Designing and Analysis of User Profiling System for Cloud Computing Security using Fuzzy guided Genetic Algorithm

Sahil
Punjab Institute of Technology Kapurthala
(PTU Main Campus)
Kapurthala, India
sahil.neelam@hotmail.com

Sandeep K. Sood
Guru Nanak Dev University
Regional Campus
Gurdaspur, India
san1198@gmail.com

Sandeep Mehmi
Punjab Institute of Technology Kapurthala
(PTU Main Campus)
Kapurthala, India
sandeep.mehmi@gmail.com

Shikha Dogra
Punjab Institute of Technology Kapurthala
(PTU Main Campus)
Kapurthala, India
shikha.dogra@outlook.com

Abstract— On one side the Cloud Computing offers scalable virtual computing resources in the form of web-services on pay-as-you-go basis; but on other side, it also raises the concerns regarding the security threats to the Cloud environment from outside and inside the environment. The existing security systems are not able to withstand the dynamic nature of threats, so some sort of augmentations are required to the existing security systems which will enable the security systems to work in more prominent way. Inter-VM attacks possess such kind of threats from inside the Cloud environment. User profiling can be helpful in this situation by analyzing the usage patterns of the users and by providing the plausible interpretation from those usage patterns to the security system and then, the security system, based on those interpretations, act in reactive and proactive manner to the analyzed threat situation. This paper is the based on the findings from our last paper, where we had found that the designing of User Profiling System based on Artificial Intelligence techniques: Fuzzy and Genetic Algorithms are individually not sufficient to deliver a comprehensive User Profiling System but it might be possible to use these two approaches in a hybrid way to design a comprehensive User Profiling System for Cloud Computing security. Hence, we used hybrid approach Fuzzy guided Genetic Algorithm to design a User Profiling System and found that it covered all the research gaps, which we had analyzed in our previous work and even it fulfill all the seven principles of the evaluating framework.

Keywords— One-time ownership cost model; Fuzzy Systems; Genetic Algorithms; Genetic Engineering; Distributed Computing; Virtual Computing; IDEs; Pay-as-you-go; Datacenters; E-assests

I. INTRODUCTION

Cloud Computing is emerging as the next-generation solution to dynamic and costly one-time ownership costing of computing resources. But, along with the advent of Cloud Computing, there also have come threats to Cloud Computing environment from inside and from outside the Cloud Computing environment, which are not being properly handled by the existing security systems alone. So, in this dynamic threat scenario, some sort of augmentations to the existing security systems can play a vital role in this context. User Profiling System is such an augmentation to existing security systems, where using profile analysis of the user, a security system can act in reactive and proactive way. Our last paper [1] highlights the research gaps in designing the User Profiling System using Artificial Intelligence techniques, where we showed that the Artificial Intelligence techniques: Fuzzy Systems and Genetic Algorithms were not sufficient in designing a comprehensive User Profiling System based on their individual implementation and suggested that a hybrid technique using Fuzzy guided Genetic Algorithm might be used to design a comprehensive User Profiling System. In this paper, we worked on this concept of hybrid approach to design a comprehensive User Profiling system for Cloud Computing security. Our work has following contributions in the field of designing a User Profiling System using Artificial Intelligence techniques:

- Study of conventional Artificial Intelligence techniques: Fuzzy Systems and Genetic Algorithms, in the context of designing a User Profiling System for Cloud Computing security.
- Identification of a reference model for evaluating the comprehensiveness of the User Profiling System.
- Analysis of a new hybrid approach, Fuzzy guided Genetic Algorithm in the context of designing a User Profiling System for Cloud Computing security.
- Introduction of special case of mutation to Elite users in Genetic Algorithms.

The second part of the paper discusses the background to the field of Cloud Computing and its security domain. The third part provides insight to the basis of our proposed work along with discussion about the User Profiling System and Artificial Intelligence. Fourth part cites some of the prominent and related works to our research work. The fifth part presents the structure of evaluating framework for our experiments, which comprises of seven principles, indicates how reliable a security system is. Sixth part of the paper presents the system modeling of the proposed approach, where the seventh part presents the design algorithms (or methodology) for our proposed system; result outcomes from the implementation; performance evaluation of the existing and proposed experiments. Last part presents the conclusion statements and future scope of our research work.

