A cost-effective 2-tier security paradigm to safeguard cloud data with faster authentication

Veena R. S.[1], Ramachandra V. Pujeri[2], Indiramma M.[3]
[1]Department of Computer Science and Engineering, RV College of Engineering, India
[2]MIT College of Engineering, India
[3]Department of Computer Science and Engineering, BMS College of Engineering, India

Article Info

Article history:

Received Dec 17, 2018
Revised Mar 25, 2019
Accepted Apr 10, 2019

Keywords:

Access control
Authentication
Cloud computing
Cloud data security
Virtual machines security

ABSTRACT

The recent technological advancement has taken cloud computing (CC) infrastructure to a significant level where the increasing level of research interest laid upon cost-effective storage management. Owing to the potential distributed and pervasive storage facility, it lacks efficiency towards fully preserving the integrity of user data attributes. Thereby, the collaborative sharing of user data leads to a situation which opens up various forms of security loop-holes. In the past various forms of security protocols are witnessed which have attempted to solve this similar issue with cryptographic solutions but at the same time lacks sustainability and robustness from a computational perspective. Thereby, the study introduces a 2-tier framework which offers higher-degree of access control along with Virtual Machine (VM) storage security. The study basically optimizes the performance of the model by speeding up the authentication process. The performance validation of the system has been done with respect to conventional encryption standards. The outcome obtained demonstrate that the proposed solution outperforms the existing security standards in terms of processing time, time to generate a secret key and key size for encryption.

Corresponding Author:

Veena R.S.,
Department of Computer Science and Engineering,
RV College of Engineering,
Bengaluru, Karnataka, India.
Email: veena.vturesearchscholar@gmail.com

1. INTRODUCTION

The increasing adoption of cloud-based storage has been witnessed in various applications such as Government, electronic health record, military/defense and other [1]. However, due to pervasive computing and optimized modeling, the cost structure for storage management got significantly improved but at the same time, different forms of technological advancement made it vulnerable to various forms of security threats where significant user data attributes can be compromised for malicious means [2-3]. Unluckily, security violations measured in 2011 and showed that reputed companies (like Google, Sony, Amazon, UK Healthcare System and so on) all experienced security occurrences. In the cloud, consumer's data are obtained to cloud service providers which can be trusted or untrusted [4]. Thereby, a need for trustworthy services, which can facilitate the data availability on time and also enforces the access control requirements arises. The study also explored significant limitations in the existing system in terms of computational efficiency and storage cost and also found few drawbacks in existing security patches which are extensively discussed in the consecutive sections 1, 3, and 5. Addressing these issues, the proposed study formulated a 2-tier cloud security architecture to minimize the possible threats towards violating data integrity. The study performed a comparative analysis where the proposed 2-tier security modeling achieved better performance as compared to existing security solutions. The overall paper is organized as follows: section 2 illustrates the design modeling of the proposed system followed by a comprehensive discussion of results obtained in Section 3 and finally, Section 4 concludes the overall contributory aspect of the study.

With the increasing growth in the development of cloud computing technology, the security has become a serious concern which needs to improve over the cloud, since of continuous accessing or uploading the data and application services from the virtual machine storage. Therefore, in order to extend the security level of cloud infrastructure, Chandrakala and Rao [6] designed a virtual machine (VM) migration tool which is utilized to balance the load, fault management, maintain the system performance and reduce the power consumption. The proposed VM migration technique capable to utilize the VMs placement owing to perform high security and improves the resource utilization with minimum energy consumption.

Zhang and Lee [7], have introduced VM cloud architecture and named as "Cloud-Monatt" is an extended version of the previous study [8]. The proposed architecture is responsible to monitor the VM’s health security. Additionally, authors designed and validated the network protocols inside the distributed system and communication performance of hardware or software modules are validated within the cloud server. The result performance of the proposed Cloud-Monatt architecture able to deliver the attestation services to the users in a reliable manner.

The previous work of Zhang and Lee [8] have explored the prototype software model i.e. Cloud-Monatt which monitor the virtual machines security health inside the cloud environment. The additional features of the proposed software module are; maintain the security level with multiple security properties. Also, it shows how to map and interpret the collected information to security features which can be understandable by the cloud users. From the result, analysis authors concluded that the proposed Cloud-Monatt" framework offers higher security health for cloud infrastructure. In the cloud computing environment, VM’s security is the primary concern for the researchers to improve the security requirement for multiple prospective for example; communication access control, storage monitoring, network anomaly detection and so on. In that context, Yin et al. [9] provided a research study on security as a service for virtual machines on infrastructure as a service (IaaS) platform. The proposed security service model employed 3 distinct layers which orchestrate different security solutions and provided security provisions for VM's an IaaS platform.

