International Journal of Engineering & Technology, 7 (4.36) (2018) 574-579

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Data Verification and Virtual Machine Monitoring

P.V. Samuel Blessed Nayagam[1*], A. Shajin Nargunam[2]

[1]Assistant Professor, Noorul Islam Centre for Higher Education, Tamildadu, India.
[2]Professor, Noorul Islam Centre for Higher Education, Tamilnadu, India. E-mail:shajin@niuniv.com
**Corresponding author E-mail:samuel@niuniv.com*

Abstract

Powerfully configurable virtualized assets make the physical area of the information and process autonomous of its portrayal and the clients have no influence over the physical arrangement of information and running procedure. In a multi-cloud condition the layer of deliberation between the physical equipment and virtualized frameworks gives a great way to convey cost reserve funds through server union and also expanded operational productivity and adaptability. This additional usefulness presents a virtualization layer that it turns into a chance of assault for the facilitated virtual administrations. The proposed access control show ensures virtual machines by receiving access control at various layers. The information shading plan help to secure the virtualized information utilized in the virtual machines. The information confirmation structure, which gives a grouping of trust wipes out the untrusted special virtual machines, and additionally utilize the confided in processing standards to guarantee the respectability of the checking condition. Safeguarding security plot ceaselessly screens the working and trade of information between the virtual machine. The test results demonstrate that this plan can viably counteract virtual machine escape without influencing the general productivity of the framework.

1. Introduction

Developing Distributed computing innovation gives preferences to end clients and business associations. The points of interest are various, for example, cost productivity, expanded capacity limit, reinforcement and recuperation, nonstop asset accessibility and area autonomy and so forth. In any case, notwithstanding these focal points, the greatest issue with the cloud is the "Security". The few favorable circumstances to cloud itself forces other security dangers. Since private information is facilitated in the cloud and they are being handled at remote machines and are directed by the cloud specialist organizations, the clients are stressed over loss of information control in the cloud. There are different purposes behind the CSP to include in unfaithful exposure or spillage of the client's information to any outer substance that may end up being a genuine protection and security worry for any client towards his/her information. Cloud Clients don't have a clue about the machines where their information are prepared, so they begin making a big deal about losing authority over their information. There are no particular systems to check if the administration level understandings made between the information proprietor and the end clients have been protected or not. To ensure trust cloud environment, the user makes an obligation and set trust into the regulatory scheme employed by the cloud service provider. To ensure trust in cloud computing, the organization needs to hand over control of the remarkable parts of privacy and security aspects. This makes it easier for an inside attacker to access the information infuriating the privacy and to create deliberate instances leading to loss or corruption of data. In cloud environment the second major jeopardy is the lack of clarity of information about data ownership. There are many limitations to safeguard the data when it is being handled through cloud services and are maintained in cloud storage. The first limitation depends on the data relocation services offered by the cloud service provider. The second one depends on the perceptibility of the state of the cloud environment and the state of the data produced by it.

2. Related works

In [1] a joined virtual machine checking framework to give significantly preferable programming security over the regular multi-programming working framework approach is introduced which utilizes data framework disengagement instrument.

A Product Dynamic Interpretation plot which can effectively identify and keep certain product misuses is introduced in [2]. In this plan without the help from the equipment, SDT can avert stack-crushing assaults totally by enlarging guidance bring instrument. This is finished by superseding the brings that exist in the stack's location go.

Conventional virtual machine checking occasionally examine the framework and catches just the objective frameworks' state. Further, surveying observing is powerless against transient assaults and irregular disappointments that influence target frameworks between checks summoned by the screen. In [3] an adaptable virtual machine observing instrument is proposed to safeguard such assaults.

In [4] a design to hold the perceivability of a host-based IDS and pulls the IDS outside of the host for more prominent assault opposition. Virtual machine checking plan accomplishes this.
An answer for at the same time address both unwavering quality and security in an observing structure is displayed in [5]. This plan recognizes the shared traits among dependability and security to manage the Hyper Tap. The hyper visor-level system effectively bolsters the two kinds of observing in virtualization conditions.