II. Background

In this era, where everything is available to individuals based on its utility, from electricity, gas to water [2]; the computing is emerging as the next-level utility. Best scenario for utility computing is well depicted through Cloud Computing, where computing resources are availed according to the user's need unlike of one-time ownership cost model of computing resources. Cloud Computing [3] is nothing more than a metaphor of the collaboration of some existing technologies [4] to handle shared and distributed computing resources in a coordinated manner to provide virtual computing resources like: computing power, storage, IDEs, softwares, OS etc., over the internet and the cost charging of computing resources is based on the amount of units used.

But the concerns regarding the security of Cloud environment [5] have originated from the basic concepts of Cloud Computing, where everything in Cloud environment is actually not present on the user premises, but somewhere else on the Cloud-provider premises (not known to user), on shared basis with other Cloud-users. So, security concerns regarding the privacy breach of user data; exposure of one's data to someone else, who is also using the same Cloud services, might access the same Datacenter of that Cloud-provider; the management of data by Cloud provider in different regions having different regulation policies etc., hinder the users to show interest in adopting the Cloud Computing as the next-level of computing and to getting the benefits of economical and scalable computing resources. That's why the security of Cloud Computing is one of the main research areas where efforts are being invested for providing assurance to users regarding security concerns.

III. User Profiling System

Security systems are exclusively not enough to handle the highly dynamic nature of threats to the Cloud environment. Some sorts of augmentations are needed to make up the security mechanisms to withstand the dynamic nature of threats. In this context, user profiling [6] can play a vital role in the domain of inter-vm attacks, where a user from inside the Cloud environment tries to harm the other Cloud-user by attacking on latter's e-assets on the same datacenter. There, user profiling can act as a watch dog and analyze user activities to find the traces of any unwanted malicious behavior within the environment. User Profiling Systems [7] are such systems, where user's behavioral patterns are analyzed and a plausible interpretation of these behaviors are made and provided to the security systems; so, appropriate and reactive or proactive, on-time counter measures could be taken.

Artificial Intelligence [8] is the concept of machine learning, where activities are exhibited in resemblance to human thinking like capabilities of reasoning, perception, decision making etc., by machines and softwares. Artificial Intelligence helps User Profiling System in building structural models to analyze the user behavior by extracting useful information from the various unstructured data of user activities and classify them to characterize their usage patterns and to identify the behaviors of significant interest, which will enable a security system to work in more potent way.

In our last paper [1], we showed how User Profiling Systems based on two different Artificial Intelligence techniques: Fuzzy Systems and Genetic Algorithms worked; analyzed their individual performances and concluded their respective research gaps. We concluded that the both User Profiling Systems were not able to withstand the intended goal of designing a comprehensive User Profiling System for Cloud Computing security. The brief description of finding from our last paper [1] as:

A. *User Profiling System based on Fuzzy Logics*

This system had initially used to enumerate the character of a user based on the current lifecycle usage activities and profiled it. But when it used to enumerate the character based on the next lifecycle usage activities and profile history of the user, it had changed the character of the user from the previous lifecycle character i.e. from Safe to Malicious or Highly Malicious, Malicious to Safe or Highly Malicious and from Highly Malicious to Safe or Malicious without any reasonable logic. We analyzed that, as our system had no mechanism for limiting the authorized resources based on the previously enumerated character, then how the character of a culprit can be changed from Malicious or Highly Malicious to Safe without any policing.

We evaluated the outcomes from our experiment based on the reference model [12] having seven identified principles for building a Risk Indicator System to validate security system's reliability and found that two of the principles were not fulfilled (TABLE I). So, we have concluded that the Fuzzy systems could only be used for profiling user activities and building behavior patterns, but not for analyzing them.

B. *User Profiling System based on Genetic Algorithm with Genetic Engineering(GAGE)*

In our second experiment, where we tried to design User Profiling System using Genetic Algorithm with Genetic Engineering, where system had initially used to search for Malicious and Highly Malicious users (because Genetic Algorithm search chromosomes, here user-profiles; based on their fitness) and recommend the amount of limitation of their authorized resources based on the defined crossover and mutation schema (because of Genetic Engineering). But, in the subsequent usage lifecycles, when User Profiling System used to search for lesser fit individuals, it took only initially profiled Malicious and Highly Malicious users because a Genetic Algorithm always pick the lesser fit individuals and limited their authorized resources further. After some subsequent usage lifecycles, a point had used to come where resource authorization to Malicious and Highly Malicious users got fully restricted and they would not be able to use authorized resources anymore. We analyzed that the GAGE had no capability to profile and build the behavior patterns, because after limiting the less fit (Malicious and Highly Malicious) user's authorized resources, there might be change in their behavior, which would be reflected in next time behavior evaluation, but here in our system, the less fit users remained less fit, even after many usage lifecycles and being kept on getting resource limitation until the authorized resources to them get fully restricted.