In another research study of Liu et al [10] proposed a secure VM framework which improves the VM security over the cloud environment. The aim was to determine the status of users applications on guest virtual machines which have operated for a certain period of time. For this, it integrates measurement principles with VM monitoring. Unlike other VMs, the proposed framework doesn't require virtual processor technology. Also, proposed technique able to detect the anomalies at user level applications by analyzing the measurement changes. As a result, proposed VM framework offers minimum performance overhead. Cloud infrastructure has a dynamic nature and flexible access control. Cloud service providers face multiple risks like; data corrupting, missing the information since of lack of hardware control on their outsourced data.

Access control policy has the ability to overcome this kind of security challenges. Different access control systems are introduced for cloud for example; in Aluvalu et al. [11] proposed hierarchical attribute-based encryption scheme which encrypts and decrypt the stored data files in the cloud using "Blowfish" algorithm. Authors proved that proposed scheme reduces the system complexity and improve the efficiency by maximizing the number of domain levels. Meanwhile, in Chennam and Lakshmi [12] proposed a cipher-text attribute-based encryption scheme which ensures a strong security policy for data sharing and protects the privacy of the cloud users with secure dynamic processing.

The biggest challenge for any distributed systems is maintaining the security during data delivery process. The basic technology to address the data delivery problem is an access control mechanism. It is an emerging technology especially applicable for distribution systems to boost security issues and prevent the fraud [13]. Another access control cipher text attribute-based encryption scheme is introduced by He et.al [14] to address the P2P storage security problems. Hence the authors designed an efficient, secure and fine-grained access control scheme, especially for the cloud storage system. From the experimental analysis have concluded that a proposed security mechanism is highly efficient for P2P cloud storage and reduces the processing overhead.

Another attribute-based access control encryption mechanism was proposed by Xia et.al [15], with the aim to access the entire encrypted shared data that is named as "key escrow problem". Additionally, the authors introduced an efficient revocation scheme to supports both backward and forward security. In Xue et al [16] explored an approach of cloud side access control mechanism for encrypted data storage. From the proposed scheme can secure the cloud storage from the external attacks and offers power consumption accountability. Also introduced two significant security protocols which help to measure and analyze the system performance.

The increasing adaption of cloud-enabled data computing and storage management has clearly focused on enhancing its performance in terms of utility and cost factors which have a significant impact on the economic conditions. The better pervasive computing solutions need better access control as well as secure storage management to ensure the reliability of data in VMs. Thereby, the existing research problem pertaining to security of cloud which is overlooked in most of the above significant studies are as follows:

- Existing security patches running on the top of cloud imposes comparatively weak security patches which do not ensure better access control of the client uploaded data in the cloud. It is also found that most of the authentication and access control mechanism is very much contemporary which doesn't yield a better security solution when the attack pattern changes.
- Most of the conventional cloud-based authentication policies are cryptography based which often found ensuring effective security patches owing to its potential encryption solution but at the same time lacks cost-effectiveness from a computational viewpoint, which is essential when the ubiquitous pattern of computing is concerned for transactional data.
- There has been very less emphasis given towards securing the cloud storage (i.e. VM instances) where heterogeneous data uploaded by clients get stored. The emergent data storing policy thereby needs a cost-effective security model which can sense the level of vulnerability arises to bridge the gap between security and communication performance.
- Existing security loop-holes in a cloud storage system due to complex big-data attributes are yet to be addressed with a full-proof solution. It can be solved by storing the data among random VMs with a non-conventional file-indexing system.

Therefore, the problem identified in this regards is- "*It is quite a challenging task to design an algorithm that can ensure cost-effective data security after the clients uploads the data in cloud storage. The challenge increases multifold when the big data stream is considered*" The presented study thereby intends to solve the identified problem with a joint framework which is two-fold where firstly it introduces i) a novel cloud access control mechanism followed by ii) a cost-effective framework for a higher degree of VM security solution.

The proposed system offers high-level security solution by presenting a combined framework which involves two stages of operations such as i) **Stage-1**: A novel access control policy along with ii) **Stage-2**: A cost-effective framework for VM security. It basically optimizes the performance of the solution by incorporating light-weight cryptography policy where a pervasive pattern of the computation made it computationally efficient and robust. The access control policy basically applies a linear keccak technique which also enhanced it scalability performance to a higher extent. The following Figure 1 shows an overview of the proposed 2-tier security modeling. The proposed architectural block-based representation clearly shows that the system modeling is of 2-fold segments which share a common research goal of strengthing the security architecture targeted to be implemented on multiple cloud or VMs. The system modeling is supported with two different algorithms which are analytically framed and implemented over a numerical platform. The system design and implementation require minimum 64-bit windows supported with 4GB internal memory and 1.2 GHz processing speed. The performance of the proposed modeling has been validated with respect to three different parameters such as *i)* Time to generate a secret key, ii) Processing time, iii) Key size for encryption. The extensive discussion of the proposed framework design and modeling is illustrated in the consecutive section

