Gene Optimized Multi-Objective Proof Accumulator for Reporting Admissible Evidence of Suspect in Cloud Forensic Services

Ms.Sripriya Arunachalam[*] , Dr. M. Sundara rajan[**]

[*] Research Scholar , Department Of Computer Science, Vels University
[**] Assistant Professor, Department Of Computer Science Government Arts College , Nandanam

Abstract- Cloud forensics involves acquisition, analysis, and reporting the information about the incidents and criminal activities. Cloud computing cause significant challenges for reliable digital-forensic investigations due to several major issues. The cloud forensics is the digital forensic reporting the collected and isolated data while protecting the privacy of information and confidentiality. In order to report the evidence and prove the crime activities inside the cloud, a Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is introduced. The main objective of the GOMOPA technique is reporting the collected and isolated data to the accumulator for identifying the malicious user. In GOMOPA technique, cloud forensic investigator submits the evidence of the malicious activity, proof of integrity, provenance information, proof of data possession, time stamp information and location information to the multi-objective proof accumulator. These multi-objective functions are optimized through the gene based approach. The GOMOPA technique determines the malicious user by validating the investigated evidence with the real suspect which is manipulated by the Cloud Service Provider (CSP). Therefore**,** GOMOPA technique efficiently identifies the suspect who launches the malicious activities over the cloud infrastructure. This helps to improve the confidentiality of the cloud users' log files and preserving the several cloud users who are the malicious users. Experimental evaluation is performed using CloudSim network simulator to show the performance of GOMOPA technique in terms of investigation accuracy, processing time and confidentiality rate compared to the state-of-the-art works.

Index Terms- Cloud computing, Cloud forensics, reporting the evidence, gene optimization, Multi-objective Proof Accumulator, Cloud Service Provider, confidentiality.

I. INTRODUCTION

A significant growth of the cloud data storage and the heterogeneous environment of the cloud computing creates challenges in the cloud forensic investigation as identification, collection and reporting the proof about the malicious users. The reporting is concerned with the presentation of collected evidence to the court of law. The various cloud forensic research works present various solutions on reporting the evidence in different cloud deployment models to identify the malicious user. Our proposed method considers analysis the multiple objectives and reports the evidence to identify malicious activities.

In [1], a secure-Logging-as-a-Service (SecLaaS) was introduced to preserve different logs generated for the actions of virtual machines running in clouds and ensures the confidentiality and integrity of such logs. However, the investigation analysis was not performed effectively in the cloud infrastructure. A Forensic Open-Stack Tools (FROST) was designed in [2] but it performed only a data acquisition phase and other phases of the process affected by cloud computing were not addressed.

An incorporated (iterative) conceptual digital forensic approach was designed in [3] based on McKemmish and NIST. However, it failed to validate the evidence made by integrated approach. A distributed data store for GRR Rapid Response was introduced in [4] that utilize the object model to store and retrieve forensic data. But, the storage space was not reduced.

A Finite state machine (FSM) automata theory was introduced in [5] with computer's virtual machine history. But, it failed to maintain the logical components for a cloud digital investigation. An Integrity verification methods was developed in [6] for secure outsourced computations in cloud computing. However, it failed to find the illegal activities efficiently.

A design and performance of a cloud-based security center for network security forensic investigation was introduced in [7]. But, the forensic analysis was not improved effectively. A current network forensics method (C-NFMs) was designed in [8] for cloud computing using strengths, weaknesses, opportunities, and threats (SWOT) Analysis. However, it was ineffective to prove the different network thread in cloud environment.

The several tools were designed in [9] to provide the digital forensic investigators for collecting the digital evidence from the devices. However, malicious user identification was remained unsolved. The results of a widely distributed survey on basic issues in the emerging area of cloud forensic were presented and analyzed in [10]. But, an effective cloud forensics analysis was not performed.

The issues presented in the existing research works such as more time to identify the malicious user, lack of integrity and confidentiality, fine illegal activities, more storage space. In order to address such kind of issues in cloud computing, an efficient multi objective optimization model is presented to identify the malicious user in forensic analysis with minimum time.

The contribution of the research work is structured as follows. A Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is introduced in cloud forensic services to report the admissible evidence for indentifying the malicious user

with minimum time. Initially, the multi objectives are analyzed with the cloud user log files. Then, the gene based optimization approach is used to find the optimal solution. This confirms that the user who creates the malicious activities inside the cloud environment. This helps to improve the confidentiality rate.

The rest of the paper is arranged in following structure. In Section 2, Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is explained with neat diagram. In Section 3, experimental settings are described and the analysis of results explained in Section 4. In Section 5, introduces the reviews related to the research works. The conclusion of research work is presented in section 6.

II. GENE OPTIMIZED MULTI-OBJECTIVE PROOF ACCUMULATOR TECHNIQUE

In cloud computing, Cloud service providers (CSP) offers different types of services to the several cloud users. A few cloud users frequently use the similar type of services based on pay-per-what-they-use and other users takes the confidential information from cloud users. Therefore, Cloud requires protection from these malicious activities and CSP monitors customer Virtual Machine (VMs) and detect malicious users. In order to perform the investigation on cloud infrastructure, the evidence of the malicious user is identified and collected. Then, the evidence is analyzed using forensic tools and presented to court of law for proving the crime activities. With this objective, Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is introduced. The architecture diagram of the GOMOPA technique is shown in figure 1.