We evaluated the outcomes from this experiment based on the reference model [12] having seven identified principles for building a Risk Indicator System to validate security system's reliability and found that two of the principles were not fulfilled (TABLE I). So, we have concluded that the Genetic Algorithms could only be used for analyzing behavior patterns of interest, not for building them.

In this paper, we have focused on these research gaps and propose a new hybrid approach to design a User Profiling System, which is evaluated on the same reference model [12] and proved it's comprehensibility in context of designing a User Profiling System for Cloud Computing security.

IV. Related Works

Multifaceted distinguishing works in the direction of designing a profiling system include: the profiling based on the analysis of user's mobile device usage data [6] to detect any misusage by different threat programs and to provide protection in a transparent and continuing way to mobile devices. Another work [9] explores the vulnerabilities on shared virtual platforms and demonstrates, how a cross VM side-channel attack can be mounted to gain access to private information of the target Virtual Machine. K. Xu, F. Wang, and L. Gu [10] introduced various challenges faced in enhancing Cloud environment security, which includes: vast and diverse traffic of cloud tenants; dynamic and variety of threats from traditional environment to the threats from Cloud computing environment; attack origins from inside and outside the cloud environments. They also proposed Profiling as a Service, where network traffic is analyzed and characterized at various levels: at Cloud networks' gateway routers, at hypervisor (at virtual servers) and at VM (at host level). A paper [11] had a study on how Artificial Intelligence played an active role in diagnose the problem of Power quality in the field of electric power distributions, which was one of the main inspiration for our work to consider Fuzzy Systems and Genetic Algorithms to design a User Profiling System for Cloud Computing security. The Artificial Intelligence tools like Fuzzy and Genetic Algorithms are helpful in analyzing and characterizing the data and provide a plausible interpretation of the problem, so response system could take action accordingly. A very characteristic work [12] presented the vision about how to avoid negative security events and the need to check any security risk as early as possible along with explaining a framework based on seven principles to build Security Risk assessment indicator system. In reference to a paper [1], authors experimented with two artificial intelligence techniques to design a User Profiling System and presented the research gaps based on the analysis of outcomes from the experiments and envisioned the possibility of using Fuzzy and Genetic Algorithms in a hybrid approach to design a comprehensive User Profiling System for Cloud Computing security.

V. Evaluating Framework

We evaluated our experiments on seven principles identified for building a Cloud Computing security risk indicator system [12], which evaluates the integrity and reliability of a security system. Our evaluating framework is based on the following seven principles, by fulfilling which, a User Profiling System ensures its own integrity and reliability and overall the reliability of the augmenting Cloud Computing security:

1. ***Scientific:*** Scientific methods are the ultimate assurance for the reliability of a risk indicator system, on which it is built upon.
2. ***Complete:*** An indicator system should cover all key risk indicators.
3. ***Systematic*:** Risk indicators should be deployed in a systematic and proper hierarchy and must be interconnected and interdependent, at same time having no intersections as well.
4. ***Feasible:*** Indicator system should be as simple as possible using appropriate indicators and must be feasible.
5. ***Quantitative:*** Qualitative and quantitative aspects of a system play a vital role in quality management. So, the system must have clear and exact calculation procedures.
6. ***Guided:*** The goal of the system should guide the functioning of the system.
7. ***Expandable:*** The structure of indicator system should be opened to future adaptations and to meet certain circumstances.

VI. System Model

The motivation behind our research work was to design a User Profiling System with Artificial Intelligence techniques, which would be a comprehensive User Profiling System to augment the Cloud Computing security. Based on the findings from our experiments [1] with Fuzzy Systems and GAGE (Genetic Algorithms and Genetic Engineering), we have proposed a hybrid approach using Fuzzy guided GAGE (Genetic Algorithm with Genetic Engineering) for designing a User Profiling System, where Fuzzy and GAGE complements each other to cover one another's research gaps found after the designing of User Profiling System; and delivers a comprehensive User Profiling System, which is more effective to the security system in Cloud.