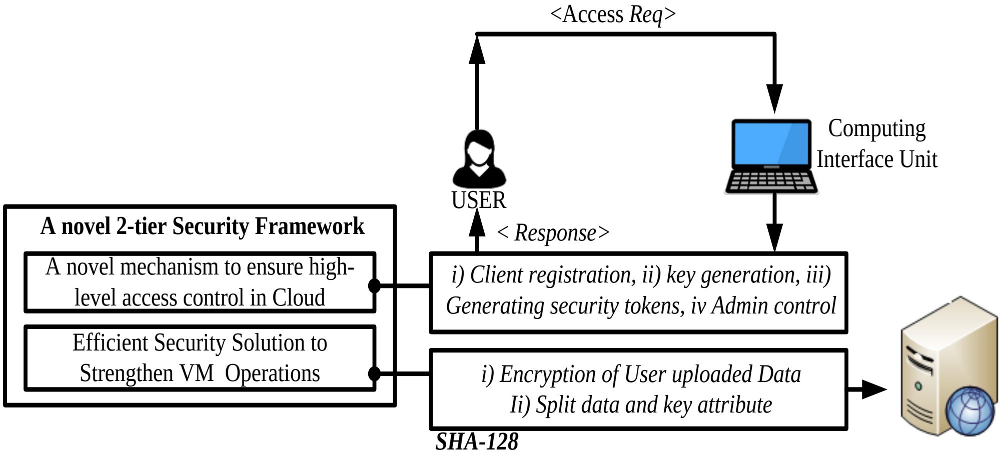
<Access Req>
Computing Interface Unit
USER
< Response>
A novel 2-tier Security Framework
A novel mechanism to ensure high-level access control in Cloud
Efficient Security Solution to Strengthen VM Operations
i) Client registration, ii) key generation, iii) Generating security tokens, iv Admin control
i) Encryption of User uploaded Data
Ii) Split data and key attribute
SHA-128

Figure 1. Proposed architecture

2. SYSTEM DESIGN

The proposed system aims to explore access control and virtual machine security. The detailed system design is given below.

2.1. Phase-one: access control for cloud users

This phase of the research aims to provide a highly secure authentication mechanism for the cloud storage system (CSS). The block representation of the proposed authentication mechanism is shown in Figure 2 where the cloud is accessed by considering user credentials and device authentication.

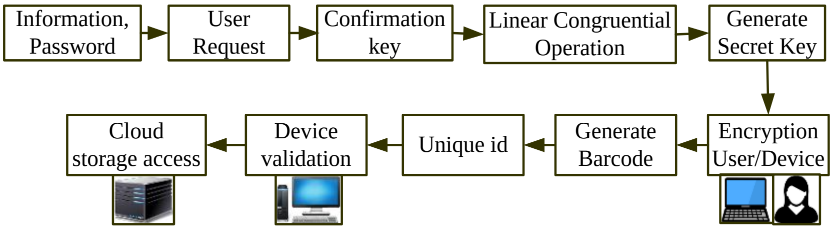

Figure 2. Block representation of an access control

In the initial stage, the user credentials will be taken and proceeded for the enrollment process. The user registration is performed by user's preformation, for that, a seed value is generated which helps in secure authentication. Later, encryption is applied in each layer for the same credentials of users. For this user will be provided with a unique identification number. Then, a seed or token for security will be generated for which similarity match will be initialized for preliminary authentication. In the next stage, to provide further security to the token user credentials is obtained as a request for security key confirmation. Further, a linear congruential operation is performed to generate a random number for encryption. The encryption is performed to handle both the trusted user and device. This generates a secret key which is embedded as a barcode to perform user decryption. Finally, the secured information from the barcode is extracted and an administrator module is build to control the user activities. The algorithm implemented for access control is given below:

Algorithm for access control of cloud users

```
Start
L-1. Initialize → Nu, Sp, Uid
L-2. Set→ $U_{inf}(M_{N,} E_{id}$, Uid), Pw
L-3. Store→ $U_{inf}$→$S_m$
L-4. Match→Uinf || $S_t$
L-5. Initialize→Pw
L-6. Define→$C_L$
L-7. Convert Pw→ ASCII character
L-8. Generate Random number→ secret key
L-9. Perform → Encryption
L-10. Embedded key→Barcode
L-11. Validate →User Credentials
L-12. Decrypt→Barcode
L-13. Store→Cloud
L-14. Verify Up→ Allow or denied permission
L-15. Create→bucket for Client activities
L-16. Manage→files&folders
L-17. Examine all the activities
L-18. Permit→Cs
End
```