A novel square plan based key assention convention to underpins different members, and can adaptably broaden the quantity of members in a cloud domain is displayed in [6]. This gathering information sharing model, utilizes recipes for producing the normal meeting key K for different members.
In [7] an inborn connection between secure distributed storage and secure system coding is displayed. This offers ascend to a precise method to construct secure distributed storage conventions.
A productive RFID Confirmation Convention (ERAP), which can achieve the validation without unveiling genuine IDs of the taking an interest labels is introduced in [8]. This plan gives solid protection and security assurance of the RFID clients. It additionally offers secrecy of labels notwithstanding label untraceability. A formal security display for validation and protection in RFID framework is exhibited. This convention provably accomplishes the properties of verification and security. What's more, it requires just little assets to play out the confirmation, which fulfills the prerequisite of very asset obliged ease RFID labels. In [9] a trust models to reason about and to enhance the security for put away information in distributed storage frameworks is displayed. It utilizes cryptographic RBAC plans for information assurance. The trust models give a way to deal with the proprietors to decide the dependability of individual jobs and clients. The job legacy and chain of importance are utilized in the assessment of dependability in jobs.
The focal point of paper [10] is the means by which to make the key updates as straightforward as feasible for the customer. This plan proposes another worldview called distributed storage examining with evident re-appropriating of key updates. By along these lines key updates can be securely redistributed to some approved gathering, and in this manner the key-refresh weight can be diminished.
In [11] an effective open evaluating convention with worldwide and testing square less confirmation and bunch reviewing is proposed. In this plan information elements are considerably more effectively upheld than is the situation of the present plans. This dynamic structure comprises of a doubly connected information table and an area cluster by which the computational and correspondence overheads can be lessened considerably.
The engineering, displayed in [12], endeavors to beat the restrictions in existing equipment bolster plans with a protected and effective convention that relocates virtual machine from source cloud area to goal cloud space by considering principal security administrations, for example, classification, trustworthiness, standard access control and non-denial. In [13] get to strategy based plan which enables the information proprietor to designate the greater part of the calculation assignments engaged with fine-grained information get to control to untrusted cloud servers without uncovering the hidden information substance is proposed. The viability is accomplished by misusing and exceptionally consolidating methods of quality based encryption (ABE), intermediary re-encryption, and apathetic re-encryption.

3. Proposed work

3.1. Trusted computing module

Information proprietor does not have authority over the physical access of information in an open cloud condition. So the responsibility of the information put away in broad daylight cloud condition is one of the significant security concern. Trustable distributed computing stage ought to guarantee the responsibility of information put away in the cloud stage. To understand the responsibility issue, an instrument to manage the information read/compose forms is proposed. This methodology stipends get to rights to clients dependent on their job and furthermore screens each entrance to the proprietor's information, checking that the administration level understandings have been damaged or not.

3.2.Data owner verification

To protect the data from unauthorized user access and to give access permission to data based on the owner privileges, a data colouring scheme is used. Data owner in consultation with the service provider uses a coding scheme to assign a colour to the data based on the identity of the data owner and the colour mapping scheme of the service provider. The coloured data are stored in the cloud. User upon submission of user data to the cloud negotiate with the cloud service provider and based on the attributes and access control limits associated with the data, relevant colour scheme is identified for data coloring. Colour generator generates the color mapping and the user data is coloured using the colour maps. The coloured data are stored in the cloud.

A. Coloured data write

During the data upload process, data owner exchanges the access control privileges and limitations with the cloud service provider. Based on the access level privileges and limitations cloud service provider generates the colour coding scheme for the data to be uploaded in the cloud environment. Colour generator generates the colour map using the coding scheme and the type of data to be stored. Data colouring module creates the coloured data set and store the coloured date in the cloud.

B. Coloured data read

During read request, based on the identity of the user and service provider coding, colour code generator generates the mapping colour code. Backward colour generator generates the colour which helps to extract data from the coloured data. Colour mapper generates the sequence of blocks of coloured data to be accessed. Data extractor extracts the user data from the coloured blocks.