Because of this hybrid approach, the issue of changing the characters of users without limiting the authorized resources of the Malicious and Highly Malicious users is now addressed by Genetic Algorithm, which now searches for Malicious and Highly Malicious users and the Genetic Engineering limit the resources authorized to Malicious and Highly Malicious users based on the defined crossover and mutation schema (Fig. 1). Whereas the issue of GAGE (Genetic Algorithm with Genetic Engineering), where algorithm goes ineffective after some subsequent usage lifecycles because of the limiting of resources of the same users (which were Malicious and Highly Malicious initially) in subsequent lifecycles (generations) and a point has comes where resources get fully restricted; is addressed by the Fuzzy System, which changes the characters of users, after each lifecycle based on GAGE's recommended limitation of resources, because after limiting the less fit (Malicious or High Malicious) user's authorized resources, there might be change in its behavior, which would be reflected in next time behavior evaluation. Consequences of which, on the next lifecycle, GAGE (Genetic Algorithm with Genetic Engineering) algorithm gets the users who are currently having the changed characters to Malicious and Highly Malicious (based on Fuzzy's determination of character change, in reflection to the changed authorized resources, which changed the usage pattern of the users and consequences of which, there's also change in users' characters), unlike of User Profiling System using GAGE, where the same users which were initially profiled as the Malicious and Highly Malicious were kept on getting resource limitation all the times, until their resources got fully restricted. Now, after each usage lifecycle, the characters of the users will be changed and GAGE will search different users next time and crossover and mutate only searched less fit users in the current lifecycle, not the users who were initially characterized less fit.

But during the implementation of Hybrid approach, we analyzed that there might be a situation, where authorized resources to a user get fully restricted after attaining Malicious or Highly Malicious character for many times at different lifecycles. So, after got fully restricted resources, a user would be restricted to involve in any type of activity and would attain Safe character after some lifecycles (because fully restricted user would not be allowed in any activity, then how it could be characterized to a Malicious or Highly Malicious user). At that instance of time, Safe user would have full restriction to authorized resources. So to resolve this issue, we also propose a special case of Mutation to Elite users.

A. *Special Case of mutation to Elite users (optimization to Genetic Algorithm)*

After getting the full restriction to the authorized resources of Malicious and Highly Malicious users, they are remain fully restricted for subsequent lifecycles, but because of the full restriction to use authorized resources, their characters changed to Safe (ELITES). But they remains fully restricted for the rest of the lifecycles, because GAGE (Genetic Algorithm with Genetic Engineering) doesn't consider them for crossover or mutation because of elite users and pass them as such to the next generation (because ELITES are fittest of all and don't require crossover or mutation) and falls in loop and don't be able to get resources in any future. So to resolve this problem, we introduce a special case of mutation to ELITES (Fittest users) in GAGE, where, when a fully restricted user having Safe character (ELITES), it mutate to get full access to authorized resources, means when a user having full restriction on authorized resources, it doesn't involve in any malicious activity, so because of its not involving in any malicious activity, the character changes to Safe and then this special case will avail full access to authorized resources. This is the case of mutation to elite users having full restriction to authorized resources.

VII. Proposed Approach

A. *Design Algorithm*

For proper understanding of the methodology, please refer our last paper [1], because the hybrid approach is built upon the two approaches, which we have been discussed in detail there. Because, for the proposed methodology, we are just indicating which stages are from the previous two experiments' methodologies.

The methodology for our Proposed User Profiling System using Fuzzy guided GAGE (Genetic Algorithm with Genetic Engineering) for Cloud Computing security follows as:

- ***S1 (Stage 1):*** In the first stage of proposed User Profiling System, it works same as of the first five stages of Fuzzy System to identify different usage patterns at different phases of Cloud user's usage lifecycle.
- ***S2 (Stage 2):*** In second stage, Fuzzy delivers the final enumerated character from the different usage patterns of the user along with G1, G2 and G3 analysis, which is now considered as the population for GAGE in the present lifecycle (generation) and then GAGE calculates the fitness value of each user based on their characters.
- ***S3 (Stage 3):*** Third stage scales the fitness value of all user character (by sorting the fitness value of all users).