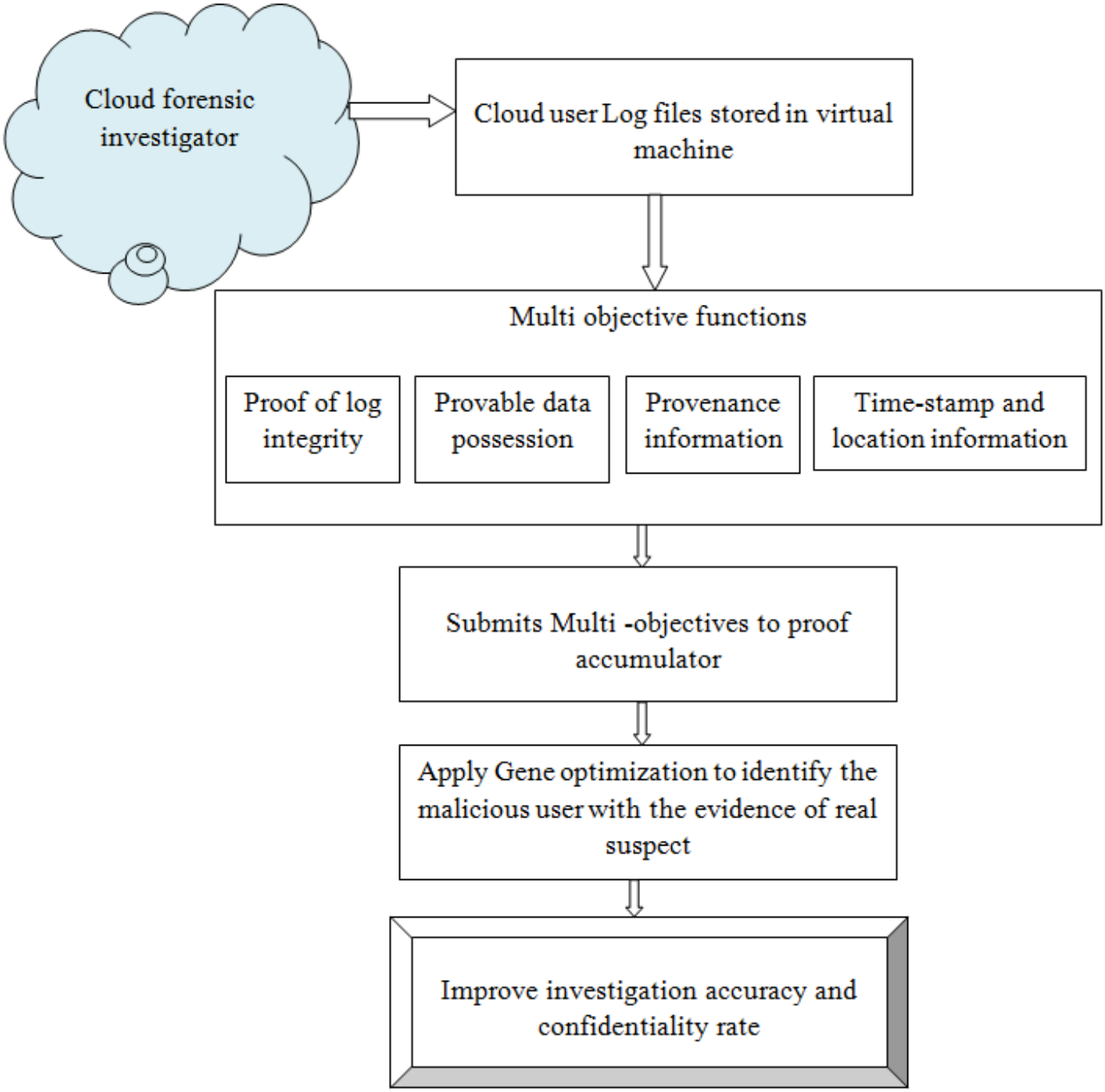

Figure 1 Architectural diagram of the Gene Optimized Multi-objective Proof Accumulator technique

Figure 1 shows the Architectural diagram of the Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique. The aim of the GOMOPA technique is to find the malicious user by validating the evidence with real suspect. This process is functioned by the cloud service provider (CSP). The CSP verifies the cloud log files which are stored in virtual machine to identify the malicious activities. The Multi objective functions are integrity, data possession, provenance information, time stamp information and location information. After submitting the evidence to the multi objective proof accumulator, the gene optimization approach is applied to identify the optimal solution (i.e. exact malicious user). This helps to improve the investigation accuracy and confidentiality rate. The brief explanation about the GOMOPA technique is presented in next sections.

2.1 Analysis of Multi objective function

The first step in the design of GOMOPA technique is the submission of the evidence (i.e. cloud user log files) to multi-objective proof accumulator by the investigator. The investigator submits the evidence about the malicious cloud user activities, evidence of integrity, provenance information, proof of data possession, time stamp and location information. Collected evidence about the malicious cloud user activities need to be preserved. Preserving the data is maintaining data integrity. In Data integrity, original data is not to be varied until the entire investigation process completed.