C. Coloured date update

During data updation process, based on the identity of the user colour code generator generates the colour map. Backward colour generator generates the colour map based on the data owner identity and access limitations of the Data. User data is extracted from the coloured data blocks. Extracted user data is updated based on the update request of the user/owner and fed to the recolouring module. Recolouring operation is done on the modified data and stores the coloured data in the cloud as shown in Figure 1.

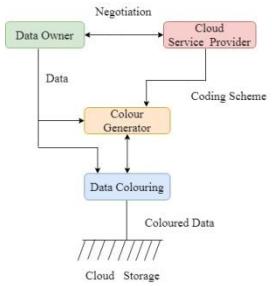

Figure 1: Data write process

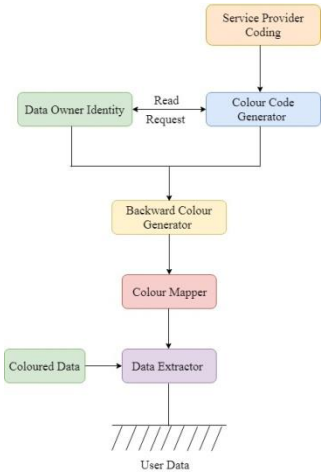

Figure 2: Data read process

Further the colouring module helps to monitor the coloured read access performed on each coloured data item. The colour mapper and data extraction activities are registered in the log file. This logging activity helps to monitor the usage of data hosted on the cloud by the data owner. The log files are also coloured based on the colour map agreed between the user and the cloud service provider. Each mismatch read activity identified by the colour mapper is also logged as mismatch attempts. Periodically the coloured log data is being audited by the data owner. This scheme ensures that data owner can oversee the read attempts performed on each coloured data item uploaded on the cloud. The record of mismatch read represents the unauthorized read attempts made on a user data uploaded on the cloud. Thus data colouring scheme ensures authorized access of data uploaded on the cloud service provider and notifies the data owner about the read attempts performed on each coloured data as shown in Figure 2.

3.2. Process monitoring scheme

In the cloud virtual machine environment monitoring the status of running process and regulating the inter-process communication of running process are not possible as in the case of other operating environment. Thus for building a trustable computing environment in cloud platform a processes role based access control scheme is used to control and regulate the execution flow of the running process in the cloud environment. The process access control is categorized based on three following factors:

i. Identity based access control list
ii. Process role based access control list
iii. Temporal based access control list

Three types of access control list are maintained in the virtualized environment. Identity based access control list maintains the access limitations of the VM/Process according to the identity of the user who imitates the VM/Process. Role based access control list maintains the access permissions of the process roles assigned at the time of creating the VM/Process. Time synchronous process allows the process to interact with the running processes which are created within the specified time limits. Time based access limits specifies the inter process or inter virtual machine access permissions with respect to the time of execution of the process/VM. Three bit coding scheme is used to represent the authorization level of each running process. Least significant bit represents the Identity Based Access Limitation Status (IBALS). Middle bit represent the Role Based Access Limitation Status (RBALS) as mentioned in the Table 1. Most significant bit represents the Time Based Access Limitation Status (TBALS) of the running process as shown in Figure 3.

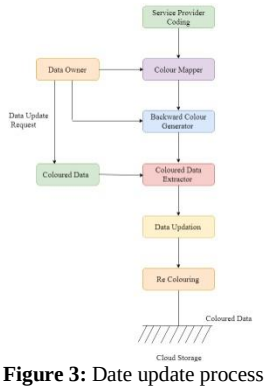

Figure 3: Date update process

Table 1: Process/VM Access Flags

Ibals	Rbals	Tbals	Level
0	0	1	Low
0	1	0	Low
0	1	1	Intermediate
1	0	0	Low
1	0	1	Intermediate
1	1	0	Intermediate
1	1	1	High

Process/VM access flags represent the access permission and limitations of running process/VM and inter process message passing or communication via shared memory access is allowed based on the flag setting of the running process/VM.

