**International Journal of Computing and Applications** | **ISSN: 0973-5704**
Volume 13, Number 1, (January-June 2018), pp 63-73
© Serials Publications, New Delhi (India)

# IFCS: INTEGRATED FRAMEWORK FOR CLOUD SECURITY FOR ENHANCED DATA AND VM SECURITY

**Veena R.S.[1], Ramachandra V. Pujeri[2] and Indiramma M.[3]**

[1]*Associate Professor, Department of Computer Science & Engg. K.S. School of Engineering & Management, Bengaluru, India*
[2]*Vice Principal, M.I.T College of Engineering, Pune, India*
[3]*Professor, Department of Computer Science & Engineering, BMS College of Engineering, Bengaluru, India*

***Abstract:*** Although cloud computing has paved the progressive path by its technology and highly pervasive service delivery, yet it still suffers from the set back of some serious security problems. We reviewed the most recent research work towards addressing security problems and found that existing techniques are shrouded with open research issues. Hence, this paper introduced 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. The study outcome of IFCS was found to excel: The time to generate secret code, key size used for final encryption, total algorithm processing time in contrast to frequently adopted security protocols in existing system.

***Keywords:*** Cloud Security, Data Security, Access Control, Key Management, Authentication.

## 1. INTRODUCTION

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.

Therefore, this paper presents a novel framework that mainly addresses the problem of data security and thereby strengthen the access policy in data centers. Using simple cryptographic protocol, the proposed technique maintains a good balance between security and communication performance. Section II discusses about the most recent research work addressing the security problems in Cloud, followed by brief discussion of problem identification in Section III. Proposed system and its contribution is briefed in Section IV, followed by illustration of adopted research methodology in Section V. Algorithm implementation is discussed in Section VI and result discussion is carried out in Section VII. Finally, the contribution of the proposed system is briefed in conclusion in Section VIII.

## 2. RELATED 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]. 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.

Chidambaram et. al., [12] have developed 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. Liang et. al., [13] have presented a 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. Mang et. al., [14] have developed a scheme that focuses on user's interest using proxy re-encryption mechanism. Xu et. al., [15] have presented 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. Yan et. al., [16] have presented a technique of data deduplication in order to further strengthen the storage security. Yang et. al., [17] have introduced a technique of secure access control over the multimedia resource sharing over the cloud environment. The authors have used encryption on the basis of attributes considering time domain analysis. The technique has also presented a novel attribute management mechanism for securing the multimedia content over the cloud. Zhou et. al., [18] have addressed the security problems of data sharing in cloud. A unique homomorphism technique which uses key-ciphertext has been deployed in order to ensure resistance to the illegitimate access from the intruders.

Chang and Ramachandran [19] have 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. Study towards secure access control was carried out by Guan et. al., [20] where encryptions based on attributes was used for carrying out security measures in cloud. The technique uses digital signature to secure the plaintext in order to store the signed data in the servers. An author has implemented a secured authorization policy that let each user to carry out validation during any form of communication in the cloud environment. The study outcome was evaluated with respect to the time to generate key, time to perform encryption and decryption, as well as overall computational time. Li et. al., [21] have investigated about the privacy problems in pervasive computing. The authors have developed a tree structure that can maintain privacy preservation. Chen et. al., [22] have presented a technique that uses public key cryptography for rendering security over cloud storage system. According to the authors, the existing keyword search techniques using public key cryptography fails to resists against guessing attack. The technique uses homomorphic encryption along with hash function to further leverage the encryption. Shaozhang et. al., [23] have also presented an attributed based security scheme over cloud. The technique uses bilinear mapping to carryout key generation process. Li et. al., [24] have discussed about quality of experience as well as quality of protection for mobile cloud networks. The authors have developed a scheme that can perform data search with higher granularity and is affected by accuracy of search, efficiency of search, dynamic search, personalized search, etc. Yang et. al., [25] have presented nearly similar line of research work using attribute based encryption using distributed hash table. The technique has targeted against cryptanalysis-based attacks e.g. Sybil attack.

