International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Improved Performance for Secured Authentication in User Devices and Cloud Environment

Veena R.S, Ramachandra V. Pujeri, Indiramma M

Abstract: ***In the last few years, various researchers have identified that securing the cloud environment requires quite a challenging decision to be made as identifying the correct security parameter is difficult. This paper presents" SRAAM: Secure Resource Access Authentication Mechanism", a collaborative framework between user mobile device and cloud infrastructure, for authenticating user and device credentials. An experimental prototype is done for proof of concept and performance matrices are evaluated based on the important decision making parameters. Also, a novel model called as Integrated Framework for Cloud Security (IFCS) that performs mainly three task i) faster and robust user authentication, ii) maintaining anonymity of data storage location, and iii) securing the virtualization platform. An experimental approach is adopted in order to testify the proposed system. Total algorithm processing time in contrast to frequently adopted security protocols in existing system.***

Keywords: Authentication, cryptanalysis, Cloud Computing, Data Access, Cloud Security, Data Security, Access Control, Key Management, Authentication

I. INTRODUCTION

Increasing growth of the user demand has forced the business organization as well as the enterprise to opt for reliable as well as easily expendable infrastructure without incurring large investment and time in order to meet growing user needs. With the emergence of cloud computing, organizations have started using the cloud service due to the vast benefits such as support to move massive data, a large storage place without the need of setting up new infrastructure and the ease of maintenance, high availability, easy scalability and so on. As the technology trend is growing, it is creating a large interest among various enterprises and organization. Cloud computing can be said as a means in which various attributes such as storage, computational power, business process, collaboration infrastructure as well as application are delivered in the form of utility or service that fulfills the user demands [1].

Manuscript published on January 30, 2020.
* Correspondence Author
Veena R.S*, Associate Professor and Head Dept. of Computer Science & Engineering. K. S. School of Engineering and Management, Bengaluru, India.
Ramachandra V. Pujeri, Director M.I.T College of Engineering, Pune, India.
Indiramma M, Professor Dept. of Computer Science & Engineering, BMS College of Engineering, Bengaluru, India.

With the help of cloud computing technology, users are provided access to, use different devices (such as PCs, laptops, PDAs and smartphones) in order to access programs, perform storage and application development using services that are being provided by cloud computing service providers.

Cloud computing has emerged as a front runner in technology and many experts believe that over the days, cloud computing can reshape information technology [2].

Although cloud computing offers vast advantages, it is prone to security threats. Typical security measures like identification, authentication and validation are no more considered reliable as they fail to provide a robust security against the attacks. Failing to provide security in the cloud computing environment may result in irreversible effect on the user and the service provider. In order to ensure security in processing information, data controllers are to be implemented with a suitable technical and organizational step, to safeguard it against various activities such as illegal access, accidental destruction or modification, illegitimate use and so on. Data stored in the cloud is sensitive and confidential. In order to ensure only legitimate user has the access to the data, a sophisticated access control framework has to be applied [3]. A robust authentication is mandatory need for any access control mechanism. In a cloud environment, authentication as well as access control plays a vital role in maintaining the security of the data as it is accessible through internet. Illegal access to cloud data may result in loss or misuse of the data and may lead to unpleasant consequences. Authentication process is significant feature since access control is basically related to primary characteristic like integrity, confidentiality and availability [4]. Many of the traditional approaches for addressing the privacy related issues are not flexible, in other words these approaches are not sufficiently dynamic. The advent of cloud computing has introduced various forms of services to the users who are majorly benefitted by the mobility of the data [1] [2]. Cloud computing offers a comprehensive virtualization platform that incorporates the data and service pervasiveness to the user irrespective of time and location [3]. One of the biggest benefit offer by cloud computing are i) usage of updated and latest software, ii) enhances IT capabilities at reduced cost, iii) flexible expenditure, iv) 24/7 service availability, v) highly sophisticated collaborative network, vi) reduced environmental impact [4]. At the same time, there are also demerits of cloud computing e.g. i) occurrences of downtime, ii) security and privacy problems, iii) highly prone to attack, iv) restricted control, v) higher dependencies of platform, etc. [5][6]. Out of all the problems, security problems are most challenging in cloud computing and cost collateral and financial damage in data centers [7].

There are 10 major security problems which are still a serious matter of concern for majority of the service providers at present [8] [9]. The first security problem is *data breach* due to massive generation of data that are to be stored in cloud servers. The second security concern is fragile authentication policies, which occurs due to defective design of security architecture of any service structure. The third security threat is compromised interface that occurs due to increasing usage of services from third party software. The fourth security risk factor is misusing the vulnerabilities of the system that occurs due to increasing use of multi-tenancy in cloud. The fifth threat to security protocol in cloud is hijacking user account due to proliferation of common risk e.g. phishing, eavesdropping, spamming etc. The sixth reason of security problem in cloud is internal adversary. Basically an internal adversary is a common and legitimate node in cloud which can suddenly become malicious due to any unknown or intentional reason. Such forms of attacks are highly unpredictable and cause collateral damage. The seventh security problem is known as parasitic threat which is a kind of malicious program (after bypassing the security firewall) that siphon-off the confidential data. The eight security issue is called as permanent loss of data which occurs due to malicious intruders. The ninth security problem is known as insufficient attentiveness which occurs due to less technical knowledge of how to use the services securely. This problem is encountered by the companies who are nascent to cloud technology. The tenth security problem is due to shared technology which is directly pointing to insecure operation by hypervisor. The eleventh security problem is the most famous one called as Denial of Service (DoS) attack. Till date, DoS attack has been known to cause a great loss to many service providers as well as users. The fountain-head of all the problems is the weak user authentication, as it adopts passwords with less strength, inferior / inappropriate key management, imprecise permission policies, defective access control, etc. [9]. It is quite an important for an organization to develop a novel strategy for identity management in order to have better visualization of risk factors involved in cloud usage. Usage of centralized identity management should find a new solution as any breach will cause massive financial damage.