The algorithm begins with the initialization of the number of users (Nu), service providers (Sp) of cloud and unique identification (Uid) number (Line-1.). Using these credentials each users information is set with a mobile number (M_N), email id (Eid), unique identification (Uid) number and then the password is set (Line-2.). All these information of users is considered as the private information collected by the Sp apart from other miscellaneous information captured and is stored in the system (Line-3). Thus, the algorithm aims to secure all these private information it takes a security mechanism to protect this information. As concatenation of the unique number results in another unique number; therefore, the concatenation operation acts as one of the simple steps in designing trapdoor function. This operation is performed to do encoding of user information and password. If the system information (Sm) and its concatenated data matches then security token St is obtained (Line-4). If positive similarity match among two concatenated security tokens is observed then the algorithm recognizes it as a legitimate user or else it indicates it as illegitimate members. This algorithm also aims to generate a secret key that could offer a better encryption process. For this, the inputs Nu, Sp, Uid, St. The generated security token is needed to be protected from any form of man-in-middle attack. Also, the secret key is utilized for authenticated passphrase generation from the virtual machine which is large in number as well as it is highly distributed.

Hence, virtual machines to be highly secured. The proposed system configures the length of the code (C_L) using two network parameters (Line-6). The security tokens are classified with respect to device identity Did. The obtained information of the encryption is further encoded in the form of the ASCII format that allows performing ciphering the obtained text further (Line-7). Further security is incorporated by applying for a pseudo-random number to obfuscate the code (Line-8) which does not allow the attacker to perform decryption on the ciphered data. The proposed system implements a linear congruential operation which brings optimization of pseudo-random numbers which offers a dual layer of security towards the illegitimate access. Further encryption operation is performed using the hashing function (Hf) that leads to a generation of encrypted data (Line-9). It should be known that this encrypted data will be only required to perform involuntary authentication mechanism over the cloud environment. The algorithm does verification of the information engraved within the device. This operation is further followed by the extraction of the encrypted information from the barcodes (Line-10).

This operation is carried out by any proprietary application running over the user device. It is also safer from a security viewpoint; as such forms of the reader, the application can perform the only extraction of the encoded information and not the original information. For extracting the original information, the encrypted data has to be passed over to the cloud storage where it is subjected to decryption. The information obtained from the decryption is not forwarded to the user, and only the access rights are forwarded to the users in the form of grant or denial (Line-11).

This algorithm presents the process of authentication level-2. The algorithm starts with a unique key which denotes by Ukey. Once the unique key is provided, then the device will check for authentication. There are two major steps for authentication which is: a) Authenticate device registration which denotes by Dr. b) Decryption of the barcode which denotes by #. The next step demonstrates for the user device, which is Decrypt, the Bar Code for the user device (Cd) (Line-12). Here, the user device will decrypt the bar code. And in the end, cloud storage will be accessible by the user who already registered into the cloud (Line-13). The access rights are offered by a match of the correct user while the privilege is offered by the subscripted opted by the user by paying a specific amount to their service provider.

In case of unauthorized access event, the administrator forwards a message of denial of any form of services to the unauthorized user otherwise, it grants the access (Line-14). After the access is granted, the user will be able to use the application. Another interesting implementation of the proposed system is that the user is offered a right to construct cloud buckets (Line-15) for repositing its file contents. Cloud buckets are the location of storage units created by an administrator to reposit the files of the user (Line-16). Such cloud buckets are highly interconnected with each other as well as highly distributed in nature. A significant multi-threading process is utilized for ensuring the distributed file management.

Apart from this, the proposed system also entitles the administrator to edit any form of operation that is currently in use by any user. The above algorithm demonstrates over attaining the access control to the cloud storage, and it is not necessities that the users have granted entire the privileges to allow activity into the cloud storage (Line-17). These privileges should provide by the administrator. Only admin may give these privileges like a grant or deny permission to the user (Line-18). These privileges give the users to make a bucket in the cloud storage, permits the user to organize the files as well as folders. It also permits the user to upload some different kinds of files with mine type authorization and even permits him/her to execute the delete performance. These privileges are set or presented by the administrator who examines entire the activity into the cloud.

2.2. Phase-two for integrated virtual machine security on multiple clouds

This stage of design and analysis includes the development of an integrated novel schema for cloud-based storage security which also offers a higher degree of privacy preservation in VMs. The secure storage access mechanism is conceptually designed and targeted to be implemented on cloud-enabled VMs with the purpose of reducing *i) vulnerability associated with* public *storage* and also *ii) data leakage problems.* Designing the security model for cloud storage also apply an optimized security principle which enhances the operational process of encryption standards by means of maintaining a well-balanced between forwarding and backward secrecy. The process of optimized encryption policy also enhances the authentication and data exchange paradigm to offer much secure and cost-effective framework of secure storage on multiple clouds. It also aims to offer a higher degree of data security in terms of privacy preservation, confidentiality, and integrity. The framework basically applies the secure splitting mechanism to store encrypted data attributes to the cloud-enabled data centers which generate VM instances. The following Figure 3 shows a block-based structured architecture of the system modeling for this phase.