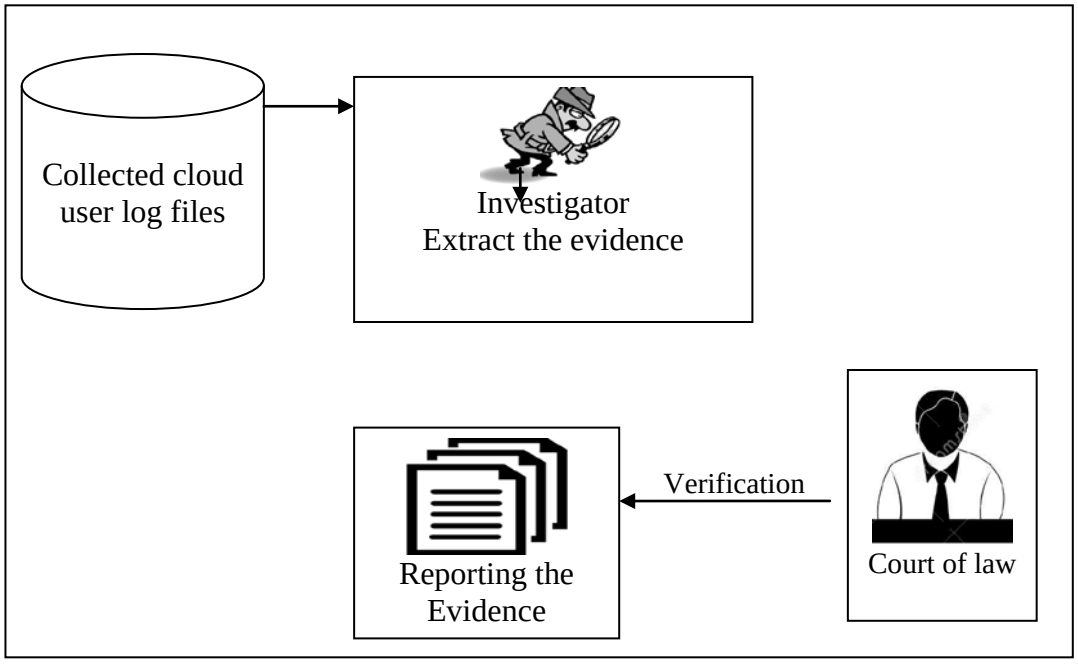

Figure 2 Cloud forensic models for crime investigation

Figure 2 shows the cloud forensic model for investigating the crime to identify the malicious user in cloud environment. Initially, the collected log files (i.e. evidence) are extracted by the investigator. Then, the extracted information is presented with real suspect to identify the malicious user. During the investigation process, multiple objectives are analyzed such as proof of integrity, provenance information, proof of data possession, time stamp information and location information.

2.1.1 Proof of integrity

In order to maintain the integrity of the evidence, a part of event related information is listed in chain of custody register which consists how, where and who launches the malicious activity over the cloud infrastructure. Chain of custody is the entire history of a portion of evidence. In ancient days, the chain of custody is based on filling in document forms or electronic forms which includes the name of investigators, a brief description of the evidence under inspection and a hash code. In recent days, chain of custody software is used closer with authenticity if the format allow the creation and maintenance of random metadata about fingerprint of evidences (what), events (how), digital signature (who), time stamping (when) and location (where). Therefore, this helps to better accepted and understood by court. Chain of custody maintenance is necessary for the forensic analysis that is functioned on a particular criminal case.

The malicious activities inside the cloud are identified by CSP and it facilitates the service to the authorized user. In any criminal investigation, the strength of information derived from inspection of the physical proof depends completely upon the care with which the evidence is preserved from contamination. In other words, if the evidence is not accurately handled, or stored, its value may be destroyed. Hence, it is important that the evidence is stored in a way that helps to guarantee their integrity. Then, the chances are increased that valuable information is extracted by examination and the proof is to be considered admissible in court proceedings. The integrity defines the original data is not changed up to the evidence submitted in front of law.

2.1.2 Provable data possession (PDP)

The PDP contains proof of data possession to prove whether the investigator possessed the actual evidence or not. These evidence are submits to proof accumulator. Content of the accumulator is the evidence of past data possession. An accumulator is a probabilistic data structure to prove whether a cloud user is a normal or not. In GOMOPA technique, tiger hash storage as a proof accumulator to store the information. Tiger/128 and Tiger/160 makes a hash length of 128 and 160 bits to offer compatibility. The tiger hash storage is used for secured cloud service provisioning and also achieving the higher confidentiality rate. The confidentiality is to guarantee the system only the authorized user receives the message from cloud server. One tiger hash stores the proof of all the cloud user log files of one static IP for a particular day. Accumulator stores the membership information in terms of a bit array. During the data possession generation, a cloud user transfers a file to server and creates the new log files in cloud environment. After getting an updated file, the CSP obtains the storage information of that specific user. The CSP hash the log files including the user

information and create the bit position from the hash value as well as updates the tiger hash with the current bit position. After that, the CSP store the updated tiger hash in the storage space. At the end of each day, the CSP retrieves the tiger hash entry of every cloud user (D_U) . Then, CSP hash the D_U and sign with its private key. Therefore, the proof of the data position (PDP) of that day is generated as,

$$PDP =< H(D_U), Sign_{PK}(H(D_U)), T > \quad (1)$$

From (1), where H (D_U) is the hash entry of every cloud user, $Sign_{PK}$ is the signature of H (D_U) with private key of the CSP, T is the time of proof generation. While increasing the number of cloud user log files, proof of data possession time gets increased and reduced the false positive probability during the malicious user identification. After computing the proof of data possession, CSP broadcast the proof of data possession with its public key on the web. The CSP keeps the information of entry of each cloud user with its private key secret to itself.

2.1.3 Data Provenance information

Provenance information is an essential feature for forensic analysis which describes the history of digital evidence. The secure data provenance method is used for digital forensics investigation with trusted evidence in cloud environment. This scheme proves that cloud data evidence is acceptable in court of law. The provenance scheme is used to preserve the records' integrity. It also satisfies the general data security properties and ensures the trustworthiness.

A GOMOPA technique handles a Provenance Store to store data provenance which is handled by CSP. Moreover, the proposed scheme stores the fundamental evidence similar to the data provenance.

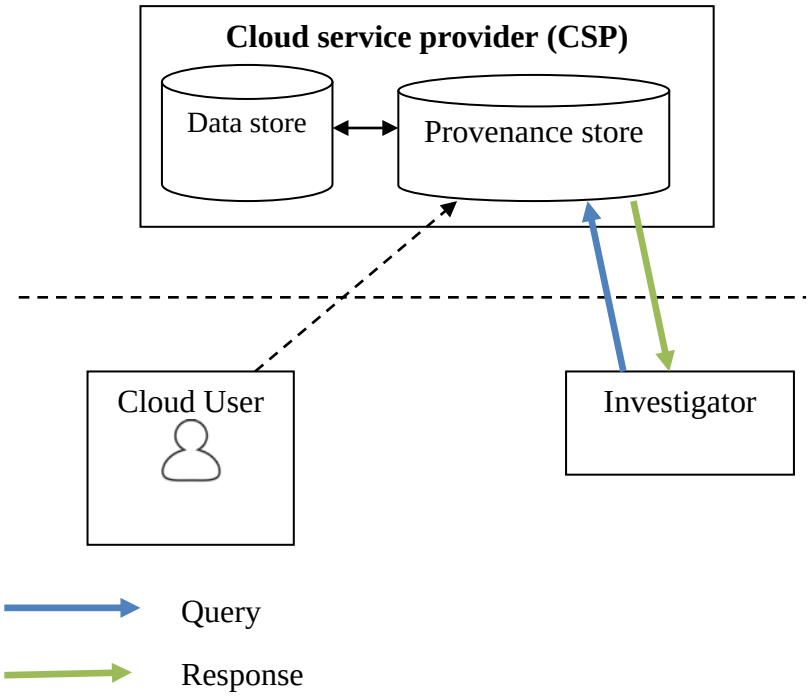

Figure 3 Data provenance in cloud

Figure 3 shows storing and searching data provenance in cloud environment. From the figure, Cloud User is a person who takes action and generates data provenance. It is handled in the trusted environment. An investigator is the one who reviews the actions taken by a cloud User. An investigator also verifies data provenance up to the origin and detects who launches the malicious activity on the source data. It is managed in the trusted environment.