II. REPORTED WORK

This section discusses about the existing research work being carried out on security issues in cloud environment. Our prior review has discussed about the emergence of the security protocol in cloud computing [10], where we have discussed about significant issues and various futuristic cloud-applications, along with its respective security requirements. Our second work has introduced a technique that performs secure authentication in cloud [11]. A technique where the data over cloud is secured using RSA algorithm. The prime idea behind the concept is to resist illegitimate access to the cloud storage. The framework was tested over amazon web services [12]. Technique where the privacy factor was emphasized in cloud environment. The authors have developed a unique search technique for encrypted data. The study outcome was assessed using key size, running time, and size of cipher text [13]. A scheme that focuses on user's interest using proxy re-encryption mechanism [14]. A similar technique by adding extensions to it. The study uses extensive proxy re-encryption scheme to carry out secure encryption of the messages. The contribution of the technique is that the process of key generation is not dependent on any preliminary ciphertext of any receiver node [15]. In this author has presented a technique of data deduplication in order to further strengthen the storage security. In this section, we will further update on the significant work being carried out most recently. We discuss on the research journal paper published between 2015-2016 pertaining to the problems of data security and access policies in cloud. Developed a framework that offers multi-layer data security. The modeling is carried out using business process modeling notation in order to use the data. The technique offers better access control and firewall system followed by potential encryption scheme and intrusion detection and prevention system [19].]. (SRAAM) The author has analyzed the possible threats and attacks in cloud and proposed a solution to reduce attacks. The author has emphasized on authenticating the user during accessing the cloud. It uses Digital ID's of employees to access the cloud in order to restrict the unauthorized access [11]. Designing a flexible Access control Model for the cloud, called category based access control, which is implemented as cloud service that allows the user to define their own security policies and can be refined by the abstract policy defined by the service provider [12]. A work on security of data was proposed an adaptive multilevel security model on the basis of cryptography mechanism which ensures sufficient security for data stored in the cloud [9]. The author has considered various factors like legal, economic, security, confidentiality, interoperability and service quality and suggested mechanism to mitigate challenges related to security, privacy and regulatory. One such analysis was carried out in [6]. Most of the research have emphasized on issues related to storage, virtualization and networks. Authors also identified loopholes in the traditional mechanism and suggested why it does not work well in cloud environment. One advancement in comparison with the traditional mechanism was carried out in [7]. The author has suggested interaction modelling based on trust and recommendation in ubiquitous computing domain, wherein the author has defined an adaptive trust evolution algorithm which dynamically adjusts trust value in accordance to the behavior of entity and thereby reducing human intervention in security management. A secure data accessing method was proposed in [8]. Reviewed identity based encryption as well as authentication using biometric and developed a data access method for cloud tenants. The authors have performed comprehensive analysis of the system in comparison with other mechanism and found it feasible and applicable for cloud tenants. (IFCS). The prior computing models like; Service-Oriented Architecture (SOA), distributed computing, and networking, these are the corner-stones of the cloud computing model [3]. The cloud system addresses the privacy concerns because the service providers can access/upload their data which is in the cloud that could suddenly or accidentally removed or changed posing business trust and legal consequences [4-6].

III. PROBLEM STATEMENT:

Another issue arises in accessing control of resources using user device is that the device is most of the time used only in accessing. These devices are not included in the process of authentication, which also provides the attacker an opportunity to access the system making use of other devices acting as user device.

Major problem encountered in the access control of cloud is the simple single level of authentication which can be easily breached by the attacker. Most of the systems fail to establish a secured connection between the client and the service provider. These systems concentrate only on providing the connection and not much emphasis is given on the security of this connection. Many systems lack the mechanism to validate the authenticity of the device used by the user to perform the access control in cloud.

Majority of the systems use generation of random code for accessing the resources that uses only the user credentials. But in case the attacker knows the credential of the client, can easily access the resources by generating random code using these credentials. In some cases, the operation carried out by the user beyond the privileges also result in security issues. Hence a proper mechanism to define privileges to the client should be maintained and monitored so that an illegal access or activity of an unauthorized client can be taken care. In order to generate a robust and secured code, multilevel cryptanalysis along with different parameters need to be performed as simple cryptanalysis with common parameters can be easily breakable by the attacker. So, there is a need to develop a secured mechanism for access control in cloud environment. Hence SRAAM is proposed to handle these issues. Although cloud computing offers extensive service with an agenda of 'pay-per-use', but owing to pervasive nature of the connectivity offered by cloud, there is always threat of security. In order to resist such potential threat, there has been a dedicated series of research work being carried out in order to address this problem. The previous section has discussed about the most recent techniques for strengthening security features over cloud data centers. However, there are some open research problems that need serious attention. Hence, the existing techniques needs reinvention in its architectural design and implementation strategies which lay more emphasis on securing distributed data storage, user authentication, and cost effective key management. Hence, all the above mentioned points will require a serious revision in implementation strategies. The proposed system therefore presents such a solution that can bridge up the open research issues in the area of data security in cloud.

IV. DESIGN AND IMPLEMENTATION OF THE VARIOUS ALGORITHMS

Simple framework that offers higher degree of resiliency against maximum security threat over cloud environment. With an enterprise application designed using Java over Linux machine with eight-core Xeon E5-2680, the proposed system has been assessed. The implementation considers multiple numbers of real-users attempting to access their privilege accounts of data storage in cloud where IFCS is responsible for authenticating the online users before even then can use it. Secondly, once the users are authenticated, IFCS creates multiple data locations using storage container that are distributed over the different data centers itself. It will mean that the file which the user wants to be stored will be stored within this storage container across different data centers. By doing this, IFCS increases the cost of attack for any malicious node even to explore the location of the data. Thirdly, the proposed system has a unique key management system. It introduces a mechanism to generate a secret code which will be used for authentication of the user; however, the novelty is none of the secret code will be seen or accessed or stored even by the user. The user gets them automatically authenticated. The generated keys are further classified into the numbers that corresponds to available number of rack servers. The newly segmented secret keys are then randomly stored in the available servers. Hence, the available servers do stores the chunks of the data based on the container created over them along with the segments of secret keys. But the sequences are maintained in different order for both stored items and segmented keys within the servers.

a. Framework to ensure VM security.