Study towards privacy preservation is again being carried out by Li et. al., [26] in order to resist differential attack on cloud. The authors have developed a searching model to discover plain text as well as ciphertext along with enhancement to conventional order preservation encryption technique. Jing et. al., [27] have presented a technique that uses the concept of functional cryptography in order to address the problems of privacy policy. The authors proposed its solution using multiple authority vector schemes that furnishes a latent policy of accessing the encoded matrix. Another attribute-based scheme was presented by Li et. al., [28] addressing the problems of multiple authority access control. The authors claimed that prior schemes of multiple authorities consider only one authority for maintaining the complete attribute that seriously degrades the communication performance and security at same time. This problem is overcome by introducing multiple authorities that together manages the consistent set of attributes. Its system model was designed using certificate authority, attribute authority, data owner, cloud server, and data user. Yao et. al., [29] have presented a unique scheme of access control in order to maintain an effective anonymity in the cloud. The technique has used hash message authentication code along with digital signature. The key management scheme comprises of key generation, key distribution, and key updating followed by authorization. The study outcome was assessed for overhead, scalability, and accountability. Zhu et. al., [30] have presented another privacy preservation scheme that outsources the location-based services to cloud after carrying out encryption. The technique has used enhanced version of homomorphic encryption approach and was assessed using experimental approach. The study also uses bilinear cryptographic pairing in order to secure the queries and response generated by location based services. The study outcome was evaluated with respect to computation cost involved in all the major modeling used in the study.

Therefore, it can be seen that there are many research work being carried out towards securing cloud data. The most frequently adopted schemes are attribute-based encryption, homomorphic encryption, key management etc. All these schemes have its own benefits as well as pitfalls too. The next section briefly highlights about the issues in existing work.

## 3. PROBLEM IDENTIFICATION

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. Following are the brief of the problems being identified from the existing research work:

- **Less emphasis on user authentication:** This is the root cause for majority of the problems. All the recent research work focuses on privacy preservation and many other such issues; however less emphasis has been given towards user identification. Existing techniques only uses static password with their user identity, which can be forged by any malicious codes. Some of the existing authentication mechanism uses complex cryptographic protocol that doesn't comply with non-repudiation.
- **Fewer studies on maintaining anonymity of data location:** We have existing software framework e.g. Hadoop, Map Reduce which performs distributed data storage as well as processing. However, they are open source and have specific architecture of distributed storage that is not difficult to intrude by even a less-skilled intruder. Existing research work doesn't specify any algorithm that performs autonomous and pattern-less distributed storage. so that location of data chunks is not known even to the service providers. Also, there are only few papers that has discussed about encrypting the data chunks.
- **Few security protocols to run in VM:** The biggest problem with the virtualization is to retain the data replicas and to map with the physical machines. At present, the data are only encrypted in the original storage point and not in the VM. Another significant research problem is that although there is good synchronization among the existing VMs, but at present one VM doesn't authenticate with each other. Moreover there no encryption mechanism that VM should run for live stream of incoming data in order to comply with non-repudiation.
- **Usage of Less effective cryptographic protocols:** Majority of the existing research work as well as real-time service providers (e.g. Amazon) uses Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA (Rivest Shamir and Adelman), Blowfish, etc. All these are quite a conventional security protocol that have already a history of compromization.

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.

## 4. INTEGRATED FRAMEWORK FOR CLOUD SECURITY

The prime purpose of the present work is to formulate a 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. This phenomenon will render near to impossible or may take more than decade just to guess the proper location of chunks of data and segments of secret key in order to access the original data in rack servers. This encryption principle: (i) reduces the authentication delay, (ii) reduces the key sizes, (iii) supports hardware acceleration. These features of encryption will thereby supported by any mobile applications too on any low-powered device with further ability to jointly work with cloud-based applications. The hardware profiles e.g. device identity, user identity. The study contributions of IFCS are as follows:

- *Multiple Layer of Secure Encryption*: IFCS encrypts the message using different types of cryptographic protocol that offers potential security resiliency against maximum forms of attacks. IFCS also offers a novel key generation method to support multiple layer of security.
- *Anonymity of Data Storage*: IFCS proposes a highly secure and distributed data storage mechanism depending on the availability of the rack servers over data centers. It indirectly assists in maintaining privacy of the data storage and anonymity of location of data centers too.
- *Two-Directional Validation*: IFCS provides two directional validations of the job-request as well as virtual machine. It will mean that both of them authenticate with each other to ensure that no malicious code make its way inside the network.
- *Potential VM Security*: A simple authentication model based on trust and reputation is built in order to check the legitimacy of the active VMs before processing the task.

## 5. RESEARCH METHODOLOGY

The proposed study was testified using experimental prototype where the objective was to develop a secure distributed system for carrying out data storage. The study deploys a concept where VM plays an important role. Figure 1 highlights the schematic architecture of the proposed system.

### A. Distributed Framework to Ensure Data Security

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.

### B. 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.

## 6. ALGORITHM IMPLEMENTATION

The design and development of the proposed system is carried out with an aid of three different algorithms viz. (i) algorithm for secret code generation, (ii) algorithm for secured and distributed data storage, and (iii) algorithm for VM security. The motive behind the algorithm is mainly to ensure that a user should be able to carry out secure storage of data by guaranteeing them about the privacy and confidentiality of the data. The algorithm also ensures that it should have enough integrity and non-repudiation features for which reason it implements some of the simple and standard cryptographic techniques that has higher supportability of both forward secrecy and backward secrecy. This section brief about the algorithm design principle with respective to its respective steps.