CSP controls the source data and its equivalent data provenance in the cloud environment. In provenance method, a user performs an action on the source data and they forward the equivalent data provenance to the Provenance Store. Then, the investigator sends a query to the Provenance Store and a result obtained as the Response. The representation of the provenance information is shown in table 1.

Table 1 Representation of provenance information

Review	Date	Time	User ID	Action	Prior Review	Hash	Signature
1 2 ..					0 1 ..	128 Bits	512 Bits

From the table 1, review represents the version number. Data and time indicates when the event is occurred. User ID denotes who perform the action. An action column provides the information of activities taken on the source data. It is separated into four sections such as Name, Reason, Explanation and Location. Name illustrates what action is performed. Reason describes why the action is performed. Explanation provides more details that contain how the action is taken. Location

designates where the action is performed. Prior review represents the version number of the action taken on the similar source data previously. Hash is the transformation of current source data into a usually shorter fixed-length value after the action has been taken using tiger hash function. This helps to avoid the forge ability. Signature is accomplished after signing the hash of the above fields with the private key of the user who performs the action. This guarantees the confidentiality and avoids the repudiation.

2.1.4 Time stamp analysis

A timestamp is a series of information identifying when a crime event occurred in cloud environment. Generally, it provides date, time of day, and small fraction of a second. When the CSP publishes the proof of data possession day by day, the generation time of evidence is identified. It may either accurate generation time or a time range in which evidence is presented. Every record includes a stamp, time field and to report the evidence time. In Cloud Forensic investigation, time keeping state evaluation plays a significant role in Cloud Computing. A secure time-stamp verification protocol runs between the VMs. The time stamp information comprises the event recorded by year, month, day of the week, day, hour, minute, second and milliseconds. These times are then converted to Universal Coordinated Time (UTC) uses the local computer's time zone and daylight savings location. After that, the location of the crime incident is identified. Then the investigator extracts evidence and presents it to the court for trustworthiness verification.

Therefore, the objective functions proof of integrity, provenance information, proof of data possession, and the time stamp information are submitted to the proof accumulator. Then these objective functions are optimized based on the collected evidence through the gene based approach. Based on the gene optimization, the proposed GOMOPA technique investigates the collected evidence to identify the malicious user with real suspect.

2.2 Gene optimization to identify malicious user in cloud forensic services

Gene optimization approach provides population of multiple objective functions for providing the confidently direct to attain an optimal solutions at each generation. Optimization is a process of creating optimal evidence to prove the crime activities and identify the malicious user with real suspect. In GOMOPA technique, Multi-objective optimization aims to find a set of most feasible evidence in view of multiple objective functions and constraints. Therefore, the optimal solution is achieved by an accurate fitness assignment approach. Based on the fitness value, the proposed GOMOPA technique facilitates the determination of the malicious user by validating the investigated evidence with the real suspect which is performed by the CSP.

A gene optimization has several parameters, operators and processes which decide its arrival to an optimal solution for identifying the malicious user inside the cloud environment. Therefore, the optimization is a major concern for determining the optimal solution from the entire feasible solutions. Gene optimizations are implemented as chromosome-like data stored in cloud service provider. The fitness function is the measure of the quality of a particular solution. The fitness function is used to determine the most optimal solution from a multiple objective solution in a population. These objective function are optimized through the gene operators selection, crossover and mutation.

Every iteration, the number of evident (i.e. gens) are analyzed to find the malicious user. In general, every genes contains more than one objective functions, the choice of which gene is selected based on the information through the fitness calculation.

$$fitness\ function = identify\ the\ malicious\ user\ based\ on\ multi\ objective\ function \quad (2)$$

The investigation is carried out based on the objective function. Therefore, the malicious user is identified through the optimal evidence information which is stored in proof accumulator. If the evidence is not qualified to identify the malicious user, then the optimization is carried out through the selection, crossover and mutation operators. Finally, then the court is verified and detect the malicious user with the evidence of a real suspect.

Selection: In GOMOPA technique, the selection process in gene optimization is used to select the most objective function determined by the fitness function. The objective functions which are not optimal are removed.

Crossover: The crossover process in gene optimization is used to exchange characteristics between two different solutions. The pairs of solutions to alternate the uniqueness are selected randomly, until an entirely new generation of solution is attained. The newly generated results are used for performing the mutation operation to identify the malicious user based on the objective function. Let us consider, two genes $G_1 =< x_1, x_2, x_3, x_4 >$ and $G_2 =< y_1, y_2, y_3, y_4 >$ with the chromosomes x and y.

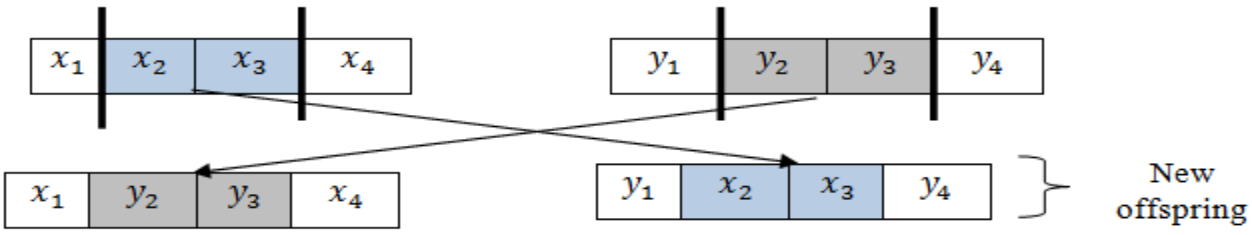

Figure 4 crossover process

Figure 4 shows the one point crossover to generate the new offspring by recombination process. A crossover point is selected according to the high quality chromosomes. Part of the chromosomes is exchanged after and before the crossover point to generate the new offspring by using parent chromosomes.