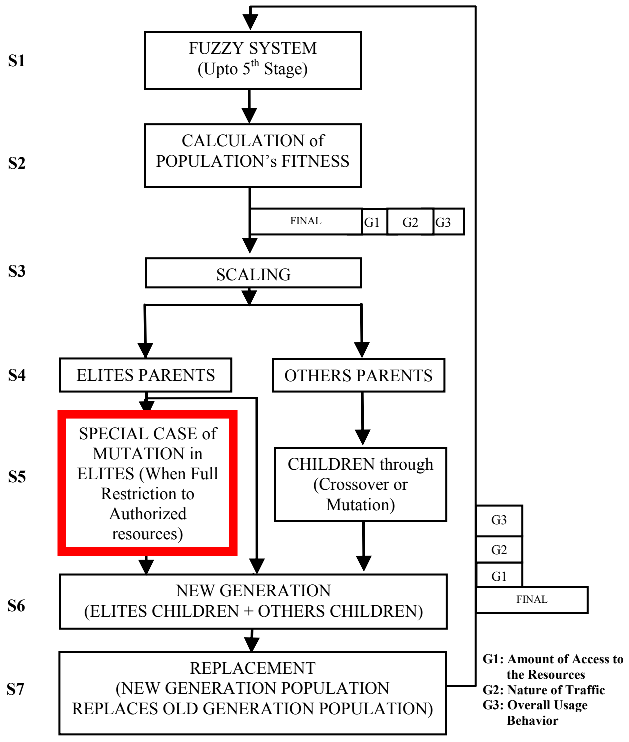
S1
FUZZY SYSTEM (Upto 5th Stage)
S2
CALCULATION of POPULATION's FITNESS
FINAL
G1
G2
G3
S3
SCALING
S4
ELITES PARENTS
OTHERS PARENTS
S5
SPECIAL CASE of MUTATION in ELITES (When Full Restriction to Authorized resources)
CHILDREN through (Crossover or Mutation)
G3
G2
G1
FINAL
S6
NEW GENERATION (ELITES CHILDREN + OTHERS CHILDREN)
S7
REPLACEMENT (NEW GENERATION POPULATION REPLACES OLD GENERATION POPULATION)
G1: Amount of Access to the Resources
G2: Nature of Traffic
G3: Overall Usage Behavior

Fig. 1. Proposed methodology flow diagram for User Profiling System for Cloud Computing security using Fuzzy guided Genetic Algorithm with Genetic Engineering (GAGE)

S4 (Stage 4): Fourth stage divides the population into two parts: ELITES parents and OTHERS parents, where ELITES are fittest (here, Safe=101 has the best fitness) and OTHERS are less fit (here, Malicious=102 and Highly Malicious=103 has the worse fitness).

S5 (Stage 5): At Fifth stage, ELITES parents are passed on as such to next generation, but in the special case, where ELITES have full restriction to authorized resources, get mutate to gain full access to authorized resources because of their character is Safe. Whereas OTHERS gone through crossover and mutation.

S6 (Stage 6): Sixth stage comprised of ELITES children (as such ELITES and Mutated ELITES) from ELITES parents and crossovered and mutated OTHERS children from OTHERS parents as a new generation.

S7 (Stage 7): At seventh stage, profiles of users are created or updated, which recommends the amount of authorized resources for next generation based on the calculations by GAGE.

B. Results and Discussions

The simulations for the proposed hybrid approach were performed on Matlab (a comprehensive suite for different simulation tools) and the sample size was four generations (or usage lifecycle).