The prime purpose of this stage of the study will be to design a framework that can manage robust security of virtual machine. A consideration is made that one VM intrusion leads to chain of intrusion of other VMs and therefore, the proposed system will work to resist it. The prime functions to be designed in this stage of the study are as follows:

- Profiling multiple VMs: This module will be responsible for profiling different types of VM, which will be broadly classified into i) Regular VM, ii) Compromised VM, and iii) Controller VM. The system will assume that compromised VMs just mimic the behavior of regular VM in order not to get caught. Therefore, the proposed study will develop a novel trust/reputation based algorithm that can map the behavior of VM and finally feed the report of VM behavior to Controller VM, who carry out policy management of different VM and act accordingly to regular or vulnerable scenario.
- Designing of Trust / reputation Algorithm: At a peak load of traffic, it is quite a difficult task to discretize the regular to malicious VM. Hence, before applying cryptographic technique to perform encryption, it is necessary to understand if the situation is really vulnerable. The system will build a trust and reputation of every job being processed by VM and will develop an encrypted report based on it. The encrypted report can be only accessed by controller VM, who will make a decision whether to perform the encryption or not based on positive or negative trust factor.

A. Algorithm for Secret Code Generation

This algorithm is mainly responsible for carrying out secured authentication for any users over cloud environment. Retention of privacy and confidentiality is the core agenda achieved by this algorithm. The step of the algorithm is as shown below:

Algorithm for Secret Code Generation

Input: i_{pswd} (stationary password of user), v (vector for initializing random numbers)

Output: Secret Code (τ)

Start

1. $[i_{psw}] \rightarrow v$
2. $r(x)=[\rho_1\ \rho_2]$ // Define Independent random function

3. $v_1 \rightarrow enc_1(v)^{\rho 1} \rightarrow p_{code1}$
4. $\rho_2 \leftarrow enc_2(p_{code1})$
5. $p_{code2} \leftarrow enc_2(p_{code1})$
6. $p_{code2} \rightarrow [|\ p_{code2}|/2] \rightarrow [\tau_1\ \tau_2]$
7. $[\tau_1\ \tau_2]_{part1} \rightarrow$ *email*
8. $[\tau_1\ \tau_2]_{part2} \rightarrow enc_3 \rightarrow$ cipher_text $\rightarrow$ QR

End

The algorithm considers its input as stationary credentials of users which are normally email id and password. For empirical computation purpose, we consider the input i_{pswd} as vector *v* (Line-1). The next step of the algorithm will be to generate a self-determining arbitrary numbers ρ_1 and ρ_2. (Line-2) We apply three different types of standard encryption algorithm (enc_1, enc_2, enc_3) in three different flows of our encoded data over the cloud (Line-3, Line5, Line8). The study has experimented with multiple versions of secured hash algorithm, message digest algorithm, and advanced encryption standard algorithm. The study uses its first encryption algorithm over the vector in order to obtain a protected code i.e. p_{code1} (Line-3) using the power of first arbitrary number ρ_1. The second arbitrary number ρ_2 is obtained by applying second encryption algorithm on the recently accomplished protected code p_{code1} (Line-5). The accomplished protected code from first encryption algorithm is 512 bits while second encryption algorithm results in new protected code p_{code2} of 128 bit. The obtained p_{code2} is further divided into two parts in random fashion in order to obtain two partial secret codes (τ_1 and τ_2) for further protection against man-in-middle attack (Line-6). One part of the secret code (say τ_1) is forwarded to the email id of the user, while the other part of the secret code (say τ_2) is further encrypted by third encryption algorithm that is secured with a machine-readable data.

B. Algorithm for Secured & Distributed Data Storage

The primary goal of this algorithm is to ensure data security while the secondary goal lies in leveraging the anonymity of the data center location. Although, data center location cannot be intruded much but it is the VM who is directly influenced by the type of the request generated by the user. Protecting VM is quite a challenging task and hence this algorithm ensures that even if the VM is compromised there is no way to get any form of access to the user's confidential data by the intruder.

After the user is initially authenticated by first algorithm (Algorithm for Secret Code Generation), the user is privileged to either access or write over their storage located in distributed rack servers. The algorithm takes the input as a request (*job_req*) which is instantly forwarded to the nearest VM *i* (Line-1). Depending upon the size of the current data, the VM *i* starts looking for the storage from all the available *n* number of rack servers (Line-2). For this purpose, it filters out only the VM whose state is free, which will mean that current job can be stored or processed by that particular rack server (Line-5). The VM starts looking for more number of rack servers and finally record its count as α (Line-6/7). It will mean that α is the total number of servers where the user can fulfill its objective of data storage. Hence, the present data is now stored in α rack servers. Further the system strengthens the privacy factor by introducing a simple technique of random key management. In this, first the VM stores all the data in *α* rack server (Line-10) and then it stores the secret code *τ* over random numbers of *α* rack server. The significant contribution of this algorithm is that it can securely store the file without giving any chances to the intruder to either find the location of storage or even extract the key. It should be also known that one data center may host more than lakhs of rack servers just to understand the minimum range. Hence, it is nearly impossible for intruder to gain an access.

C. *Algorithm for VM Security*

This algorithm is mainly responsible for selection of the most secured VM while performing data storage and accessing by the user.