3.3. Security defense status

Similar to protecting the process/VM based on the access control permission and limitations, security defending schemes are also employed to protect the process/VM from unauthorized access. For security defense the nodes agreed for running process/VM maintains the record of defense mechanism employed in each node. The security defense status of each node is represented with a three bit status value. The defense mechanism employed are represented as follows:

1. Malware protection availability in each node in the cloud
2. Watch dog which closely monitors the functional flow of each running process
3. Data curtaining scheme which prevents the leakage of data by malicious process

Three bit coding scheme is used to represent the defense security status of each node in the cloud. Least significant bit represents Malware Protection Availability Status (MPAS). Middle bit represent the Watch Dog Function Status (WDFS). Most significant bit represent the Data Curtaining And Leakage Protection Status (DCLPS) of the running process.

3.4. Malware protection

Malware protection is a node level security defense scheme which monitors the malicious activity which infringes the code of a running process. This status flag represent whether malware protection has been employed in that node or not. This enables the scheduler to schedule the process which requires high level of security to nodes having malware protection.

3.5. Watch dog protection

In the cloud environment hypervisor act as an interpreter for interpreting the codes generated by the virtual machine and schedule it to the physical computing system for further processing. Watch dog scheme helps to monitor the process flow of scheduled job at node level to identify any malicious unexpected activities. This notification scheme ensures/monitors the unexpected activities during physical computation.

3.6. Data curtaining

Memory curtaining is a data access protection scheme to prevent unauthorized access to data by another process. To protect the data during physical access at node level, each virtual machine data is protected with boundary access limit value. Each memory read/write operation is controlled by the base and offset limits and the memory access is denied if the offset limit exceeded as shown in Table 2.

Table 2: Security Defense Status Flag

DCLPS	WDFS	MPAS	Level
0	0	1	Low
0	1	0	Low
0	1	1	Intermediate
1	0	0	Low
1	0	1	Intermediate
1	1	0	Intermediate
1	1	1	High

3.7.Trust evaluation module

The trust factors employed and the access control and security defense schemes used to ensure the trustworthiness needs to be normalized to eliminate the deviations caused due to the difference in the state of Process/Node in the cloud domain. Window based timestamp is used to represent the real time running status of the running Process/VM. In the i^{th} timestamp Δt_i, n cloud resources are assumed to be evaluated. Thus n refers the total number of measurement samples. The measurement sample set is represented as $\{y_1, y_2, y_3, \ldots y_n\}$. Let m be the number of security status imposed on the Process/VM during the i^{th} timestamp.

$$Y(\Delta t_i) = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{pmatrix} = \begin{pmatrix} y_{11}\ y_{12}\ y_{13} & & y_{1m} \\ y_{21}\ y_{22}\ y_{23} & & y_{2m} \\ y_{31}\ y_{32}\ y_{33} & & y_{3m} \\ y_{41}\ y_{42}\ y_{43} & \ldots & y_{4m} \\ \cdot\ \cdot\ \cdot & & \cdot \\ \cdot\ \cdot\ \cdot & & \cdot \\ y_{n1}\ y_{n2}\ y_{n3} & & y_{nm} \end{pmatrix} \quad (1)$$

In this each row shall be normalized into [0.01 to 0.99]. The normalized equation is:

$$r_{ik} = \frac{0.01 + (y_{ik} - min(y_{ik}))(0.99 - 0.01)}{max(y_{ik}) - min(y_{ik})} \quad (2)$$

$$R(\Delta t_i) = \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \\ \cdot \\ \cdot \\ \cdot \\ r_n \end{pmatrix} = \begin{pmatrix} r_{11}\ r_{12}\ r_{13} & & r_{1m} \\ r_{21}\ r_{22}\ r_{23} & & r_{2m} \\ r_{31}\ r_{32}\ r_{33} & & r_{3m} \\ r_{41}\ r_{42}\ r_{43} & \ldots & r_{4m} \\ \cdot\ \cdot\ \cdot & & \cdot \\ \cdot\ \cdot\ \cdot & & \cdot \\ r_{n1}\ r_{n2}\ r_{n3} & & r_{nm} \end{pmatrix} \quad (3)$$