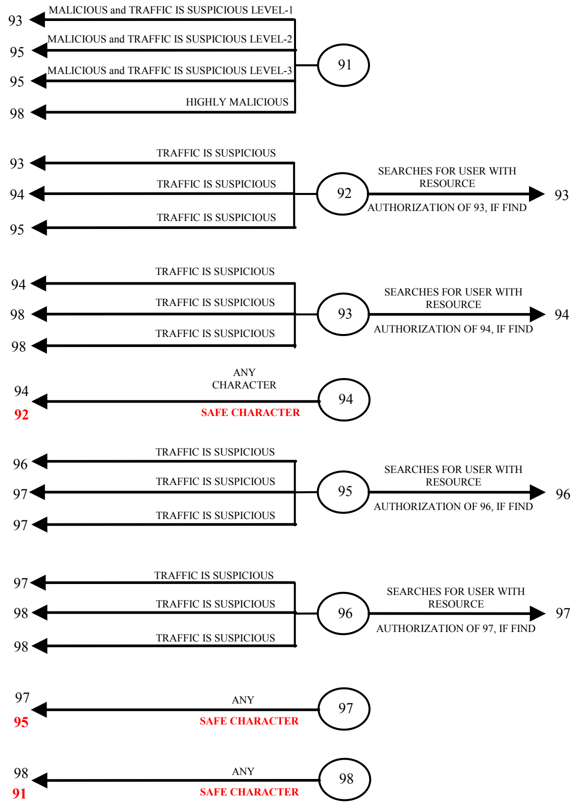

Fig. 2. Crossover and Mutation schema for Genetic Algorithm with Genetic Engineering (GAGE) with the special case of mutation to elite users.

The Fuzzy implementation was based on the Sugeno FIS (Fuzzy Inference System) for discrete membership functions and for the implementation of Crossover and Mutaion functions of GAGE, traversing, searching and basic mathematical operations were used. For graphical representation of the implementation outcomes, Stem plotting was used.

The simulation of the proposed hybrid approach for four generations (or usage lifecycles) by 16 users (in simulation outcomes, 16 users are shown on horizontal axis) with amount of resources authorized to them (scales on vertical axis in the form of colored bars) are described as:

- 91 is Full Access to Network (Intranet + Internet).
- 92 is Full Access only to Intranet.
- 93 is Partial Access to Intranet.
- 94 is Full Restriction to Intranet.
- 95 is Full Access only to Internet.
- 96 is Partial Access to Internet.
- 97 is Full Restriction to Internet.
- 98 is Full Restriction to Network (Intranet + Internet).

The Colored bars depict the enumerated user character as:

- Green Colored bars for Safe User.
- Red Colored bars for Malicious User.
- Blue Colored bars for Highly Malicious User.

The simulation outcomes of the proposed methodology for Fuzzy guided GAGE are as follows:

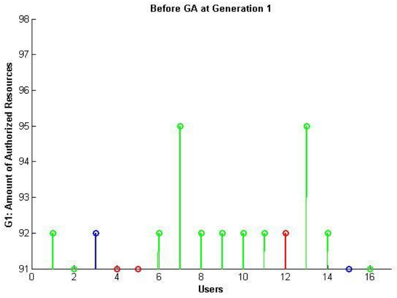

Fig. 3. Character enumerated by Fuzzy System during first generation

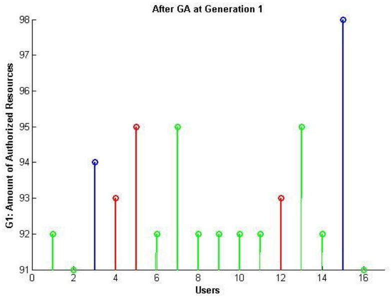

Fig. 4. Resource limitation by GAGE based on Fuzzy System's character enumeration during first generation

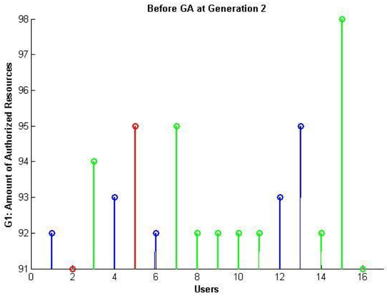

Fig. 5. Character enumerated by Fuzzy System during second generation after the recommendations by GAGE of first generation

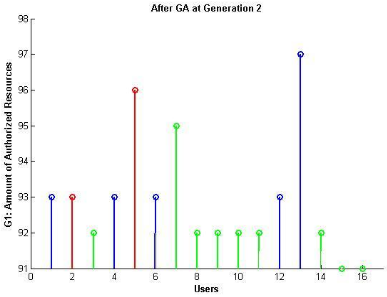

Fig. 6. Resource limitation by GAGE based on fuzzy System's character enumeration during second generation with application of special case on 3rd and 15th user

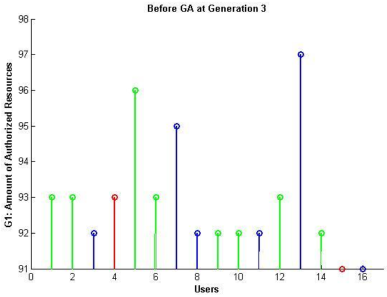

Fig. 7 Character enumerated by Fuzzy System during third generation after recommendations by GAGE of second generation