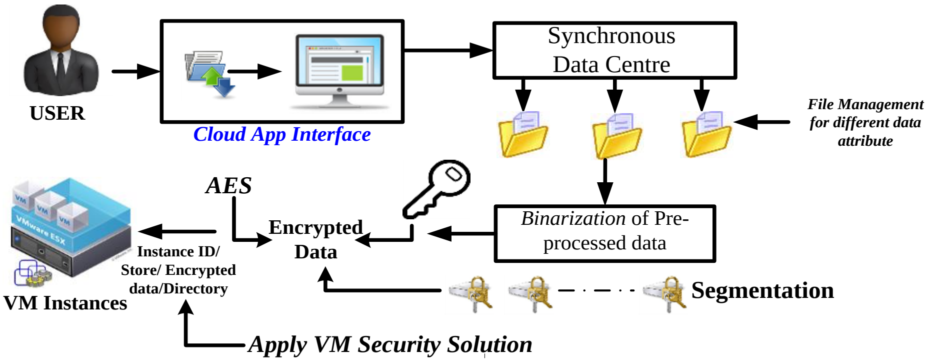
USER
Cloud App Interface
Synchronous Data Centre
File Management for different data attribute
AES
Encrypted Data
Binarization of Pre-processed data
Instance ID/ Store/ Encrypted data/Directory
VM Instances
Segmentation
Apply VM Security Solution

Figure 3. Architecture for VM security solution

The efficient cloud storage management intends to safeguard the data storing policy, where data get uploaded by the cloud users through different cloud applications. The system formulates a multi-level and distributed cloud architecture where cloud security get imposed to attain better security of data. Usually, users are more concerned about securing their private information which can be useful for future requirement and analysis. The core design principle of the proposed technique is completely analytical and also reinforce privacy protection of data to fulfill the requirement of i) Optimizing complexity problem while handling bigger key size, ii) strengthening the key generation process while iii) implementing a robust simplified secure authentication schema. The core steps involved to assess the computation of the proposed algorithm is presented below. In this stage the algorithm formulation, the user has to give input of an entity **C*req***, which is further subjected to consecutive operations. Here, **C*req*** refers to the user request to store specific data attribute into cloud storage or VM instance. After processing the algorithm in a numerical computing environment, the algorithm generates encrypted data which is further segmented prior placing to the VM storage element.

Algorithm for secure cloud storage management using key-splitting/Segmentation

```
Input: $\mathbf{C}_{req}$ (User request to store specific data attribute)
Output: VM ← $\mathbf{D}_{Ecrypt}$ (Successful placement of encrypted data attribute)
Start
L-1: Initialize: $\boldsymbol{DB}_{Con}$ . U → App (i), $D^1$, $\mathbf{C}_{req}$
L-2: Obtain $\mathbf{U}_{ID}$ and $\mathbf{U}_{pass}$
L-3: $\boldsymbol{\mathcal{E}} \leftarrow$ MD5 ($\mathbf{U}_{pass}$)
L-4: Validate $U_{ID}$ and $U_{pass}$
L-5: Convert [0, 1] ← $D^1$
L-6: [$\#^1$, $\#^2$] ← $G_{key-1,2}(\mathcal{E}, \mathbf{U}_{pass})$   // Secret key Generation phase
L-7: $\Delta \leftarrow AES_{En}(D^1)[\#^1, \#^2]$ // Encryption of data
L-8: Apply Rijndel key scheduling process and compute $R_{key}$
L-9: Compute BitXOR ← $f(S_{byte}, \text{Block-}R_{key})$
L-10: Apply Non-Linear Substitution
L-11: Check for the state of $St_{row}$, $St_{Col}$
L-12: Check Size of the data $S_\Delta$
L-13: Compute $R_{em} = S_\Delta$ / number of VMs
L-14: perform segmentation of data and estimate the size of segmented data $S_{Data}(\Delta)$
                                        $S_{\Delta-} R_{em}$ / Number of VMs
L-15: Compute last data size = $S_{Data}(\Delta) + R_{em}$
L-16: Key←Split [$\#^1$, $\#^2$] attributes
L-17:                   for (i == 1: n) for all $VM_i \subseteq N_{(VM)}$
L-18:                             Randomize cloud elements
L-19:                             Process $\mathbf{C}_{req}$
L-20: stop
L-21: Insert key values along with $S_{Data}(\Delta)$ randomized VMs
Stop
```

In step-1 of the algorithm, a connection gets established between the user interface where application interface basically process and validates the requested data (D^1) sequence. The system basically takes user ID (**U_{ID}) and password (U_{pass}**) into consideration which is highlighted in line-2. In line-3, a secure data is generated using MD5, in which the user password get protected. Further, the system also applies the 1st layer of authentication policy to validate the user ID and Password (Line-4). Further, the data which is to be securely placed inside a VM storage is subjected to go through a pre-processing stage where the data get converted into a sequence of binary bit pattern (Line-5). On the other hand, a function named $G_{key-1,\ 2}()$, applies a secret key generation process which is further used in encrypting the data attributes using AES-128 encryption standard (Line-6 and Line-7).