Mutation:

The mutation operation in gene optimization alters some bits of chromosome in a newly generated offspring. The changes occurred in the bits to confirm the evidence with the real suspect to identify the malicious user. The generated offspring are included into the population and the least chromosomes with low fitness values are removed from the population.

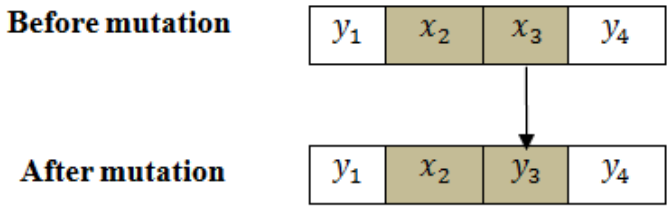

Figure 5 Mutation

As shown in figure 5, the mutation operation is performed and the new offspring chromosome value of the gene x_4 is changed with the exact chromosome of y_3. Mutation is the process of randomly interchanging the chromosome for creating the new offspring to increase the fitness value. If the newly offspring is failed to satisfies the fitness threshold, it is removed and the iterations gets repeated. The mutation process is used to avoid the local minimum and it searches for the global optimal solution. Therefore, the GOMOPA technique effectively determines the malicious user by obtaining the investigated evidence with the real suspect which is handled by the CSP. The GOMOPA technique efficiently identifies the real suspect who launches the malicious activities over the cloud infrastructure. The algorithmic description of the GOMOPA technique is described as follows to improve malicious user identification accuracy with minimum time in cloud forensic environment.

Input : No. of genes (i.e. evidence), Two parent gene with chromosomes $G1 =< x_1, x_2, x_3, x_4 >$ and $G2 =< y_1, y_2, y_3, y_4 >$
Output : identify the malicious user in cloud
Step 1 : Begin
Step 2: For each investigated evidence
Step 3: Calculate the fitness value
Step 4: if (fitness ≥ threshold) then
Step 5: Number of iteration has been completed and identify the malicious user
Step 6: Selecting more optimized objective function in each iteration
Step 7: Perform crossover operation generates new solution
Step 8: Perform mutation operation
Step 9: Obtain the global optimized solution to identify the malicious user
Step 10: End if
Step 11: End for
Step 12: End

Figure 6 Gene Optimized Multi-objective Proof Accumulator algorithm

As shown in figure 6, the Gene Optimized Multi-objective Proof Accumulator algorithm is described. For a number of evidence, gene population generation is initialized to identify the malicious user through fitness value calculation. Based on fitness calculation, an optimal objective functions are selected with the specified threshold value. If the fitness is greater than the threshold value, the iteration gets stopped otherwise the selection process is carried out. Based on selection, the malicious user is identified with evidence of real suspect to improve the confidentiality. Then, the crossover is performed to generate the new optimal solution. Finally, the mutation is performed to identify the exact malicious user. This process is repeated until the entire evidence is verified. This helps to improve the malicious user identification accuracy with minimum time.

III. EXPERIMENTAL EVALUATION

An effective Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is introduced using java language with CloudSim network simulator. The CloudSim simulator uses Amazon EC2 dataset to identify the malicious user. The CloudSim simulator performed on Cloud environment provides different cloud services with the presented resources. The particular toolkit is selected as a simulation platform in Cloud environments. The Cloudsim requires minimum time to identify the malicious user in cloud forensic environment. The performance evaluation of GOMOPA technique compared with existing approach SecLaaS Scheme [1] and A Forensic Open-Stack Tools (FROST) [2]. The following metrics such as, investigation accuracy, processing time and confidentiality rate are evaluated to improve the performance of GOMOPA technique.

IV. RESULT ANALYSIS

To perform the analysis of the proposed Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is compared with existing SecLaaS Scheme [1] and A Forensic Open-Stack Tools (FROST) [2]. Experimental analysis is carried out with different parameter such as investigation accuracy, processing time and confidentiality rate using Amazon EC2 dataset. Performance is evaluated along with the following metrics with help of tables and graph values.

4.1 Impact of Investigation accuracy

Investigation accuracy is measured as the ratio of the number of malicious user identified to the total number of cloud users. It is measured in terms of percentage (%). The mathematical formula for investigation accuracy is measured as follows,

$$Investigation\ accuracy = \frac{(No.of\ cloud\ user - No.of\ malicous\ users)}{No.of\ cloud\ users} * 100 \quad (3)$$

Table 2 Tabulation for investigation accuracy

Number of cloud users	Investigation accuracy (%)		
	GOMOPA	SecLaaS scheme	FROST
10	80.12	60.10	58.35
20	82.45	63.48	60.13
30	83.67	65.10	63.14
40	85.10	68.52	65.75
50	87.46	70.13	68.12
60	89.10	73.65	70.41
70	92.13	75.42	72.54
80	93.45	77.10	75.47
90	95.75	79.65	77.42
100	98.61	82.56	79.24

Table 2 describes the investigation accuracy to identify the malicious user inside the cloud environment among the number of cloud users through reporting the admissible evidence with real suspect. The proposed GOMOPA technique improves the investigation accuracy with existing SecLaaS Scheme [1] and FROST [2].