Algorithm for VM Security

Input: *i* (number of VM), *job_req* (request for job accessing or writing), t_i (trust of i^{th} VM), r_i(Reputation of i^{th} VM)

Output: Validating VM

Start

1. i→validate(job_req)
2. if (job_req=1)
3. *i* accepts job_req
4. else
5. backlist (source(job_req));
6. For i=1:m $\forall m \subseteq i_{ON}$
7. If (t_i<T && r_i<R)
8. i→flagged($Compromise_{VM}$); break
9. i++
10. If ($t_i \geq T$ && $r_i \geq R$)
11. i→flagged($normal_{VM}$)
12. end
13. end
14. Update i

End

Initially, the algorithm checks for the incoming job request for data storage or accessing. This is quite easier to do as the algorithm s required to just validate the original secret code generation and will need to check its authenticity (Line-1). If the job request is found to be validated than only the VM *i* is permitted to accept the incoming request (Line-3) or else it blacklist the IP address of the user's machine that has generated this illegitimate request. The proposed algorithm is also built on the concept of trust and reputation in order to confirm if the selected VM *i* is safe to perform communication with the data centers. We assume that there is a sole Trusted Authority which will be required to be consulted by each VM for evaluating its trust factor. Hence, we don't record any trust value within the VM and it is resided only within the Trusted Authority. We also assume that Trusted Authority cannot be compromised. Hence, once the carrier VM i forwards the request of its trust value, it has to wait until it receives the acceptance from trusted authority. At the same time, the VM i also receives the reputation values from its neighbor VMs. For reliable outcomes, we consider only the VM that has previously forwarded the data securely can only cast their value of reputation. Applying probability theory, we also re-model the entire trust and reputation building model with threshold value based on any specific enterprise application.

We consider both R and T will lie somewhere between 0.05-0.07 to be called as genuine and legitimate VM. If the individual reputation or trust value shrinks down (Line-7), the communication through the selected VM is aborted and soon new VM is searched for selection (Line-9). Otherwise, the carrier VM is flagged as regular VM and is eligible for performing data forwarding.

Figure 1 illustrates the process of client registration on cloud service. Here the client registers by providing the credentials such as username, email and so on which are unique for the client or user. At the time of the registration, the client need to provide the unique device ID associated with his/her device. On successful registration, the cloud performs a secured sharing with the service provider. On completion of the secured sharing, a secured session is established among the client and the service provider via the cloud. Once a secured session is established, two levels of authentication are to be followed to make a mechanism robust.

Hence, the entire three algorithms jointly ensures data privacy, confidentiality, integrity, and non-repudiation.

The next section discusses about the outcomes being accomplished from the algorithm implementation.

b. Design of SRAAM

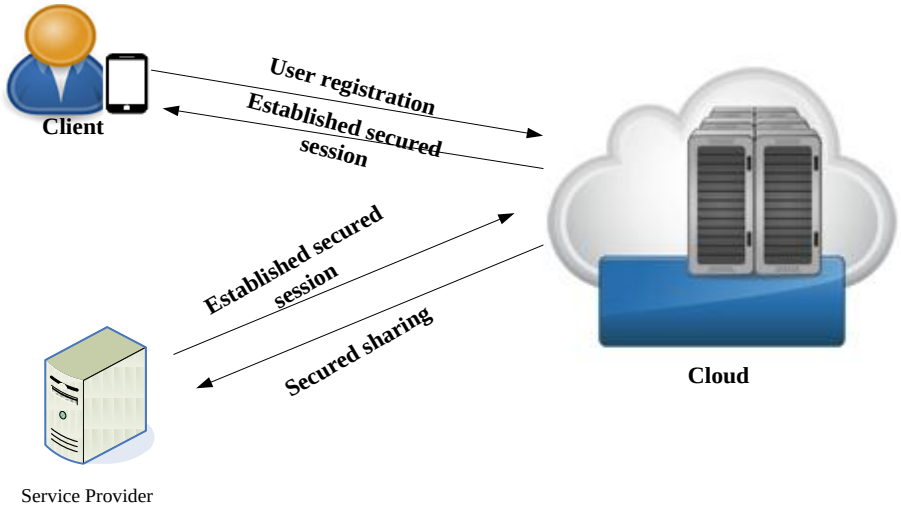

Figure 1: Client Registration

Level 1 Authentication:

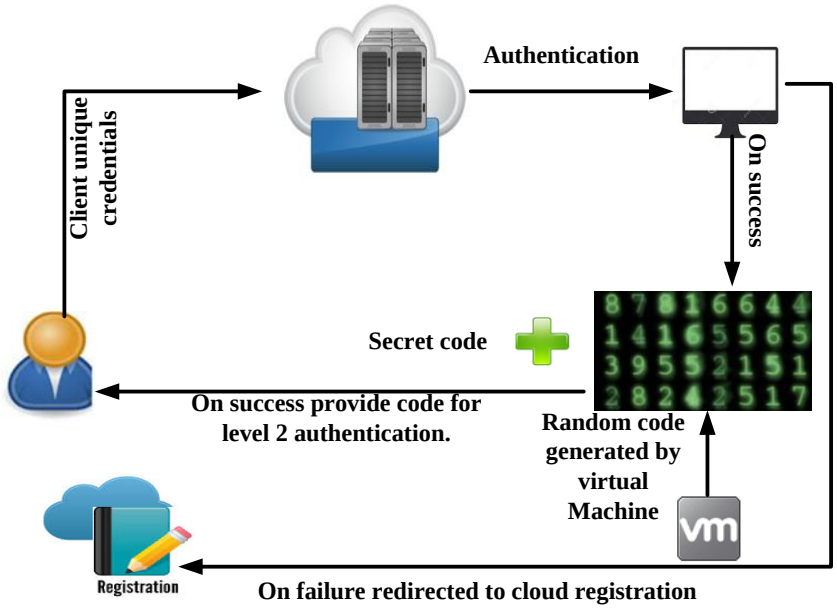

Figure 2: Level 1 Authentication

Figure 2 shows the process of Level1 authentication. Here a secret code is generated using the client's unique credentials as well as the device ID. The advantage of these attributes is the assumption that no two clients or users can have same credentials. Even though they share same credentials, no two devices can ever have same ID.

Hence the mechanism provides a robust security in this case. On receiving the secret code, the process of validation is performed. The validation process checks if the information provided by the user is valid. If it is valid, the unique code for level 2 authentication is sent to the user. Otherwise the user is redirected to cloud registration phase.