The process further optimized the key scheduling by means of applying a novel Rijndel key scheduling process which is highly cited in most the significant security paradigm and also compute the round key attributes R_{key} (Line-8). The encrypted data attribute size in terms of byte along with a block of round key entity is further subjected to corresponding BitXOR computation where the operational functionality is computationally enhanced with respect to processing speed. The further computational process applies non-linear substitution where the old byte get substituted with the newly arrived byte of data attributes while referencing the LookUpTable (Line-9-10). The process also checks for the state of row and state of the column which is associated with the encrypted data attribute and also compute the size of the data. This step further assist in the computation of segmented data size and also in key splitting (Line-12-16).

Finally, the process randomizes the cloud environment and select random VMs to store extracted key attributes along with the $S_{\mathrm{Data}}(\Delta)$ (Line-17-21). The accessing unit of the application interface only responsible for dealing with $\mathbf{C}_{req}$ and the process of the response for storage allocation. The data get segmented and further undergoes through data indexing where the generated secret key perform encryption with AES encryption standard. Then the segmented data along with split key attributes get stored into multiple-rack servers which are maintained by a distributed random cloud environment. The proposed system offers higher-degree of VM storage security even if a chunk of data gets compromised while attaining high-level scalability performance as it doesn't operate with a specific type of file size. The next section of this study highlights a comprehensive discussion on the performance assessment of the proposed solution and also shows the outcome obtained from the simulation environment.

3. RESULT ANALYSIS

A test-bed is constructed to make a replicative environment for the cloud environment. To assess the effectiveness of the internal processing of the proposed algorithm, no existing proprietary cloud-based services are analyzed. It is because it is not feasible to assess the internal processing of any cloud-based services.

3.1. Analysis of access control

The frequently adopted security protocols are the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Secure Hash Algorithm (SHA) and are used to build the secure cloud service. The industries also aimed to develop security patches with the same protocols to enhance their security. As the proposed security model which gives a lightweight authentication mechanism; thus, it chooses processing time as performance parameters for performing a comparative analysis with AES and DES.

Figure 4 shows DES algorithm consumes maximum processing time as it consumes triple times the normal processing speed owing to its inherent dependencies of the maximum size of the block. Furthermore, AES cannot be termed as secure algorithm although its speed is slightly slower than DES as the block developed by AES during encryption bears similar dimensional aspects making the pattern more vulnerable. However, the proposed system doesn't use any of these existing schemes nor does it implement any complex rounds over increasing simulation trials. Hence, the proposed system offers faster processing compared to AES as well as DES.

There are two variants of the SHA as seen to be exercised in the existing system, i.e., SHA-1 and SHA-2. SHA-1 is the preliminary version which is still used by many service providers irrespective of its reported to being obsolete; however, SHA-2 claims of offering more security benefits. Figure 5 shows the measurement between the proposed techniques and both the variants of the SHA algorithm. The proposed technique attains superior computational outcomes in evaluate to the SHA-1 algorithm; the proposed method is also established to have superior computational components evaluated to the SHA algorithm. It gives a superior security characteristic by creating a secured code in evaluate to SHA that itself has been a victim of various attacks in the past. Both the variants of SHA leads to the generation of collision attack to some extent of time. The proposed analysis also finds no significant difference in processing time for both the variants of SHAs while the proposed system offers slightly faster computation just by using the normal hash function. Hence, the proposed system offers more security and also is considered as the highly faster response time.