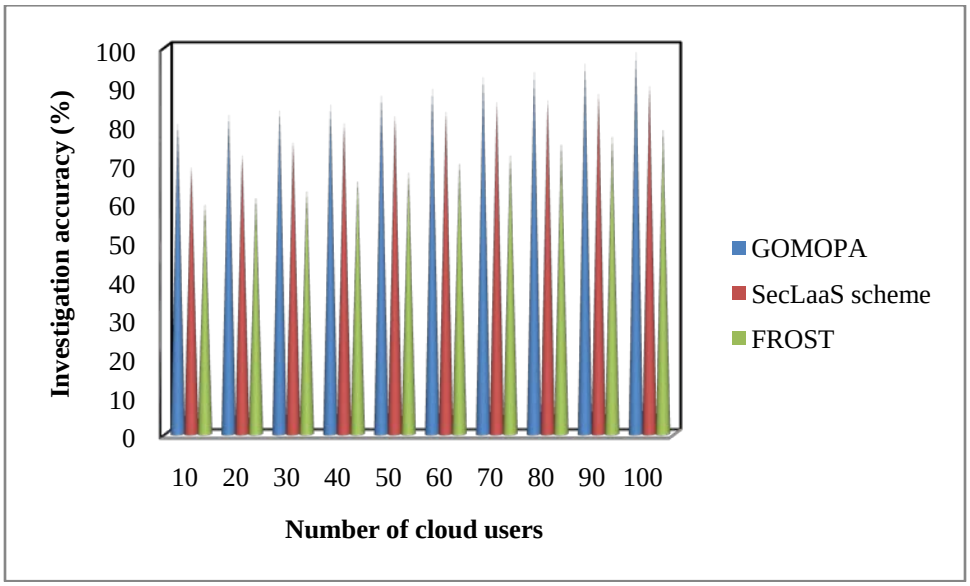

Figure 7 Measure of Investigation accuracy

Figure 7 shows the analysis of Investigation accuracy with respect to number of cloud users. For the experimental evaluation, the number of cloud user is varied from 10 to 100. While increasing the number of cloud user, the investigation accuracy gets increased in proposed GOMOPA technique than the existing methods. This is because; Gene Optimized Multi-objective Proof Accumulator effectively proves the malicious activities. In GOMOPA technique, the investigator presents proof of malicious activity, evidence of integrity, provenance information, evidence of data possession, time stamp information and location information to the multi-objective proof accumulator. Then the proposed gene optimization is performed to attain the optimal solution based on the fitness function. In gene optimization, the evidence with the multiple objective functions is selected and performs the crossover operation to generate a new optimal solution. Finally, Mutation is performed to detect the exact malicious user identified with real suspect who launches the malicious activities over the cloud infrastructure with the evidence of real suspect. This process is repeated until the entire evidence is validated. This helps to improve the investigation accuracy. Therefore, the investigation accuracy is considerably increased by 9% and 28% compared to existing SecLaaS Scheme [1] and FROST [2] respectively.

4.2 Impact of processing time

Processing time is defined as an amount of time taken to detect the malicious user based on reporting the admissible evidence. The processing time is measured as follows,

$$PT = Number\ of\ cloud\ users * Time\ (identify\ the\ malicious\ user) \quad (4)$$

From (4), where PT is the processing time which is measured in terms of milliseconds (ms).

Table 3 Tabulation for processing time

Number of cloud users	Processing time (ms)		
	GOMOPA	SecLaaS scheme	FROST
10	18.24	25.12	30.12
20	22.45	30.14	33.48
30	25.54	33.47	36.14
40	30.12	38.11	40.12
50	33.54	42.55	44.25
60	38.46	45.47	48.79

70	40.25	48.78	50.10
80	45.35	51.47	53.46
90	48.75	53.42	56.12
100	55.69	56.13	64.25

As shown in table 3, processing time is measured based on the number of cloud users in cloud environment. Among the several users, the time taken to identify the malicious users is reduced in proposed GOMOPA technique compared with existing SecLaaS Scheme [1] and FROST [2]. The result of the processing time is shown in figure 8.

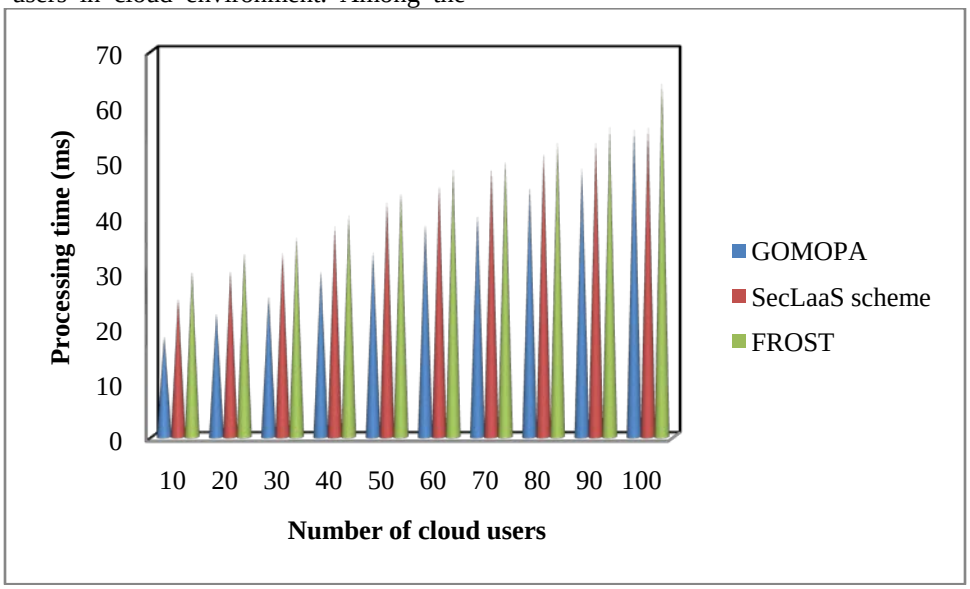

Figure 8 Measure of processing time

As shown in figure 8, the processing time of the malicious user identification is performed with the number of cloud users. As shown in figure, the proposed GOMOPA technique reduces the processing time than the existing methods. This significant improvement in proposed GOMOPA is attained by applying the gene optimization approach. The GOMOPA contains the information about the malicious activities. In GOMOPA, integrity provides the original data which is not changed until the evidence is submitted. Then the provenance information is presented which describes the history of digital evidence to show that malicious user in court of law. Proof of data possession is generated and reduced the false positive probability during the malicious user identification. Then the time analysis is carried out to identify the malicious event occurred in cloud environment. Finally, the location of the crime event is identified. These multiple objective functions are submitted to the proof accumulator. From that, the gene optimization is carried out to find the exact malicious user with minimum time. Therefore, the processing time is significantly reduced by 17% and 23% compared to existing SecLaaS Scheme [1] and FROST [2] respectively.

