which an individual object is created. Each object must belong to the class whose data access nature and sources are common. Now, as an entity of the cloud, subjects will serve their resources to other entities by further spreading their objects boundaries.

Each object of the subject will have permission or privileges with respect to that only the information up to a certain level of sensitivity is accessed by the user. Thus, a sharing of information will only be allowed for same group objects. The rules are maintained by the security administrator as its controlling part.

Other than security rules, the administrator can also add, modify or delete rules and classes based on the conflicts of interest factors. Primarily the user's data is classified into various groups and usage behaviors.

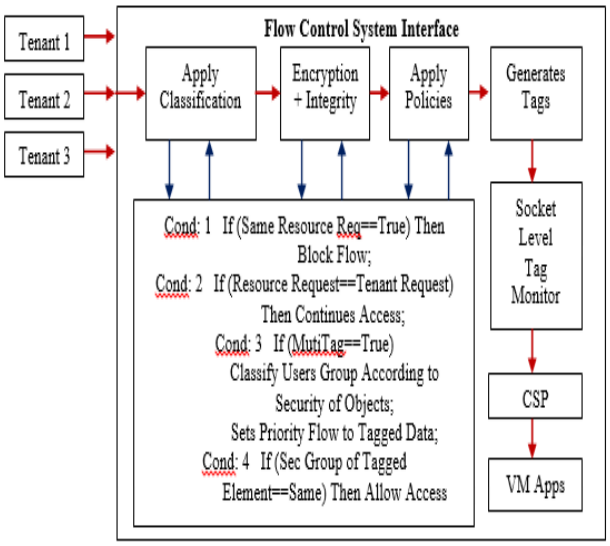


Fig. 1: Proposed Flow Control Using Tag Based Filtration.

When the data enters into system or when a request of data access is generated the classification rules and the filtration policies are applied into the system by information flow modules of infrastructure as a service layer. For maintaining the flow the system is working in different stages starting with classification, encryption/ integrity, policy applicability, tagging, socket level analysis, VM creation and rule mapping.

The proposed flow control system will applies the security constraints on the data to create a sensitivity level access. At the initial level for maintain the users behavior towards the traffic flow patterns and other entities we are applying the tagging. It will also maintains the data that is previously tagged with multiple labels than, they all are removed and which later on applies a unified tag by which overall security interpretations can be made. The module also adds the tags form the traffic and separates them accordingly. This separation of object based data is done in multiple classes formed according the properties of their subjects and actions of creators.

These classes are security groups sharing common data and sources or devices. With cloud environment, the VM instance regularly monitors the types of information flowing from the VM to the provider or the users. If the flow violates the security rules, such data dissemination is blocked. After all the rules are satisfied then only the requester gets the data access accordingly. Flow can be in between various cloud providers and users makes the system operation very complex.

Thus the rules which forces the security operations gets reduced and simplified with a unique rules formation to direct further flows of traffic.

VII. RESULT EVALUATION

Cloud computing is an advance new technique, that uses higher computational power and improve storage

capabilities. Cloud computing is a new processing idea in which computer processing is performed in the network, so that users need not concern themselves with the processing details. Cloud enables flexible computing which is impossible with existing system. To preventing the system from outside world, so that no one can damage or change the system and system can serve its services continuously. With this work the aim is to improve the existing fault tolerance mechanism which is capable of reducing the system overheads and provides the security solution. It must assures the data isolations using compartmentalization and flow is tracked using the identifying their priorities based on scheduling tags.

It can be implemented using some of the parametric evaluation criteria's. It shows the operating condition of system as static and dynamic. The isolation here is achieved using the virtualization phenomenon of cloud computing. For deciding the flow of information between the internal components of the system then it must have track of data accordingly like domain level, process level and message level. Security engineering involves tradeoffs between security and efficiency. The designers of FC systems will select their threat models to inform any compromises they need to make within the FC design space.

The most damaging aspect is the loss of data and software. Some of sources for damaging or harming the systems are computer viruses, computer hacking and denial of service attacks, have become more common. Some of the damaging aspects are intentionally performed by which the system gets threatened. Any security mechanism implemented for cloud must have some control on the flow of the information passing out between the different components of the system. Also the cloud is serving the services out of distributed environment thus maintaining their records for them are again a typical task.

Now this dissertation implemented the proposed concept which improves the flow controlling using different tagging system. Now the question arises how to evaluate the suggested approach. As it was only implemented for single cloud thus for making the comparison it faces some complexities. Also during this work no such practical implementation of any other tool is made available during the research. Still some factors which are showing the effectiveness of the tool is covered here as analytics factors. But still there is some process which needs to be verified using these evaluation parameters.