The attribute set $\{r_{1k}, r_{2k}, r_{3k} \ \ldots \ r_{nk}\}$ denotes the normalized trust factor of cloud resources with process/VM k. The entropy value for attribute R is denoted as;

$$E(I_z) = -k \sum_{k=1}^{n} p(r_{zk}) \ln p(r_{zk}) \quad (4)$$

Where k is a constant and k=1/lnm, $p(r_{zk})$ denotes the probability mass function. r_{zk} exhibit the trusted probability of the trust attribute I_z at the time window Δt_i.

Where $p(r_{zk}) = {}^{r_{zk}}/_{\sum_{z=1}^{n} r_{zk}}$ (5)

In this larger value represent that the resource service operation is more trustworthy.

3.8. Security defense trust degree

Security defense trust degree in a time window Δt_i based indicator for nodes registered in the cloud service provider. Let N_1, N_2, N_3, … N_n be the registered nodes in the cloud service provider.

$$D(\Delta t_i) = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ \cdot \\ \cdot \\ \cdot \\ d_n \end{pmatrix} = \begin{pmatrix} d_{11}\ d_{12}\ d_{13} & & d_{1m} \\ d_{21}\ d_{22}\ d_{23} & & d_{2m} \\ d_{31}\ d_{32}\ d_{33} & & d_{3m} \\ d_{41}\ d_{42}\ d_{43} & \ldots & d_{4m} \\ \cdot\ \cdot\ \cdot & & \cdot \\ \cdot\ \cdot\ \cdot & & \cdot \\ d_{n1}\ d_{n2}\ d_{n3} & & d_{nm} \end{pmatrix} \quad (6)$$

Since different security defense mechanisms are employed in each registered node, it varies with respect to time and the security defense trust degree is represented in time window normalized representation is required to calculate the security defense trust degree of registered nodes.

The normalized security defense operation vector is $r_z = (r_{z1}, r_{z2}, r_{z3} \ \ldots \ r_{zm})$ and $r_z$is computed using the normalized equation.

$$r_{zk} = \frac{0.01 + (d_{zk} - min(d_{zk}))(0.99 - 0.01)}{max(d_{zk}) - min(d_{zk})} \quad (7)$$

Let $D_{n_z}(\Delta t_i)$ be the normalized security defense mechanism employed on node n_z within the i^{th} time window (Δt_i).

Where

$$D_{n_z}(\Delta t_i) = r_z \times \{\omega_1, \omega_2, \omega_3, \ldots \omega_k, \ldots \omega_m\} \quad (8)$$

The normalized security defense operation vector $r_z = (r_{z1}, r_{z2}, r_{z3} \ \ldots \ r_{zm})$, r_{z1} is calculated using the Equation (7)

$w = (\omega_1, \omega_2, \omega_3, \ldots \omega_k, \ldots \omega_m)$, ω_k represent the cumulative defense status flag representation value. The computing task for w is a problem of multi-attribute decision making. This scheme helps to identify the optimum security defense mechanism employed in the registered nodes with respect to the multi-security-defense scheme employed in a multi-cloud environment.

4. Experimental setup and performance analysis

To analyze the trustworthiness of the nodes and the process/VM running on each registered nodes, a multiple cloud environment is setup using the cloud simulation tool. The multiple cloud environment consist of five cloud clusters managed by five cloud managers. Each cluster consist of cloud resources in the form of registered nodes capable of providing virtual machine VMs. Trust manager keeps track of the security defense mechanism and process/VM access limitations imposed on each running process. The main aspects consider for the evaluation of the proposed scheme are accuracy and efficiency.