4.3 Impact of confidentiality rate

The confidentiality is the ability of the system to protect the cloud user log files from the unauthorized access in cloud environment. It is measured in terms of percentage (%). The formula for confidentiality rate is measured as follows,

$$confidentiality\ rate = \frac{Number\ \ of\ log\ files\ are\ protected}{Number\ \ of\ cloud\ \log\ files} * 100 \quad (5)$$

Table 4 Tabulation for Confidentiality Rate

Number of cloud log files	Confidentiality rate (%)		
	GOMOPA	SecLaaS scheme	FROST
5	79.35	63.36	44.68
10	82.45	69.89	48.20
15	83.64	70.23	52.65
20	85.11	72.54	56.78
25	87.42	73.58	60.12
30	89.69	75.86	63.58
35	90.10	80.17	68.45
40	92.77	82.65	75.12
45	94.36	83.52	79.25
50	95.42	85.46	82.36

Table 4 clearly describes the confidentiality rate with the number of cloud user log files. Higher confidentiality rate is achieved in GOMOPA than the existing SecLaaS Scheme [1] and FROST [2].

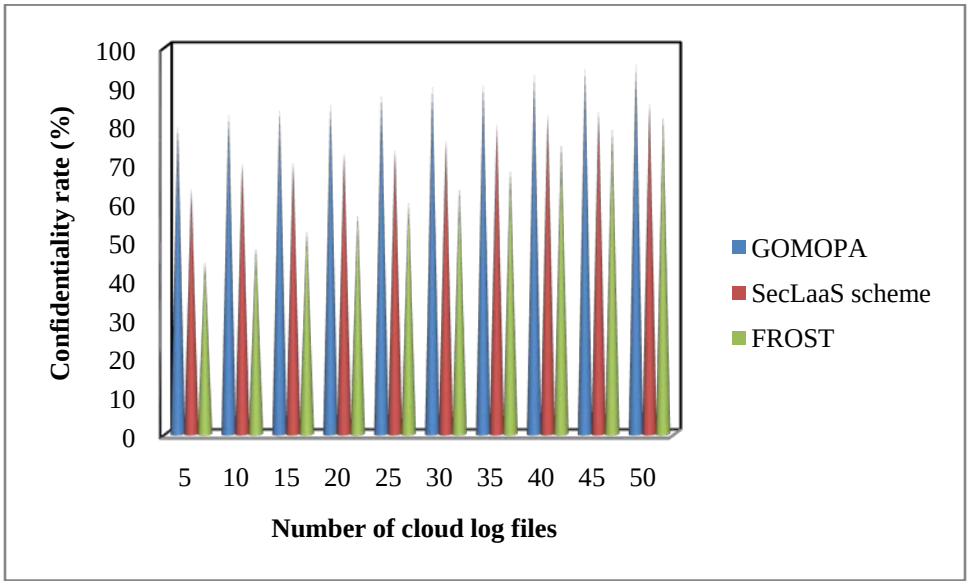

Figure 9 Measure of confidentiality rate

As shown in figure 9, measure of confidentiality rate is obtained with number of cloud user log files. From the figure, it is clearly evident that the proposed GOMOPA improves the confidentiality rate than the existing methods. This considerable development is obtained by optimizing the multi objective function which is stored in proof accumulator. While reporting the evidence (i.e. log files), the proposed GOMOPA significantly protects the multiple log files from the unauthorized access. In GOMOPA, gene optimization approach determines the malicious user by validating the investigated log files as the evidence of a real suspect. This process is functioned by the CSP. This helps to preserve the privacy level of the cloud user log files simultaneously ensures confidentiality. Therefore, the GOMOPA technique protects the evidence as the cloud user log files from the unauthorized access. This helps to improve the confidentiality rate by 17% and 43% as compared to existing SecLaaS Scheme [1] and FROST [2] respectively.

Therefore, a Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique improves the malicious user identification by reporting the evidence and to show the crime activities within the cloud.

V. RELATED WORKS

An architecture of cloud computing was designed in [11] using various tools in different locations that reduce the chance to seize the information. But, it failed to conduct forensic investigation on cloud. The GOMOPA effectively performs the investigation on cloud forensic and improves accuracy to identify the malicious user.

A Security Information and Event Management (SIEM) approach was introduced in [12] to collect the proof for cloud forensics investigation. However, the optimization of the evidence was not solved for forensics purpose. The gene optimization is used in GOMOPA to select the optimal evidence.

A digital forensics investigation procedure and the digital forensics as a service (DFaaS) model were analyzed in [13]. But, the multiple objective functions were not investigated. The GOMOPA improves the investigation accuracy with minimum time.

A Cloud Forensics Investigation Team (CFIT) was presented in [14] to improve the trustworthiness of the CSP. But, it failed to identify the malicious user effectively. The GOMOPA efficiently identifies the malicious user in cloud environment.

An efficient analysis of cloud forensics challenges, their feasible solutions relating to various phases of the forensic process, and brief analysis of the selected results was presented in [15]. But the secure provenance played a critical part in cloud forensics. The GOMOPA effectively perform the data provenance to identify the history of evidence.

A novel digital forensics construction for RSA signature in cloud computing was introduced in [16] to achieve the privacy. However, it requires large storage space for storing multiple files. The GOMOPA uses less storage space for storing the log files using tiger hash storage function.

A forensic triage as a real-time calculation difficulty with particular technical requirements was formulated in [17]. But an investigation on multiple objective functions in cloud forensic remained unaddressed. The GOMOPA significantly performs the investigation on multiple objective functions to identify the malicious user.

In [18], an overview of multiple challenges was created through digital forensics in cloud environment. However, it failed to identify who launch the malicious activities in cloud environment. The GOMOPA effectively identified the malicious activities with the evidence of real suspect.

The description of cloud computing with the computer forensic was explained in [19] but the integrity was not achieved effectively. The GOMOPA obtains higher integrity rate through the entire process.