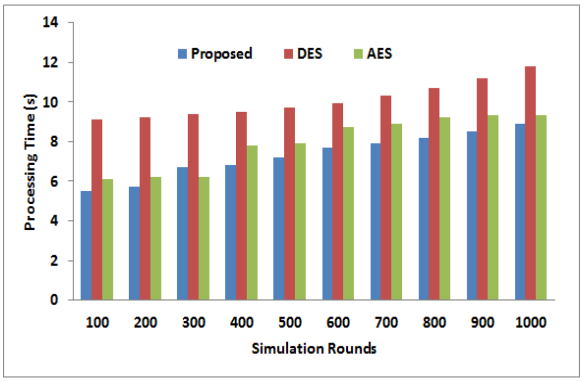

Figure 4. Comparative analysis with AES and DES

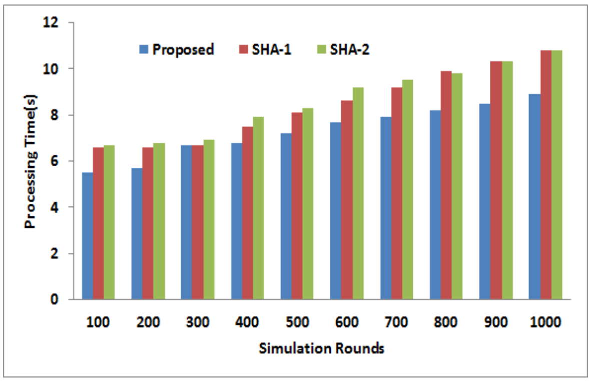

Figure 5. Comparative analysis with SHA-1 and SHA-2

3.2. Analysis of virtual machine security

The system explores the different data-centers and cloud provider utilizes the different cryptographic algorithms like AES, DES, RSN and Blowfish for the encryption process. Hence, the results of the proposed study have been compared with all these cryptographic algorithms. The keys size is the performance parameter which requires a specific memory where it can be stored. The devices with memory constraints will always have dependencies on memory efficient algorithms i.e. algorithms with highly reduced key size. However, the key size is also proportional to security. The proposed algorithm uses a discrete cryptographic hash algorithm in an easier manner where the algorithm complexity is always taken care of by discarding it if it is already applied. Therefore, this lowest key size will provide an equal level of security what "RSA" can generate with bigger size of the key and therefore proposed system can be considered as one of the cost-effective algorithms. Figure 6 illustrates that RSA protocol groups the larger number of key size also defines high memory dependency which usually not conflicts with existing. Conversely, Blowfish and AES also have the same feature but from the computational point of view, AES is better than other security protocols.

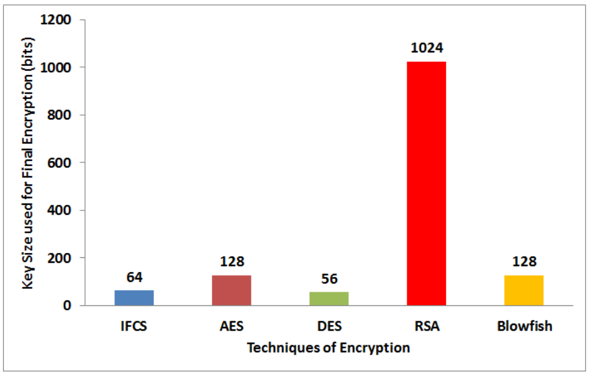

Figure 6. Comparative analysis of key-size used for encryption

One of the significant performance parameter to assess the effectiveness of the proposed system is to calculate the total processing time. In this research study, the system evaluates the all algorithm processing time which includes some essential steps like secret key generation, key updation, and encryption so on. For all these implementations, the system takes minimum time irrespective of hardware and software resources presents in the user device. The processing of the algorithm with higher speed is also assisted with effective implementation in the computational device with resource constraints. Figure.6 represents that the proposed framework will provide faster computational speed for algorithm processing as compared with other existing methods. Figure 7 illustrates that complexity of time will maximize for RSA with maximizing the traffic load. Though utilization of RSA could be furnished best for computing devices with no resource constraints it's not more applicable to low energized devices and resource computing device. Conversely, Blowfish, DES, and AES contain high supportability of low energized devices, but due to its constant key-lengths, its increasing processing time period is higher than the proposed technique. From the above figure, it can be seen that the proposed framework provides a faster speed processing time. Since the proposed algorithms authentication utilizes nonrecursive operations, lower key-size and faster key-updating operation. Therefore, the decryption operation is quite better than encryption operation and will not affect even if incoming traffic load increases.

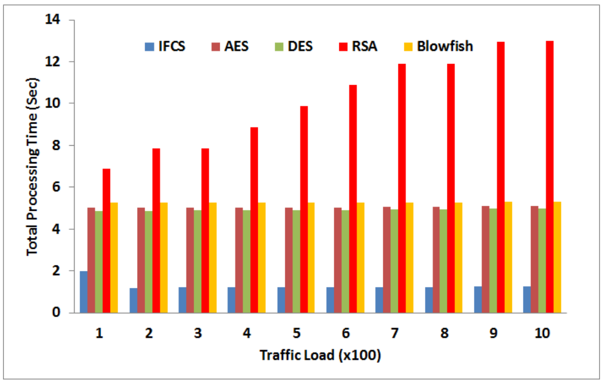

Figure 7. Analysis of Traffic load with respect to overall processing time(s)

4. CONCLUSION

This paper targets to address the security gap that increases with emerging growth of the user requirement and it has forced the enterprises as well as organization to adopt reliable and scalable infrastructure without more investment in a short duration to fulfill the user's requirements. With the improvement in cloud computing, organizations are exploiting the cloud services to transmit a huge amount of data in a short period, provides enormous storage space without setting up new infrastructure as well as ease of maintenance with high availability and scalability so on. Although cloud technology provides several advantages, it also susceptible to security threats as other technologies. The security can be measured in terms of authentication, identification, and validations are not considered as reliable as they fail to offer a high security against the attacks. In this paper, a simplified version of modeling has been carried out where the prominent focus was to eliminate authentication and data security problems. The outcomes of the access control model are tested using experimental modeling, the reliability and technical adoption of the outcomes are quite acceptable in real-world problems of security. The proposed access control model offers ~ 80% of the reduction in overall computational complexity in contrast to the existing system. Similarly, the VM security model outcomes show that it offers ~65% improvement in reducing encryption time without any serious spatial complexity.