Level 2 Authentication:

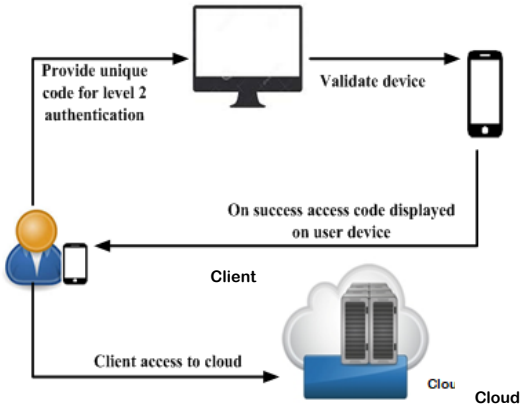

Figure 3: Level 2 Authentication

Figure 3 illustrates the level 2 authentication. Here the unique identification code obtained in level 1 is used. On receiving this code, the system checks for the device authorization i.e it checks if the device is registered or not. This process uses the unique device identification number provided by the user at the time of registration. If the device is registered, the access code embedded within a barcode is visible in the user device. This is done by scanning barcode with application dedicated to decrypt the barcode. Using this code, the user can now have an access to the cloud storage.

On achieving the access control to the cloud storage, it is not mandatory that the user can perform all the activities in cloud storage. The privileges need to be granted to the user in order to perform certain activities. These privileges allow the user to create and manage bucket/folder in the cloud storage. It allows the user to upload different types of files with Multipurpose Internet Mail Extension (MIME) type authorization and even to perform the delete operation. These privileges are set or provided by the administrator who monitors all the activities in the cloud as shown in Figure 4. User privileges are contained in the user profile of respective user or client.

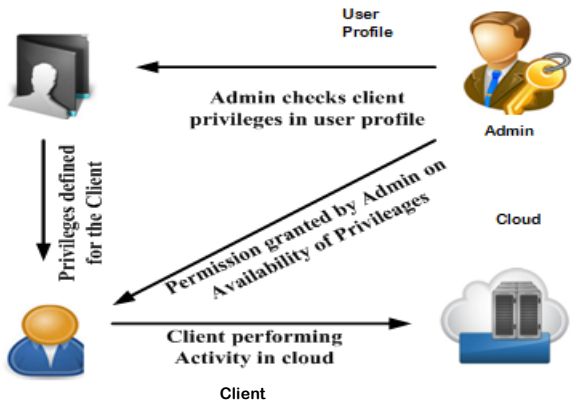

Figure 4: Administrator Privileges

The above process have been developed as an algorithm and it have been implemented for an authentication process. Here the authentication is performed by considering the beta (β) which represents the unique credentials as well as the DID. The virtual machine generates the random code which is illustrated in algorithm. The two levels, high represented by τ and low represented by σ are set for the length of the code. The code generation is based on the Linear congruential formula. The output result Q is a random number denoted by R_c which is later converted into character denoted by ε using ASCII function. Secret code is generated using Rc and secret code input SD_{in}. Here SD_{in} is subjected to hash function and the result of the hash function is a 128 bit (16 byte) value which is expressed in 32 digit hexadecimal number that denotes secret code. Another encryption is performed on inputs DID and SD_{in} that results in 128 bit value. This hash function is denoted by F(x) that result in D-key. Final encryption operation is carried out by g(x) on SD and output of previous encryption function F(x). The result of g(x) encryption also results in 128 bit secret code ED which is embedded within the barcode.

Administration Privileges:

On achieving the access control to the cloud storage, it is not mandatory that the user has been granted with all the privileges to carry activity in cloud storage. These privileges are provided by the Administrator. These privileges allows the user to create bucket/folder in the cloud storage and to manage the folders and files. The different types of files with MIME type authorization can be uploaded and even the delete operation can be performed.

$$\beta = \beta_1, \beta_2, \ldots . \beta_t$$

Where β represents the buckets in the datacenter up to t number of clients.

$C_x \rightarrow \beta_e (_e \in t)$

$U_{ad} \rightarrow \phi\{P_1, P_2, \ldots P_r\}$

If $\acute{\alpha} \subseteq \sum_{t=0}^{r} \phi$

$C_x \rightarrow$ Permission granted

Or else

Permission Denied && Activity Aborted.

Here privilege is represented using P, U_{ad} represents admin. The above algorithm illustrates the privilege management by the administrator. Here the user tries to create a bucket within the cloud. At that instant, the administrator checks the user profile for the information about the permission and grants provided. If it finds that the user has violated the permission, it denies the activity. Otherwise it allows proceeding for an activity. This is applicable to all the tasks and activities such as creating folders, deleting folders, uploading or downloading files and so on.

c. Distributed Framework to Ensure Data Security:

The study deploys a concept where VM plays an important role. Figure 5 highlights the schematic architecture of the proposed system. This part of the study will focus on data security along with various other issues viz. issues pertaining to data leakage, vulnerability of public storage area, and usage of defective encryption policy.

The prime purpose of the proposed system is to design a secure repository and accessible framework in cloud computing that can offer greater deal of privacy, confidentially, and integrity. The main aim will be to design a cloud security architecture which can be developed to maintain the data security of various cloud applications and to authenticate the users from performing any types of illegal activity the objectives of the proposed system are e.g.

- Verification: The system should allow online users to get authenticated and verified by the cloud application interface
- Secure Data Upload: The system should generate a novel mechanism of highly distributed allocation of keys to secure the data which have been uploaded by the genuine users
- Distributed Key Mechanism: the system will provide a distributed key mechanism to secure the uploaded data. The system will provide distributed ciphers for encryption and decryption of the uploaded and downloaded data respectively.