A. Parameters of Study:

The parameters are given as:

- Authorization Time: It is the total time used to categories the traffic; apply tags and sensitivity analysis along with group cluster matching. Here the average authorization of processes or system modules per unit time for total number of security groups is verified.
- Memory Utilization: It gives the usage habits for executing the flow control application on cloud. For outsourced environment the resources are distributed over the channel. It only measures the total memory require for holding the tagging verification and applying process.
- CPU Utilization: It shows the number of processing cycle requires per unit time for separating, reading or writing each tag according to sensitivity model and rules.

Now, once the user gets authenticated and monitored using the given tool, further analysis can be presented. Each user is capable of serving some of the services selected by him.

S. No	User Name	Cloud Tool	CPU Utilization	
			Before	After
1	User 1	Aneka 2.0	42%	22%
2	User 2		27%	20%
3	User 3		19%	10%
4	User 4		47%	41%

(a)

S. No	User Name	Cloud Tool	RAM Utilization	
			Before	After
1	User 1	Aneka 2.0	59%	42%
2	User 2		52%	48%
3	User 3		47%	42%
4	User 4		42%	38%

(b)

S. No	User Name	Cloud Tool	Page Faults	
			Before	After
1	User 1	Aneka 2.0	30%	29%
2	User 2		28%	26%
3	User 3		26%	24%
4	User 4		24%	23%

(c)

Table 1: User wise Utilization Statistical Analysis (a), (b), (c)

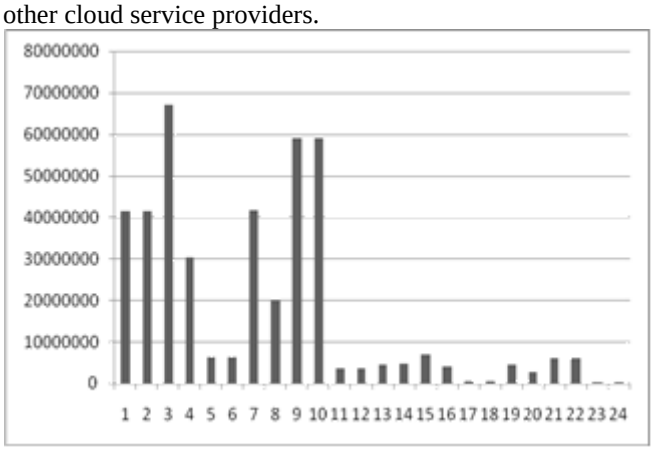
Now when the user gets some service registered starts using it the resource starts working and their allocation statics are figured out. If the process having less requirements and occupies high resources then it could be terminated. This decision is only taken after monitoring the complete allocation and service management process. This feature is uniquely provided by the developed tool only.

User	Service Name & ID	Priority Class	Tags	Physical Memory Usage	Authorization Time	Status
User 1	Service 1 (6020)	Normal	No Tag	41549824	01:39	Started
		Moderate	Med/LIFO	41550080	01:37	Allowed
	Service 2 (9836)	Normal	No Tag	67092480	00:04	Started
		Low	Low/FIFO	30326528	00:96	Suspended
	Service 3 (1696)	Normal	No Tag	6266880	00:06	Started
		High	VeryHigh/SJF	6267136	00:06	Direct Access
Use	Service	Normal	No Tag	41623892	01:38	Started

r 2	1 (1524)	Low	Low/FIFO	20157896	01:68	Suspended
	Service 2 (6235)	Normal	No Tag	58974525	00:04	Started
		High	VeryHigh/SJF	58992453	00:03	Direct Access
	Service 3 (2458)	Normal	No Tag	3589741	00:07	Started
		Moderate	Med/LIFO	3590452	00:06	Allowed
User 3	Service 1 (6542)	Normal	No Tag	4567893	01:49	Started
		Moderate	Med/LIFO	4575452	01:38	Allowed
	Service 2 (4251)	Normal	No Tag	6852436	00:06	Started
		Low	Low/FIFO	4023568	00:94	Suspended
	Service 3 (6398)	Normal	No Tag	358974	00:05	Started
		High	VeryHigh/SJF	348962	00:04	Direct Access