The accuracy aspect is used to verify whether the proposed mechanism and the security algorithm employed is capable of providing accurate and consistent trust calculation. The efficiency aspect is used to verify the additional overhead incurred and the performance failure rate of the proposed scheme.

The experimental environment result has been observed based on the following four key functions. They are CPU frequency, Average Response Time (ART), Average Task Success Ration (ATSR) and Self Security Competence (SSC). In the cloud environment the VMs are classified Highly Trusted VMs ‘H’, Moderately Trusted VMs ‘M’, Intermediate Trusted VMs ‘I’ and Untrusted VMs ‘U’. The more number of VMs falling to top 25 percentage of trust operation shows the accuracy of the proposed security algorithm with respect to trust prediction. The following graph shows the number of hit VMs falling to top 25 percent value as shown in Figure 4.

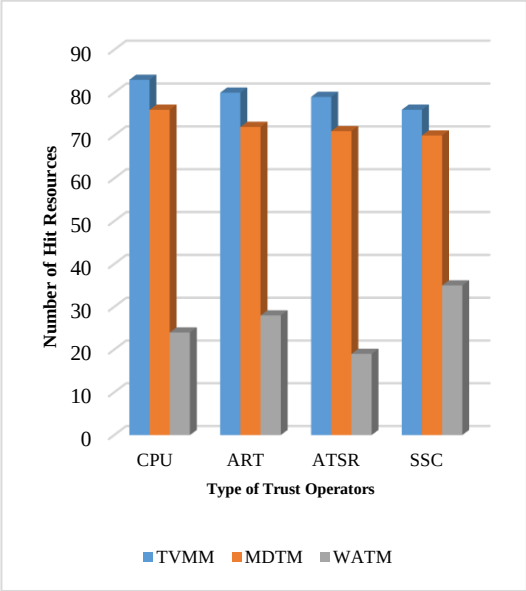

Figure 4: Number of HIT VMs in the Top 25 present of trust operators

The number of hit rate with respect to CPU Frequency, Average Response Time, Average Task Success Ratio and Self Defense Competence are high in the proposed Trusted Virtual Machine Monitoring (TVMM) scheme compared with Multi-Dimensional Trust Model (MDTM) and Weighted Average Trust Model (WATM). It shows the accuracy in determining the trust factor associated to each VMs in the cloud computing environment and it is better than the other trust models.

Then to analyze the performance falling under the opposite condition i.e. the number of hit VMs falling under the bottom 25 present is evaluated from the experimental setup for the four trust operations as shown in Figure 5.

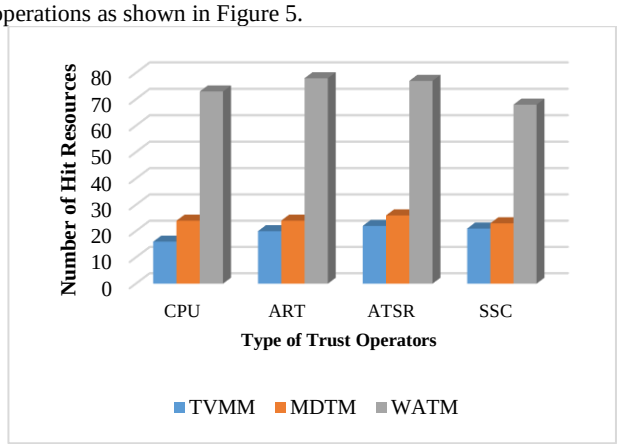

Figure 5: Number of HIT VMs in the bottom 25 present of trust operators

The Figures 7-9 shows that the number of hit VMs fallen in the negative decision of the trust operations is less in TVMM compared with MDTM and WATM. This shows that the misjudgment in the proposed TVMM scheme is less than the other trust models with respect to four trust models. To evaluate the efficiency of the proposed TVMM scheme, three resource scenarios have been setup with different number of VMs having different trust levels.

Trust Model/Scenarios	H	M	I	U
S1	85%	5%	5%	5%
S2	65%	15%	10%	10%
S3	50%	10%	20%	20%

The average job failure rate for the three different resource scenarios are compared with the existing trust models.