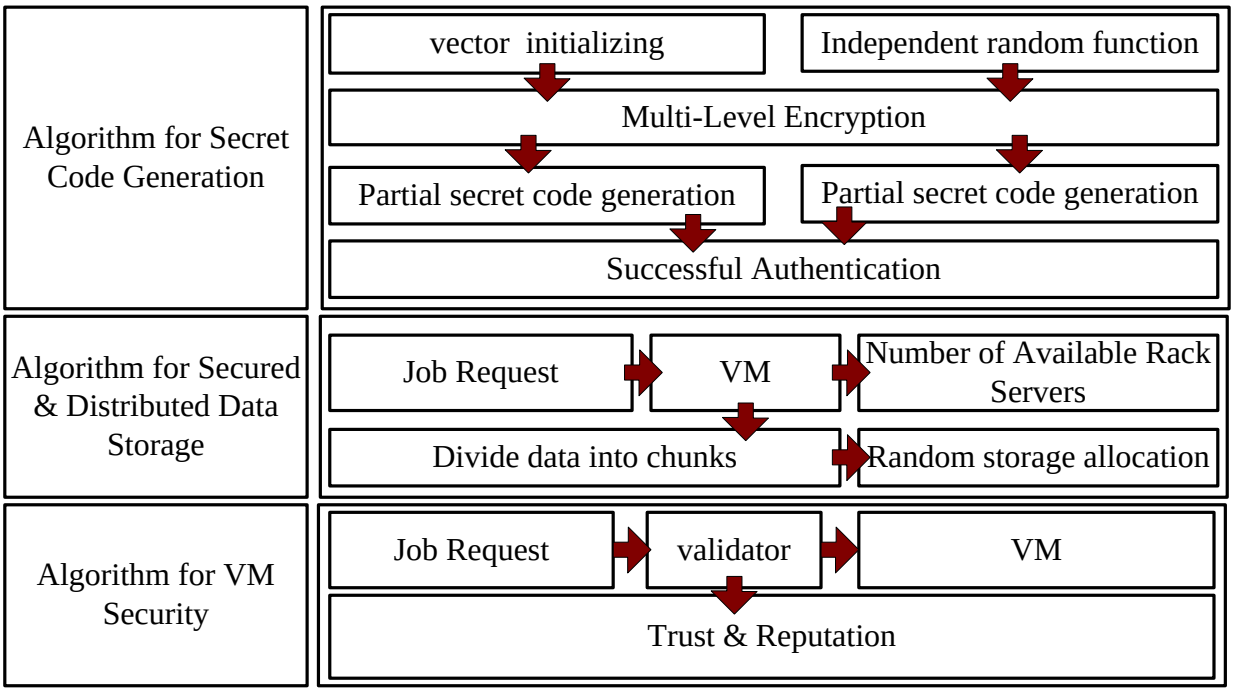

Figure 5: Schematic Architecture of IFCS.

V. RESULTS AND DISCUSSIONS:

This section presents an extensive analysis of SRAASRAAM in comparison with the existing system. A comparative study and analysis is graphically presented with respect to the time and iteration. In comparison with the DES encryption SRAAM is found tp have beter feasibility of Implementation on software. Figure 6 below provides the comparison between SRAAM and DES algorithm and it is evident that SRAAM performs better in terms of computational speed.

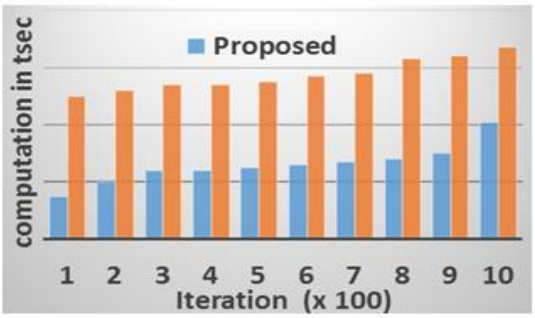

Figure 6: Computational Time Analysis with respect to DES

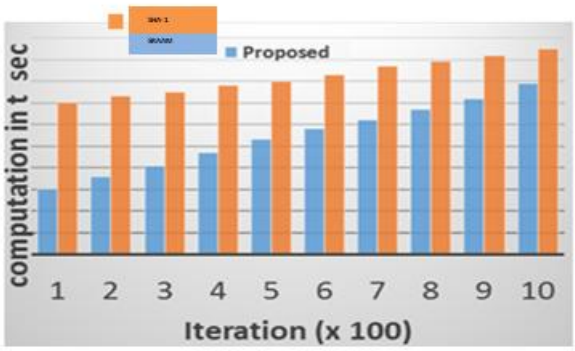

Figure 7: Computational Time Analysis with respect to SHA-1

Figure 7 shows the comparison between SRAAM and SHA-1 algorithm. SRAAM provide a better security feature by generating a secured code in comparison with SHA-1 which itself has been a victim of different attacks in recent past. This section discusses about the results being accomplished for the proposed study.

We explore that various datacenters and cloud service provider uses AES [31], DES [32], RSA [33], and Blowfish algorithms [34] as a means of encryption standards.

Therefore, the outcome of the proposed system has been compared with all these security protocols. As the proposed system is implemented over java, hence programming Java with its enriched security APIs is not a difficult task for implementation. Following are the inferences of the outcomes being accomplished:

Analysis of Time to Generate Secret Code

Time to generate secret code is computed as total time required by the first algorithm to generate secret code for the purpose of authenticating the user.

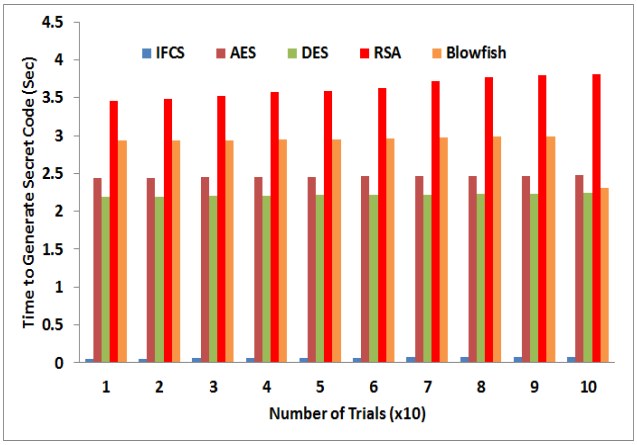

Figure 8 Analysis of Time to Generate Secret Code

Figure 8 shows that proposed system offers approximately 99% of minimal time consumption in generating the secret code as compared to any existing security protocols. The prime reason behind this is majority of the security protocols uses one single key size for carrying out encryption, hence it creates an overhead with increasing number of trails. On the other hand, proposed IFCS has applied variable sizes of keys on different stages of encryption where the key sizes always lowers down. This is one of the significant feature which let IFCS to instantly generate the secret code whereas other existing system takes more amount of time to do the authentication.