Table 2: User Tags Allotment and Evaluation on Performance Factors

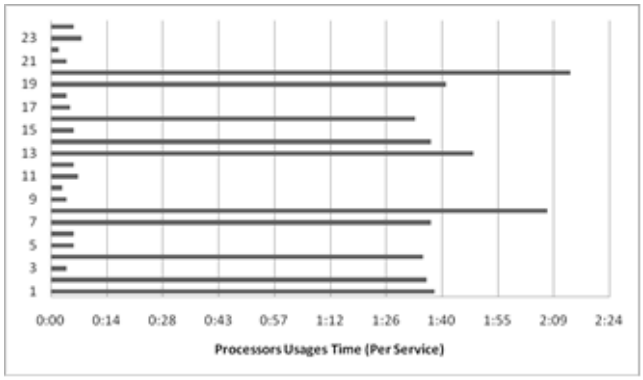
From the statistics of table, by comparing the Aneka Services user tags allocation it is found that the service works on different resources which are callable and dynamic in nature. Getting the distributed control on the information flow somewhere the systems performance is compromised but in terms of the security its robustness gets highly increased. Services, one can easily analyze that in the Aneka 2.0 cloud services, the CPU Power Usage saves with 7.3% and Memory Usage save with 27.2%. Aneka service gives Better performance than any other existing tool for the same working scenarios. Result shows that IFC algorithm cloud performance based on CPU and memory usage is better than other cloud service providers.



Graph 1: Tags Analysis on Physical Memory Usage for User: 1-Service: 1

B. Graph Interpretation: (Graph Wise):

Similar graph can be plot for different combinations of Tags, Users and there selected services.



Graph 2: Tags Analysis on Processor Time (Utilization) for User:1-Service:1

VIII. CONCLUSION

As Cloud computing is getting popular day by day, Cloud service providers need to update their systems with the policies which may lead to better performance as well as flow control. Cloud computing is growing in the companies and individuals because of its characteristics and cost effectiveness. Enormous amount id flowing from the user to CSP and vice versa. There a strong need of flow control mechanism which can have great control over the information, our work introduces a novel tag based information flow control policy governed by predefined rules.

Our work opens a new area of research in access control fro cloud computing moreover any strong encryption policy can also be incorporated to make the system more secure.

REFERENCES

[1] Daniel HEDIN and Andrei SABELFELD "A Perspective on Information-Flow Control".
[2] Mingsen Xu "Mandatory Flow Control Models" power point.
[3] Vasilis Pappas, Vasileios P. Kemerlis, Angeliki Zavou, Michalis Polychronakis, and Angelos D. Keromytis "CloudFence: Data Flow Tracking as a Cloud Service".
[4] Safwan Mahmud Khan, Kevin W. Hamlen and Murat Kantarcioglu"Silver Lining: Enforcing Secure Information Flow at the Cloud Edge"
[5] Andrew C. Myers Barbara Liskov "A Decentralized Model for Information Flow Control"Symposium on Operating Systems Principles, Saint-Malo, France, October 1997.
[6] Andrei Sabelfeld and Andrew C. Myers "Language-Based Information-Flow Security" IEEE Journal On Selected Areas In Communications, Vol. 21, No. 1, January 2003
[7] Mirza Basim Baig, Connor Fitzsimons, Suryanarayanan Balasubramanian, Radu Sion, and Donald E. Porter"CloudFlow: Cloud-wide policy enforcement using fast VM introspection"
[8] Indrajit Roy Donald E. Porter Michael D. Bond Kathryn S. McKinley Emmett Witchel "Laminar: Practical Fine-

Grained Decentralized Information Flow Control" in ACM 2009.
[9] Afshar Ganjali, David Lie "Auditing Cloud Administrators Using Information FlowTracking" in ACM 2012.
[10] Deyan Chen ,Hong Zhao"Data Security and Privacy Protection Issues in Cloud Computing"2012 International Conference on Computer Science and Electronics Engineering
[11] Doaa Hassan , Amr Sabry "Encoding Secure Information Flow with Restricted Delegation and Revocation in Haskell" in ACM 2013.
[12] Xing Xie, Indrakshi Ray, Raman Adaikkalavan"Information Flow Control for Stream Processing in Clouds"in ACM 2013.
[13] David Schultz, Barbara Liskov"IFDB: Decentralized Information Flow Control for Databases" in ACM 2013.
[14] Jun Zhang, Member, IEEE, Chao Chen, Student Member, IEEE, Yang Xiang, Senior Member, IEEE,Wanlei Zhou, Senior Member, IEEE, and Athanasios V. Vasilakos Senior Member, IEEE"An Effective Network Traffic Classification Method with Unknown Flow Detection"IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 2, JUNE 2013.
[15] Lei Mao, Yongguo Yang "Design and Optimization of Cloud-Oriented Workflow System" JOURNAL OF SOFTWARE, VOL. 8, NO. 1, JANUARY 2013
[16] Jean Bacon, Fellow, IEEE, David Eyers, Member, IEEE, Thomas F. J.-M. Pasquier, Member, IEEE,Jatinder Singh, Ioannis Papagiannis, and Peter Pietzuch, Member, IEEE"Information Flow Control for Secure Cloud Computing"IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 11, NO. 1, MARCH 2014