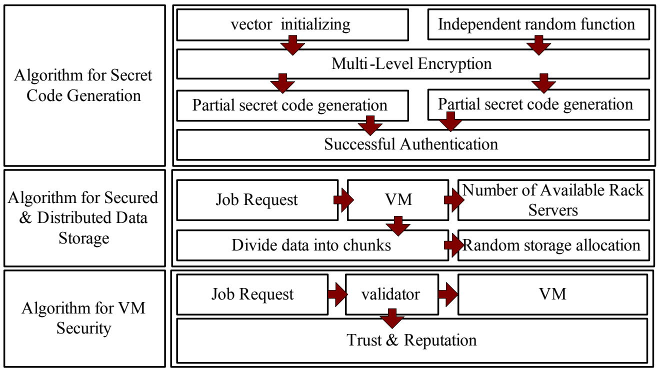
Algorithm for Secret Code Generation
vector initializing
Independent random function
Multi-Level Encryption
Partial secret code generation
Partial secret code generation
Successful Authentication
Algorithm for Secured & Distributed Data Storage
Job Request
VM
Number of Available Rack Servers
Divide data into chunks
Random storage allocation
Algorithm for VM Security
Job Request
validator
VM
Trust & Reputation

**Figure 1: Schematic Architecture of IFCS**

### 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 ($\tau$)

**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 $\rho_1$ and $\rho_2$ (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 $\rho_1$. The second arbitrary number $\rho_2$ 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 ($\tau_1$ and $\tau_2$) for further protection against man-in-middle attack (Line-6). One part of the secret code (say $\tau_1$) is forwarded to the email id of the user, while the other part of the secret code (say $\tau_2$) 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. Following is the step maintained by the algorithm:

**Algorithm for Secured & Distributed Data Storage**

**Input:** *i* (number of VM), *rs* (rack servers), *job_req* (request for job accessing or writing), *n* (total number of rack servers)

**Output:** Secured data storage in cloud

**Start:**

```
1. job_req → $i$
2. for rs=1:n
3.     if (state=busy)
4.         rs++
5.     if (state=free)
6.         $\alpha$ = count (rs)
7.         return $\alpha \rightarrow i$
8.     end
9. end
10. $i \xrightarrow{\text{job\_req}} (\alpha)$
11. $i \xrightarrow{\tau} \text{rand}(\alpha)$
```

**End**

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 $\alpha$ (Line-6/7). It will mean that $\alpha$ is the total number of servers where the user can fulfill its objective of data storage. Hence, the present data is now stored in $\alpha$ 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 $\alpha$ rack server (Line-10) and then it stores the secret code $\tau$ over random numbers of $\alpha$ 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. $i \rightarrow$ 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.         $i \rightarrow$ flagged (Compromise$_{VM}$); break
9.         $i$++
10.        If ($t_i \geq T$ && $r_i \geq R$)
11.        $i \rightarrow$ 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.

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.

## 7. RESULT ANALYSIS

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:

### A. 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.

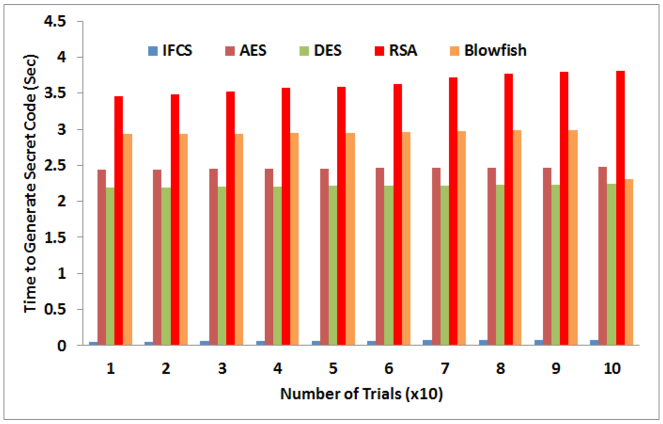

**Figure 2: Analysis of Time to Generate Secret Code**

Figure 2 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.

### B. Analysis of Key Size

Key size is one of the important performance parameter in any security-based application. Figure 3 clearly shows that RSA posses bigger size of key also specifies higher memory dependency that is normally not compatible with existing as well as futuristic low powered embedded computing device with resource constraint. On the other hand AES and Blowfish also have similar size of key but from operational viewpoint AES is much better than other variants of DES with respect to its supportability of hardware acceleration. However, AES has complex cryptographic structure which may lead to overhead for long run and peak traffic condition.