The proposed IFCS algorithm has a discrete use of cryptographic hash function in a very simple manner where the spatial complexity of the algorithm is always taken care of by disposing it once it is used. Hence, such lower size of key provides similar level of security what RSA can provide with higher size of key and hence IFCS can be inferred as one of the cost effective algorithm.

Proposed system has faster processing time because the algorithms designed for authentication uses non-recursive functions, lower size of key (64 bit), and faster update operation of key. Hence, decryption step is quite faster than encryption steps and doesn't get affected even if the incoming traffic is increased.

Table 5.1 Comparison Table for the Proposed System.

Algorithms	Processing Time	Traffic Load	Key Size	Time to Generate Secret Code
IFCS	2	10^2	64	0.1
AES	12	10^2	128	2.5
DES	5	10^2	56	2,25
RSA	5	10^2	1024	3.5
Blowfish	5	10^2	128	3.0

Table 5.1 illustrates the performance analysis with respect to the various algorithms and their response time. Our proposed IFCS algorithm generates the secret code in the least time compared to other algorithms. Next is processing time is also reduced to 2times as compared with the other conventional algorithms for the same traffic load. Therefore our proposed method overall performance is improved to 50percentage which is much better than the conventional algorithms.

VI. CONCLUSION

Increased use of cloud computing has given rise to the threats, attacks and unauthorized accessing of data and resources. In order to mitigate these effects, various methods have been proposed. The traditional methods lack the ability to provide the dynamic robustness as well as secure accessing. The SRAAM provides a high level accessing control by making use of two level authentications. The SRAAM also makes use of the user device in the process of authentication which provides additional advantage in mitigating the security issues. The SRAAM is compared with the existing approaches and is found to provide a better and efficient result in terms of robustness and computational time. We hope to use SRAAM to evaluate the overall performance on real workloads.

Security is still an unsolved problem in the area of cloud computing inspite of many number of research papers. Reviewing the most recently published research papers are found to use complex cryptographic protocol that couldn't balance between security and communication. The present paper has emphasized on the multiple-level of user authentication that can successfully maintain both forward and backward secrecy. The novelty of proposed system is its unique manner of generation of secret code which cannot be controlled or governed or manipulated by any user. At the same time, proposed technique provides data anonymity by splitting the data of the user only on the available rack servers. The storage is carried out in a highly distributed manner. The second novelty of the study is also privacy and confidentiality of data by storing the secret key randomly into cloud servers. Hence, such security policy offers a higher degree of security in cloud computing. The study outcome was also found to possess faster response time as compared to existing security techniques is listed on the table5.1.

REFERENCES

1. R. Hill, L. Hirsch, P. Lake, S. Moshiri,"Guide to Cloud Computing: Principles and Practice",Springer Science & Business Media, Computers, pp. 278, 2012
2. B.Furht, A. Escalante, "Handbook of Cloud Computing",Springer Science & Business Media, Computers, pp. 634, 2010
3. S.Pearson, G.Yee,"Privacy and Security for Cloud Computing",Springer Science & Business Media, Computers, pp. 308 pages, 2012
4. N.Meghanathan, "Review of Access Control Models For Cloud Computing", In Proceedings of the 3th International Conference on Computer Science, Engineering & Applications , ICCSEA, P.77, 2013