Further, the proposed models of cloud can be considered to improve the workability and quality of service (QoS) factors under high traffic load situation. Usage of cryptographic algorithms could be evaluated to target high efficiency over performance parameters. Also, the models can be used towards implementing the cryptographic authentication mechanism for examining the legitimacy of clients as well as data and traffic load being generated.

REFERENCES

[1] L. Grandinetti, O. Pisacane, M. Sheikhalishahi, "Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectives", *IGI Publication, Advances in Systems Analysis, Software Engineering, and High-Performance Computing*, ISBN-13: 978-1466646834, 2013.

[2] G.R. Vijay, A.R.M. Reddy, "Investigational Analysis of Security Measures Effectiveness in Cloud Computing: A Study", *Computer Engineering and Intelligent Systems*, Vol.5, No.7, 2014.

[3] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", *Recommendations of the National Institute of Standards and Technology, Special Publication* 800-145, 2011.

[4] A. J. Adoga, G. M. Rabiu, A. A. Audu, “Criteria for Choosing An Effective Cloud Storage Provider”, *International Journal of Computational Engineering Research*, Vol.04, Iss.2, 2014.

[5] R.A. Popa., J.R. Lorch., D. Molnar., H.J. Wang., and L. Zhuang., “Enabling Security in Cloud Storage SLAs with Cloud Proof”, In *USENIX Annual Technical Conference*, Vol. 242, 2011.

[6] Chandrakala, N., and B. Thirumala Rao. "Migration of Virtual Machine to improve the

[7] Security of Cloud Computing." *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 8, No. 1: pp. 210-219, 2018.

[8] Zhang, Tianwei, and Ruby B. Lee. "Design, Implementation, and Verification of Cloud Architecture for Monitoring a Virtual Machine's Security Health." *IEEE Transactions on Computers,* vol. 67, no. 6, pp. 799-815, 2018.

[9] Zhang, Tianwei, and Ruby B. Lee. "Monitoring and Attestation of Virtual Machine Security Health in Cloud Computing." *IEEE Micro,* vol. 36, no. 5, pp. 28-37, 2016.

[10] Yin, Xueyuan, Xingshu Chen, Lin Chen, Guolin Shao, Hui Li, and Shusong Tao. "Research of Security as a Service for VMs in IaaS Platform." *IEEE Access,* vol. 6, pp. 29158-29172, 2018.

[11] Liu, Qian, Chuliang Weng, Minglu Li, and Yuan Luo. "An In-VM measuring framework for increasing virtual machine security in clouds." *IEEE Security & Privacy,* vol. 8, no. 6, pp. 56-62, 2010.

[12] Aluvalu, Rajanikanth, Vanraj Kamliya, and Lakshmi Muddana. "HASBE access control model with Secure Key Distribution and Efficient Domain Hierarchy for cloud computing." *International Journal of Electrical and Computer Engineering (IJECE),* vol. 6, no. 2, pp. 770-777, 2016.

[13] Chennam, Krishna Keerthi, and M. Akka Lakshmi. "Cloud Security in Crypt Database Server Using Fine Grained Access Control." *International Journal of Electrical and Computer Engineering,* vol. 6, no. 3, pp. 915-924, 2016.

[14] Hu, Vincent C., D. Richard Kuhn, and David F. Ferraiolo. "Access Control for Emerging Distributed Systems." *Computer,* vol. 51, no. 10, pp. 100-103, 2018.

[15] He, Heng, Ruixuan Li, Xinhua Dong, and Zhao Zhang. "Secure, efficient and fine-grained data access control mechanism for P2P storage cloud." *IEEE Transactions on Cloud Computing,* vol. 2, no. 4, pp. 471-484, 2014.

[16] Xia, Zhihua, Liangao Zhang, and Dandan Liu. "Attribute-based access control scheme with efficient revocation in cloud computing." *China Communications,* vol. 13, no. 7, pp. 92-99, 2016.

[17] Xue, Kaiping, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage." *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 8, pp. 2062-2074, 2018.

BIOGRAPHIES OF AUTHORS

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 20 years of experience. Her current research deals with Cloud Computing. She has published 13 papers in National and International Conferences and 3 papers in peer-reviewed International Journals.

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. MIT College of Engineering, Pune, Maharashtra. India

Indiramma M., received 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.