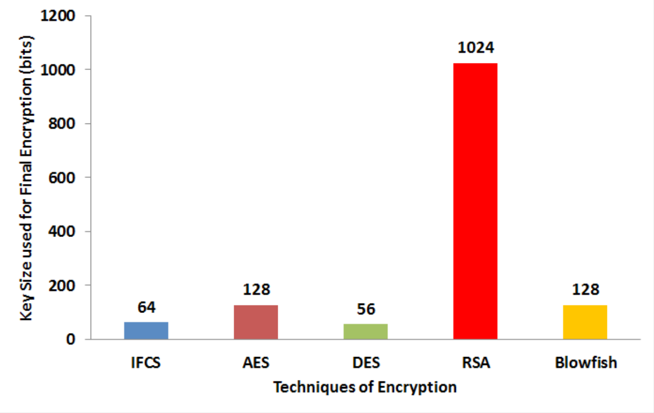

**Figure 3: Analysis of Key Size used for Final Encryption (bits)**

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.

### C. Analysis of Total Algorithm Processing Time

Algorithm processing time is one of the essential performance parameter to justify the effectiveness of the proposed technique. For a security algorithm to dodge the adversaries, it is essential that all the critical steps e.g. key generation, encryption, decryption, key update, etc. consumes a minimal time irrespective of the software and hardware resources present on device of the user. An algorithm with faster speed also supports effective working on the computing device with resource constraints. Figure 4 shows that proposed system offers highly competitive speedy algorithm operation as compared to any existing system. A closer look into Figure 4 shows that time complexity increases for RSA with increasing traffic load. Although, usage of RSA can be rendered good for devices with no resource constraints but it is not much applicable over low-powered and resource constraint computational device. On the other hand AES, DES, and Blowfish has better supportability of low-powered devices, but owing to its static key sizes, its cumulative processing time is more than proposed system.

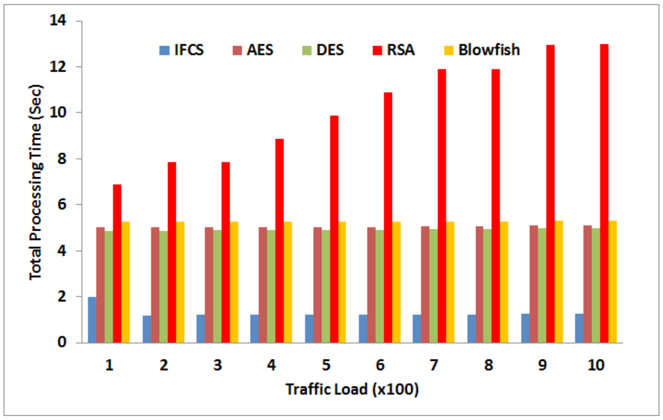

**Figure 4: Analysis of Total Algorithm Processing Time**

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.

## 8. CONCLUSION

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 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 offer higher degree of security in cloud computing. The study outcome was also found to possess faster response time as compared to existing security techniques.

## *References*

[1] Kannan, Rajkumar, "Managing and Processing Big Data in Cloud Computing", IGI Global Computers, pp. 307, 2016.

[2] 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.

[3] S. Murugesan, I. Bojanova, "Encyclopedia of Cloud Computing", John Wiley & Sons Technology & Engineering, pp. 744, 2016.

[4] Z. Ma, "Managing Big Data in Cloud Computing Environments", IGI Global Computers, pp. 314, 2016.

[5] L. Fiondella, A. Puliafito, "Principles of Performance and Reliability Modeling and Evaluation", Springer, pp. 655, 2016.

[6] M. Margarida, Pinheiro, "Handbook of Research on Engaging Digital Natives in Higher Education Settings", IGI Global, pp. 500, 2016.

[7] Z. Huang, X. Sun, J. Luo, J. Wang, "Cloud Computing and Security: First International Conference", Springer, pp. 562, 2016.

[8] S.Y. Zhu, R. Hill, M. Trovati, "Guide to Security Assurance for Cloud Computing", Springer, pp. 229, 2016.

[9] A.A. Saidi, R. Fleischer, Z. Maamar, O.F. Rana, "Intelligent Cloud Computing: First International Conference", Springer, pp. 169, 2015.

[10] 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.

[11] Veena, "SRAAM: Secure resource access authentication mechanism using user-device credential hybridiztion in cloud environment", Retrieved, 06th October, 2016.

[12] 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.

[13] 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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] T. Yang, J. Li and B. Yu, "A Secure Ciphertext Self-Destruction Scheme with Attribute-Based Encryption", Mathematical Problems in Engineering, 2015.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] V.K. Pachghare, "Cryptography and Information Security", PHI Learning Pvt. Ltd, pp. 416, 2015.

[32] E. Biham, A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer Science & Business Media, pp. 188, 2012.

[33] 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.

[34] 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.