5. J.Sen,"Security and Privacy Issues in cloud Computing","Innovation Labs,Tata Consultancy Services Ltd,Kolkata,INDIA, Retrived, 26th Sep, 2015
6. Hashizume, "An analysis of security issues for cloud computing",Journal of Internet Services and Application, Vol. 4(5), 2013
7. IItaf ,"Modeling interaction using trust and recommendation in ubiquitous computing environment",Eurasip journal on wireless communication and networking, pp.1687-1499, 2012.
8. C. Rong and H.Cheng, "A secure Data Access Mechanism for Cloud Tenants",Cloud computing the third internattional conference on cloud computing,Grids,and virtualization, 2012
9. S.Devi, Dorairaj and T.Kaliannan, "An adaptive multilevel Security Framework for the data stored in cloud environment".Hindawi Publishing Corporation the scientific world journal, Article ID 601017, 2015
10. Fotiou,"Acess control as a service for the cloud", Journal of Internet Services and Applications, Vol. 6:11,Doi 10.1186/s 13174-015-0026-4, 2015
11. Min,"Cloud computing security issues and Access Control Solutions",Journal of security Engineering,Vol 9, No 2,2012.
12. Khamadja "Designing Flexible Access Control Models for the cloud",ACM, pp. 978-1-4503, 2011
13. Computing", IGI Global Computers, pp. 307, 2016
14. S.C. Satapathy, A. Joshi, N. Modi, N. Pathak, "Proceedings of International Conference on ICT for Sustainable Development: ICT4SD 2015, Volume 2", Springer, pp. 819, 2016
15. S. Murugesan, I. Bojanova, "Encyclopedia of Cloud Computing", John Wiley & Sons Technology & Engineering, pp. 744, 2016
16. Z. Ma, "Managing Big Data in Cloud Computing Environments", IGI Global Computers, pp. 314, 2016
17. L. Fiondella, A. Puliafito, "Principles of Performance and Reliability Modeling and Evaluation", Springer, pp. 655, 2016
18. M. Margarida,Pinheiro, "Handbook of Research on Engaging Digital Natives in Higher Education Settings", IGI Global, pp. 500, 2016
19. Z. Huang, X. Sun, J. Luo, J. Wang, "Cloud Computing and Security: First International Conference", Springer, pp. 562, 2016
20. S.Y. Zhu, R. Hill, M.Trovati, "Guide to Security Assurance for Cloud Computing", Springer, pp. 229, 2016
21. A.a.Saidi, R.Fleischer, Z. Maamar, O. F. Rana, "Intelligent Cloud Computing: First International Conference", Springer, pp. 169, 2015
22. R.S. Veena, R. V. Pujeri, and M. Indiramma, "An Investigation towards Paradigm Shift of Cloud Computing Approach and Need of New Security Protocol", International Journal of Computer Applications, vol. 130, no. 9, 2015
23. Veena R. S. R. V. Pujeri, and Indiramma M., "SRAAM: Secure resource access authentication mechanism using user-device credential hybridiztion in cloud environment", Retrieved, 06th October, 2016
24. N. C. Raj, P. Thenmozhi, and R. Amirtharajan, "Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique", International Journal of Digital Multimedia Broadcasting, pp. 6, 2016
25. K. Liang, X. Huang, F. Guo and J. K. Liu, "Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2365-2376, 2016
26. S. Mang, L. Fenghua, S. Guozhen, G. Kui and X. Jinbo, "A User-Centric Data Secure Creation Scheme in Cloud Computing", Chinese Journal of Electronics, Vol.25(4), pp.753-760, 2016
27. P. Xu, T. Jiao, Q. Wu, W. Wang and H. Jin, "Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email," in IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79, Jan. 1 2016.
28. Z. Yan, M. Wang, Y. Li and A. V. Vasilakos, "Encrypted Data Management with Deduplication in Cloud Computing," in IEEE Cloud Computing, vol. 3, no. 2, pp. 28-35, Mar.-Apr. 2016.
29. K. Yang, Z. Liu, X. Jia and X. S. Shen, "Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach," in IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940-950, 2016.
30. S. Zhou, R. Du, J. Chen, H. Deng, J. Shen and H. Zhang, "SSEM: Secure, scalable and efficient multi-owner data sharing in clouds," in China Communications, vol. 13, no. 8, pp. 231-243, Aug. 2016.
31. V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138-151, Jan.-Feb. 1 2016.
32. Z. Guan, T. Yang, and X. Du, "Achieving secure and efficient data access control for cloud-integrated body sensor networks", International Journal of Distributed Sensor Networks, vol. 142, 2015.
33. L. Li, R. Lu and C. Huang, "EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data," in IEEE Internet of Things Journal, vol. 3, no. 2, pp. 206-218, April 2016.
34. R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 4, pp. 789-798, April 2016.
35. S. Niu, S. Tu and Y. Huang, "An Effective and Secure Access Control System Scheme in the Cloud," in Chinese Journal of Electronics, vol. 24, no. 3, pp. 524-528, 07 2015.
36. H. Li, D. Liu, Y. Dai and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when QoE meets QoP," in IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, August 2015.
37. T. Yang, J. Li and B. Yu, "A Secure Ciphertext Self-Destruction Scheme with Attribute-Based Encryption", Mathematical Problems in Engineering, 2015.
38. K. Li, W. Zhang, C. Yang and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption-Based Cloud Data Search," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1918-1926, Sept. 2015.
39. J. Wang, C. Huang, K. Yang, J. Wang, X. Wang and X. Chen, "MAVP-FE: Multi-authority vector policy functional encryption with efficient encryption and decryption," in China Communications, vol. 12, no. 6, pp. 126-140, June 2015.
40. W. Li, K. Xue, Y. Xue and J. Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484-1496, May 1 2016.
41. X. Yao, H. Liu, H. Ning, L. T. Yang and Y. Xiang, "Anonymous Credential-Based Access Control Scheme for Clouds," in IEEE Cloud Computing, vol. 2, no. 4, pp. 34-43, July-Aug. 2015.
42. H. Zhu, R. Lu, C. Huang, L. Chen and H. Li, "An Efficient Privacy-Preserving Location-Based Services Query Scheme inOutsourced Cloud," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7729-7739, Sept. 2016.
43. V. K. Pachghare, "Cryptography and Information Security", PHI Learning Pvt. Ltd, pp. 416, 2015
44. E.Biham, A.Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer Science & Business Media, pp. 188, 2012
45. H.A.Sulaiman, M.A.Othman, M.F.I.Othman, Y. A. Rahim, N.C. Pee, "Advanced Computer and Communication Engineering Technology", Springer Technology & Engineering, pp. 1090, 2014
46. H. Ibrahim, S. Iqbal, S.S. Teoh, M.T. Mustaffa, "9th International Conference on Robotic, Vision, Signal Processing and Power Applications: Empowering Research and Innovation", Springer,pp. 861, 2016

AUTHORS PROFILE

Veena R. S, has completed her B.E. in Computer Technology from Nagpur University in 1997, her MTech in Computer Science & Engineering from VTU in 2007. She is currently pursuing her PhD in Computer Science & Engineering from VTU, Belagavi. She has total 21 years of experience. Her current research deals with Cloud Computing. She has published more than 16 papers in National and International Conferences and Journals.

Dr. Ramachandra V Pujeri, Received his B E in Electronics and Communication Engineering from Karnataka University, Dharwad, ME in Computer Science and Engg from PSG College of Technology, Coimbatore, Ph.D. in Information and Communication Engineering from Anna University, Chennai, MBA in Human Resource Management, from Pondicherry University, Pondicherry, in 1996, 2002, 2007 and 2008 respectively. He is active life member of ISTE, SSI, MIE, ACS and IEE. He has written three textbooks. He is having around 20 years of teaching experience in the various top ten engineering colleges in India.

He is an active expert committee member of AICTE, NBA, DoEACC, NACC and various Universities in India. Currently, under him ten research scholars pursuing their Ph.D. His research interests lie in the areas of Computer Networking, Operating System, Software Engineering, Software Reliability, Modelling and Simulation, Quality of Services and Data Mining. Currently, he is working as Director of MIT College of Engineering, Pune, Maharashtra. India

Dr Indiramma M, Received her BE in Computer Science and Engineering from PES college of Engineering, Mandya in 1988, ME in Computer Science and Engineering in 1999 and PhD from VTU, Belagavi in 2010. She is having 30 years of teaching experience. Her research areas are Cloud Computing, Service Oriented Grids, Artificial Intelligence and Machine Learning Algorithms. She has published more than 40 publications in National, International Journals and Conferences. She is currently working as a Professor and Convener-IIIC Department of Computer Science and Engineering BMS College of Engineering, Bull Temple Road, Basavanagudi, Bengaluru.