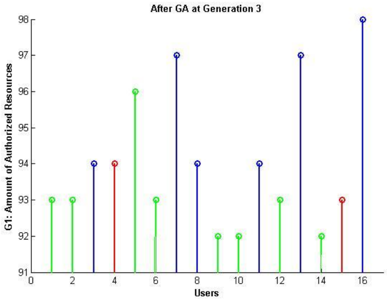

Fig. 8. Resource limitation by GAGE based on Fuzzy System's character enumeration during third generation

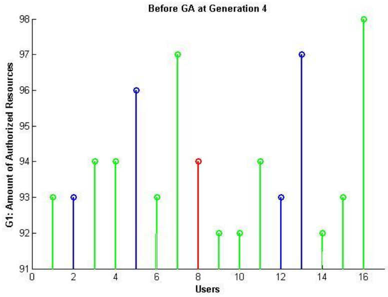

Fig. 9. Character enumerated by Fuzzy System during fourth generation after recommendations by GAGE of third generation

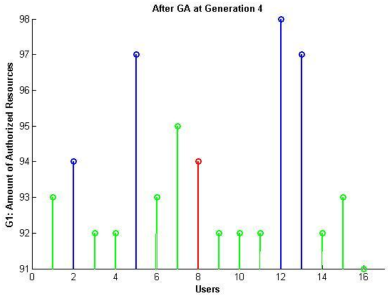

Fig. 10. Resource limitation by GAGE based on Fuzzy System's enumeration during fourth generation with application of special case on 3rd, 4th, 7th, 11th and 16th user

1) Analysis of results

1. During the first generation, initially Fuzzy System enumerated the characters of each user.
2. Then, GAGE limits the amount of resources authorized to Malicious and Highly Malicious users (character enumerated by Fuzzy at same generation) using crossover and mutation schema and raise the bars of OTHERS (Red and Blue colored). Raising the bars means limiting the resources.
3. During the second generation, Fuzzy System enumerated character of each user based on the recommendations for limiting the authorized resources by GAGE of first generation.
4. GAGE again limits resources using crossover and mutation for OTHERS, whereas 3rd and 15th user are ELITES, but because they are fully restricted to use authorized resources, so GAGE mutate these users to access authorized resources fully (Special Case).
5. Fuzzy system during third generation enumerates characters based on the recommendations by GAGE of second generation.
6. GAGE during third generation again limits the resources of OTHERS, using crossover and mutation based on the enumerated characters by Fuzzy System on same generation.
7. Fuzzy System during fourth generation enumerates characters based on the recommendations by GAGE of third generation.

8. GAGE limits the resources using crossover and mutation for OTHERS, whereas 3rd, 4th, 7th, 11th and 16th users are ELITES, but are fully restricted to use authorized resources, so GAGE mutate these users to access authorized resources fully (Special Case).

2) *Performance Analysis*

We analyzed the performance of proposed User Profiling System based on Fuzzy guided GAGE based on the seven principles of the reference model [12] for building a Risk Indicator System to validate security system's reliability and we got the following results:

1. ***Scientific:*** The system we implemented is scientific, as it is based on the well defined scientific mechanisms to enumerate characters with the help of Fuzzy System and search for Malicious and Highly Malicious users and crossover or mutate the Malicious or Highly Malicious users based on GAGE principles.
2. ***Systematic:*** This system is systematic as it starts from enumerating the character as Initial Population and gone through GAGE to recommend limitation factor for Malicious and Highly Malicious users only, then again it limits resources and again enumerate character.
3. ***Feasible:*** This System is feasible, because it provides the the logic for Fuzzy's changing of characters, based on the limitation of resources and enables the GAGE to not crossover and mutate the same initially profiled Malicious and Highly Malicious users all the times; because now character changing is the combined reflection of the profile history of the user and resource limitation in the last generation.
4. ***Quantitative**:* Yes, this system is quantitative as it quantifies the amount of authorized resources along with enumerating the character and determines limiting factor based on the usage patterns.
5. ***Guided:*** This system is highly guided by its goal to enumerate characters of users based on the different usage patterns and limit the amount of authorized resources based on the enumerated characters of the users.
6. ***Expandable:*** This system is expandable and can work with different Artificial Intelligence techniques.
7. ***Complete:*** This System is complete, as this system covers each and every aspect for profiling of character.