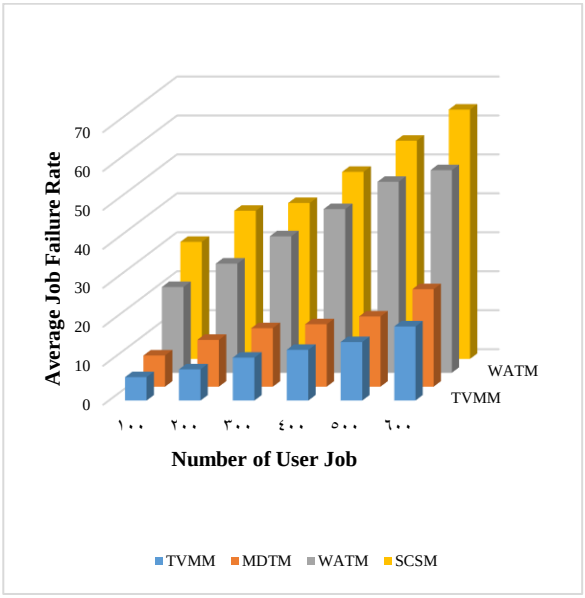

Figure 6: Average job failure rate under scenario S1

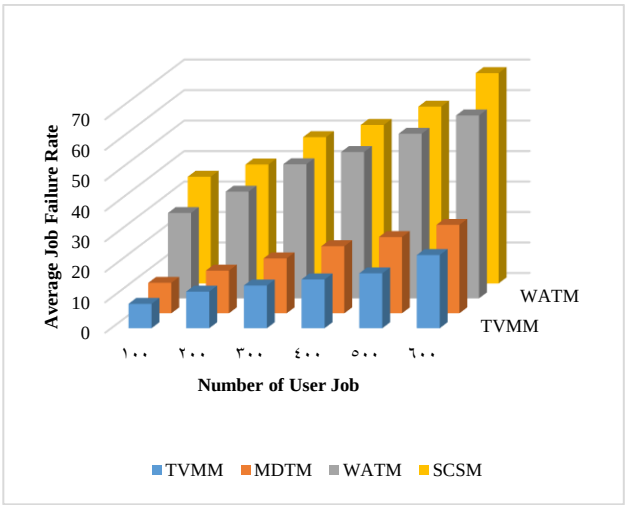

Figure 7: Average job failure rate under scenario S2

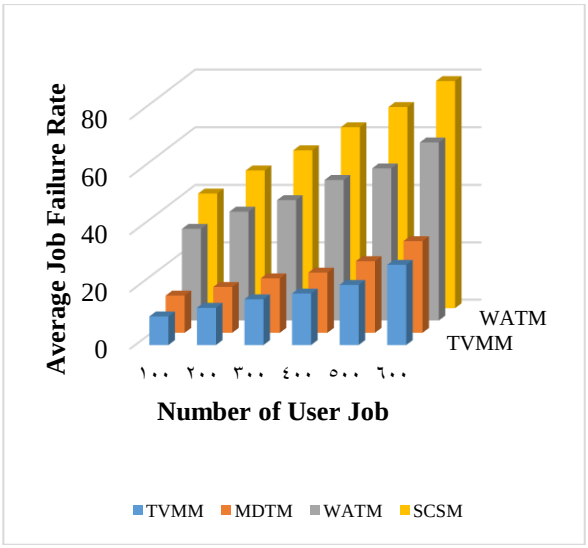

Figure 8: Average job failure rate under scenario S3

The average job failure rate of the proposed TVMM scheme is compared with MDTM, WATM and Strict-Cost Based Match Making Mechanism (SCSM). As the percentage of untrusted VMs in a cloud environment increases the average job failure rate also increases. In the existing schemes the trust is computed as

additional entity and verified during the course of operation. But in the proposed TVMM Scheme trust factor is imbibed in the Virtual Machine creation process. So the created VMs perform computation in a trustable manner. So the average job failure rate is less compared with the existing schemes.