A novel secure provenance method was introduced in [20] based on group signature and attribute-based signature process. However, an effective investigation was not carried out. The GOMOPA performs efficient investigation to identify the accurate malicious user based on reporting the admissible evidence.

As a result, Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique reports acceptable proof of suspect in cloud forensic services for identifying the malicious user inside the cloud environment.

VI. CONCLUSION

A Gene Optimized Multi-objective Proof Accumulator (GOMOPA) technique is introduced to report the acceptable evidence and identify the malicious user in the cloud. In GOMOPA, cloud forensic investigator reports the evidence of malicious activities and multiple objective functions to the proof accumulator. An accumulator contains multiple objective functions. These objective functions are optimized through the gene based approach. Among the multiple functions, the GOMOPA optimizes the global optimum solution to identify the malicious user through the fitness calculation. Then, the optimization operators such as selection, crossover and mutation are carried out to identify the user who initiates malicious activities with the evidence of real suspect. In addition, the GOMOPA secures the confidentiality of the cloud users' log files. Experimental evaluation is carried out the proposed GOMOPA to evaluate the performance parameters such as investigation accuracy, processing time and confidentiality rate with cloudSim simulator. The result shows that the GOMOPA technique improves investigation accuracy with minimum processing time and also improves the confidentiality rate than the state-of-the-art methods.

REFERENCES

[1] Shams Zawoad, Amit Kumar Dutta ,Ragib Hasan, "Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service", IEEE Transactions on Dependable and Secure Computing ,Volume 13, Issue 2, 2016 , Pages 148 – 162

[2] Josiah Dykstra and Alan T. Sherman, "Design and implementation of FROST: digital forensic tools for the open stack cloud computing platform", Digital Investigation, Elsevier, Volume 10, 2013, Pages 87–95

[3] Ben Martini and Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, Elsevier, Volume 9, Issue 2, 2012, Pages 71–80.

[4] Flavio Cruz, Andreas Moser, Michael Cohen, "A scalable file based data store for forensic analysis", Digital Investigation, Elsevier, Volume 12, 2015, Pages 90-101

[5] Sean Thorpe, Indrajit Ray, Tyrone Grandison, Abbie Barbir, "Cloud Digital Investigations based on a Virtual Machine Computer History Model", Future Information Technology, Application and Service, Springer, Pages 741-745

[6] Zhen Xu, Cong Wang, Kui Ren, Lingyu Wang, Bingsheng Zhang, "Proof-Carrying Cloud Computation: The Case of Convex Optimization", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 11, 2014, Pages 1790 – 1803

[7] Zhen Chen, Fuye Han, Junwei Cao , Xin Jiang, Shuo Chen, "Cloud computing-based forensic analysis for collaborative network security management system", Tsinghua Science and Technology, Volume, 18, Issue 1, 2013, Pages 40 – 50

[8] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Salman Iqbal, Ahmed Abdelaziz, Omar Adil Mahdi, Abdelmuttlib Ibrahim Abdalla Ahmed,Muhammad Shiraz, Yusor Rafid Bahar Al-Mayouf, Ziar Khan, Kwangman Ko, Muhammad Khurram Khan, Victor Chang, "Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis", IEEE Access, Volume 4, 2016, Pages 9800 – 9820

[9] Farhood Norouzizadeh Dezfoli, Ali Dehghantanha, Ramlan Mahmoud, Nor Fazlida Binti Mohd Sani and Farid Daryabar, "Digital Forensic Trends and Future", International Journal of Cyber-Security and Digital Forensics (IJCSDF), Volume 2, Issue 2, 2013, Pages 48-76

[10] Keyun Ruan, Joe Carthy, Tahar Kechadi, Ibrahim Baggili, " Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey result", Digital Investigation, Elsevier, Volume 10, 013, Pages 34–43

[11] **Ghania Al Sadi, "Cloud Computing Architecture and Forensic Investigation Challenges", International Journal of Computer Applications, Volume 124, Issue 7, 2015, Pages 20-25**

[12] Muhammad Irfan, Haider Abbas, Yunchuan Sun, Anam Sajid and Maruf Pasha, "A framework for cloud forensics evidence collection and analysis using security information and event management", Security and Communication Networks, 2016

[13] R.B. van Baar, H.M.A. van Beek, E.J. van Eijk, "Digital Forensics as a Service: A game changer", Digital Investigation, Elsevier, Volume 11, 2014, Pages 54–62

[14] Sheik Khadar Ahmad Manoj, D.Lalitha Bhaskari, "Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment", Procedia Computer Science, Elsevier, Volume 85, 2016, Pages 149 – 154

[15] Ameer Pichan, Mihai Lazarescu, Sie Teng Soh, "Cloud forensics: technical challenges, solutions and comparative analysis", Digital Investigation, Elsevier, Volume **13,** 2015, Pages 38–57

[16] Chu-Hsing Lin, Chen-Yu Lee and Tang-Wei Wu, "A Cloud-aided RSA Signature Scheme for Sealing and Storing the Digital Evidences in Computer Forensics", International Journal of Security and Its Applications, Volume 6, Issue 2, 2012, Pages 241-244

[17] Vassil Roussev, Candice Quates, Robert Martell, "Real-time digital forensics and triage", Digital Investigation, Elsevier, Volume 10, 2013, Pages 158–167

[18] Deoyani Shirkhedkar and Sulabha Patil, "Analysis of Various Digital Forensic Techniques for Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 5, Issue 4, 2014, Pages 104-107

[19] Agreeka Saxena, Gulshan Shrivastava, Kavita Sharma, "Forensic Investigation in Cloud Computing Environment", International Journal of Forensic Computer Science, Volume 2, 2012, Pages 64-74

[20] Jin Li, Xiaofeng Chenb, Qiong Huangc, Duncan S. Wongd, "Digital provenance: Enabling secure data forensics in cloud computing", Future Generation Computer Systems, Elsevier, Volume 37, 2014, Pages 259–266

AUTHORS

First Author – Ms.Sripriya Arunachalam, Research Scholar , Department Of Computer Science, Vels University
Second Author – Dr. M. Sundara rajan, Assistant Professor, Department Of Computer Science Government Arts College , Nandanam