The comparative analysis of the evaluation framework outcome of the all three approaches to design a User Profiling System for Cloud Computing security is presented in TABLE I.

3) *Final Discussion*

Hence, from the analysis of the results from the all three experiments and their evaluation based on the risk indicator system [12], we found that the designing of User Profiling System using hybrid Artificial Intelligence technique: Fuzzy guided Genetic Algorithm with Genetic Engineering delivered a comprehensive User Profiling System for Cloud security.

VIII. Conclusion and Scope

A. Conclusion

It is concluded from the outcomes from our research work that, by using Fuzzy System in conjunction with GAGE (Genetic Algorithm with Genetic Engineering), a User Profiling System for Cloud Computing security can be designed, where both Fuzzy and GAGE complements each other in hybrid way to cover one another's research gaps which were found after their individual implementations for designing a User Profiling System for Cloud Computing security. Our proposed system enumerates characters of each user based on their usage patterns (through Fuzzy System) and recommends action to limit the amount of authorized resources of Malicious and Highly Malicious users (through GAGE) and even recommends to avail the fully restricted resources to the Safe users. The result analysis of the proposed User Profiling System shows that the system changes the characters of users based on the limiting of resources and the limitation to users will not fully restrict the resources if the characters of user changes on limiting of its resources. Hence, this hybrid system performs effectively for user profiling for Cloud Computing security.

TABLE I. Comparison of Result outcomes of the Evaluating Framework

Parameters	UPS using Fuzzy	UPS using GAGE	UPS using Fuzzy guided GAGE
1. **Scientific**	√	√	√
2. **Systematic**	√	√	√
3. **Feasible**	×	×	√
4. **Quantitative**	√	√	√
5. **Guided**	√	√	√
6. **Expandable**	√	√	√
7. **Complete**	×	×	√

B. Scope

We developed the proposed User Profiling System for Cloud environment, but this proposed system can be developed for any networking system, the only requirement is to adapt the Fuzzy System and GAGE (Genetic Algorithm with Genetic Engineering) according to that networking system environment. Even, we can research for better

Artificial Intelligence techniques and can test their effectiveness in various combinations (hybrid approaches) in context of designing a User Profiling System to make it more intelligent and to enable the security system to take action in a better way, in response of the User Profiling System's intelligence. This system can be used as an integral part in the security model to augment the security. We implemented it in simulation environment, but can be tested in real environment too.

REFERENCES

[1] Sahil, S.K. Sood, S. Mehmi, and S. Dogra, "Artificial intelligence for designing user profiling system for cloud computing security: Experiment," in *2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)*, Ghaziabad, UP, 2015, pp. 51-58.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation computer systems,* 2009, vol. 25, no. 6, pp. 599-616.

[3] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and grid computing 360-degree compared," *IEEE Grid Computing Environments Workshop (GCE'08)*, 2008, pp. 1-10.

[4] S. Dogra and Sahil, "Cloud Computing and its Security Concerns A Survey," *International Journal of Innovative Technology and Exploring Engineering*, 2014, vol. 3, no. 12, pp. 15-18.

[5] D. Hubbard, and M. Sutton, "Top Threats to Cloud Computing V1. 0," *Cloud Security Alliance*, 2010.

[6] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," *10th European Conference on Information Warfare (ECIW),* 2011, pp. 307-314.

[7] Wikipaedia (2016, April 1). *System Profiler* [online]. Available: http://en.wikipedia.org/ wiki/System_profiler

[8] Wikipaedia (2016, April 1). *Artificial Intelligence* [online]. Available: http://en.wikipedia.org/wiki/Artificial_intelligence

[9] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," in *16th ACM Conference on Computer and Communication Security (CCS)*, New York, NY, 2009, pp. 199-212.

[10] K. Xu, F. Wang, and L. Gu, "Profiling-as-a-service in multi-tenant cloud computing environments," in *32nd IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW),* Macau, 2012, pp. 461-465.

[11] W. R. Anis Ibrahim, and M. M. Morcos, "Artificial Intelligence and Advanced Mathematical Tools for Power Quality Applications: A Survey," in *IEEE Transactions on Power Delivery,* 2001, vol. 17, no. 2, pp. 668-673.

[12] J. Zhang, D. Sun, and D. Zhai, "A research on the indicator system of Cloud Computing Security Risk Assessment," *2012 IEEE International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE)*, 2012, Chengdu, pp. 121-123.