5. Conclusion

Trusted computing schemes intend to provide a trustworthy cloud computing environment for the users requesting the cloud services. An effective, trustworthy cloud computing scheme is presented in this paper. Handling the user data and monitoring the usage of uploaded data in a cloud environment is difficult while providing a flexible computing environment to the cloud users. The data colouring scheme provide a flexible, cost-effective means for monitoring the usage of data uploaded in the cloud. Auditing scheme enables the data owner to verify the user/process who access the data. The trusted computing environment should have schemes to regulate the execution flow of a process/VM to protect the cloud resources from unauthorized access. The identity based, role based and time based access control scheme helps to regulate the execution flow in an effective manner. The normalized trust degree enables the scheduler to select the highly trustable process/VMs during job scheduling. The security, defense degree also depicts the defense mechanism employed in registered nodes. The accuracy in identifying the trusted pool of resources of the proposed TVMM is compared with other trusted computing models. Analysis shows that in the proposed TVMM scheme, number of trusted hits in process/VMs in the top twenty five percentage is higher compared with the other existing trust models and the number of untrusted hits in process/VMs in the top twenty five percentage is less compared to the other existing schemes. The efficiency of the proposed scheme is compared in terms of average job failure rate for three different scenarios and average job failure rate of the proposed TVMM scheme is less than the other trust models.

References

[1] Madnick SE & Donovan JJ, "Application and Analysis of the Virtual Machine Approach to Information System Security and Isolation", *Proceedings of Workshop on Virtual Computer Systems*, (1973), pp.210–224.

[2] Scott K & Davidson JW, "Safe Virtual Execution using Software Dynamic Translation", *Proc. 18th Ann. Computer Security Applications Conference*, (2002), pp.209–218.

[3] Payne BD, de Carbone M & Lee W, "Secure and Flexible Monitoring of Virtual Machines", *Proceedings of 23rd Annals Computer Security Applications Conference*, (2007), pp.385–397.

[4] Garfinkel T & Rosenblum M, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", *Proceedings of Network and Distributed Systems Security Symposium*, (2003), pp. 191–206.

[5] Pham C, Estrada Z, Cao P, Kalbarczyk Z & Iyer RK, "Reliability and security monitoring of virtual machines using hardware architectural invariants", *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, (2014), pp.13-24.

[6] Shen J, Zhou T, He D, Zhang Y, Sun X & Xiang Y, "Block design-based key agreement for group data sharing in cloud computing", *IEEE Transactions on Dependable and Secure Computing*, (2017), pp.1-1.

[7] Chen F, Xiang T, Yang Y & Chow SSM, "Secure cloud storage meets with secure network coding", *IEEE INFOCOM*, (2014), pp. 673–681.

[8] Shen J, Tan H, Moh S, Chung I & Wang J, "An efficient RFID authentication protocol providing strong privacy and security", *Journal of Internet Technology*, Vol.17, No.3, (2016).

[9] Zhou L, Varadharajan V & Hitchens M, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage", *IEEE Transactions On Information Forensics And Security*, Vol.10, No.11, (2015).

[10] Yu J, Ren K & Wang C, "Enabling cloud storage auditing with verifiable outsourcing of key updates", *IEEE Transactions on Information Forensics and Security*, Vol.11, No.6, (2016).

[11] Shen J, Shen J, Chen X, Huang X & Susilo W, "An efficient public auditing protocol with novel dynamic structure for cloud data", *IEEE Transactions on Information Forensics and Security*, (2017).

[12] Zeb T, Ghafoor A, Shibli A & Yousaf M, "A secure architecture for inter-cloud virtual machine migration", *10th International Conference on Security and Privacy in Communication Networks (SecureComm)*, (2014).

[13] Yu S, Wang C, Ren K & Lou W, "Achieving secure, scalable, and fine-grained data access control in cloud computing", *Proceedings of IEEE INFOCOM*, (2010), pp.1–9.