ADAPTIVE CHIMP OPTIMIZATION ALGORITHM BASED SECURE WORKLOAD CONTROL STRATEGY IN REAL TIME DATABASE MANAGEMENT SYSTEMS

By

SOMASUNDARA RAO M * KODUGANTI VENKATA RAO ** KRISHNA PRASAD M.H.M. ***

* Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation University, Green Fields, Vaddeswaram, Andhra Pradesh, India.
** Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Telangana, India.
*** Department of Computer Science and Engineering, Jawaharlal Nehru Technological University College of Engineering Kakinada, Andhra Pradesh, India.

https://doi.org/10.26634/jdf.2.1.20301

Date Received: 11/01/2024 Date Revised: 30/03/2024 Date Accepted: 25/07/2024

ABSTRACT

To control various workloads, a Real-Time Database Management System (RTDMS) serves as a framework for executing transactions. Database management systems support both the storage and recovery of data across various application services. However, since security and Quality of Service (QoS) are evaluated separately during user transactions, the performance of these transactions has not been optimized. To address these issues, this paper incorporates both security strength and QoS optimization. In this paper, workload conditions during user transactions in real-time database systems are managed using the Adaptive Chimp Optimization Algorithm (AChOA). This algorithm enhances the security strength of the RTDMS by optimally selecting the security policy based on user requests. Additionally, the search performance of the Chimp Optimization Algorithm (ChOA) is improved through the use of a chaotic series generator with tent mapping. Moreover, an Intrusion Detection and Protection System (IDPS) with a high detection rate is implemented to improve response time. Simulation results demonstrate that the proposed scheme achieves better security strength and response time.

Keywords: RTDMS, Adaptive Chimp Optimization Algorithm, Intrusion Detection and Protection System (IDPS), Workload.

INTRODUCTION

Data is stored in a Database Management System (DBMS) to simplify information retrieval, manipulation, and processing. A DBMS is a tool for managing data in a database in various ways. It also ensures confidentiality and safety for the database, maintaining data stability even with many users. Data freedom, synchronization control, utility services, and recovery services are all provided by the database management framework (Vadivoo et al., 2017).

The most common DBMSs include the Document Database Management System (DoDBMS), Columnar Database Management System (CDBMS), and Relational Database Management System (RDBMS) (Gunjal & Koganurmath, 2003; Wickramasinghe & Raza, 2021; Xu et al., 2015). There are many different types of database management systems, including several that are becoming crucial in broad applications such as robotics, mobile interaction infrastructure, the armed forces, and atomic reactor control systems. These DBMSs are known as Real-Time Database Management Systems (RTDMSs), where accurate processing is crucial (Deng et al., 2020; Pandey & Astya, 2017; Samaiya & Agarwal, 2018).

The process of transactions has specific significance since RTDMSs (Real-Time Database Management

Systems) are time-aware. The level of time awareness in RTDMSs is largely determined by transaction scheduling methods. Real-time constraints may be present in the transaction management of database frameworks. The real-time database framework, also known as a transaction execution framework, is designed to handle workloads in which all transaction deadlines are met. In describing these kinds of frameworks, appropriate transaction management and scheduling execution time are crucial.

In many cases, systems used for security-sensitive applications must simultaneously meet usage time constraints, and the RTDMS, which controls data integrity, is designed to address these challenges (Ali et al., 2020; Chauhan & Tripathi, 2019). This paper presents an adaptive optimization algorithm-based secure workload control strategy for real-time database management systems. list of the proposed methodology's significant contributions:

Data Analyzer: It is used to analyze incoming requests and estimate workload intensity.

AChOA: An adaptive Chimp Optimization Algorithm (AChOA) is introduced to enhance the security strength of RTDMSs.

Chaotic Sequence Generator: A chaotic sequence generator based on tent mappings is proposed to further improve the search capabilities of the ChOA algorithm.

IDPS: An Intrusion Detection and Prevention System (IDPS) is utilized to achieve reduced response time and computational resource usage.

1. Related Works

A few articles present workload management schemes for database management systems. Ge et al. (2021) introduced a deep reinforcement learning framework with attention-based tuning, named WATuning, for optimizing system performance. Initially, the authors achieved the tuning process by designing ATT-Tune for WATuning. The procedure involved generating a matrix of weights that considered workload characteristics and performed operations within the internal matrices of the framework. The algorithm selected the most suitable configuration using the internal matrices and weight values. WATuning handled various workload types by generating additional instance structures. Ultimately, WATuning fine-tuned itself based on the different workloads. The simulation results in the article showed that WATuning increased throughput by 52% and decreased latency by 31%.

Toapanta et al. (2020) aimed to address security issues in DBMS. They sought to present an efficient security technique to protect data in databases. To achieve this goal, they introduced a deductive scheme and an exploratory research method. Specifically, they presented a Security Framework Assessment Prototype for Databases, a database security algorithm, a security management structure prototype using blockchain for databases, a management framework's logical structure in blockchain, and a prototype designed to counter cyberattacks. Due to the proposed hybrid blockchain structure, the system's performance improved with optimal security, and the results indicated that security efficiency improved by 99.5%.

Maté et al. (2021) aimed to avoid security risks in NoSQL databases by presenting security mechanisms. They introduced a modernization scheme focused on access control and enhancing the security of related information frameworks and applications. The authors used domain ontology for detecting sensitive data and created a conceptual database structure. They applied their proposed scheme to a medical database using the familiar document-oriented NoSQL database known as MongoDB. The proposed scheme used to ignore the problems of missing critical access control. Besides, the cost and effort required for the modernization scheme have been reduced. The researchers have enhanced the security at the system level as a result of the suggested strategy.

The challenges faced by DBAs are increased by the growth and complexity of DBMSs. Moreover, these frameworks become more difficult to manage, which also increases the overall cost of ownership. Autonomic databases with self-management functionality offer a way to lower these costs. Self-management decisions are

made based on the database workload.

To address the issues of workload monitoring and change detection, a feedback-controlled cycle was designed for workload analysis and tracking of lightweight tasks to achieve their goal (Mozaffari et al., 2020). They used a reconfigurable colored Petri net concept to build the proposed workload model. The findings of the article revealed that the suggested technique was effective at identifying significant changes in workload in NoSQL systems and demonstrated good scalability.

Raza et al. (2018) aimed to address the problem of workload heterogeneity and complexity in DBMSs. They predicted and controlled the workload by understanding the workload type in advance. For workload prediction, they presented the Autonomic Workload Performance Prediction model. Using this model, they predicted the performance of the DBMS before executing the workload. Additionally, they addressed the issue of workload control by introducing the Case-Based Reasoning method. This approach allowed the authors to achieve better precision compared to existing machine learning models.

Bu and Cho (2020) presented a role-based access control framework dependent on database intrusion detection. Specifically, they proposed a learning classifier system based on Convolutional Neural Networks (CNN), which designed queries for roles by incorporating CNN with the learning classifier system. For feature selection, an enhanced Pittsburgh-style learning classifier system was used in the approach. Additionally, for modeling and classification, CNN was applied to a synthetic query dataset. The simulation outcomes in the paper demonstrated that the accuracy of the proposed method improved to 92.53%.

2. AChOA Based Secure Workload Control Strategy in RTDMS

2.1 Overview

The overview schematic of the suggested scheme is shown in Figure 1. The database administrator receives information on workload intensity and security policies in addition to incoming user requests. The data analyzer can be used to examine arriving requests and estimate their amount and workload. To enhance the security strength of RTDMS, AChOA is introduced to optimally select security policies based on user requests. By integrating a chaotic sequence generator based on a tent map, the ChOA algorithm's search capabilities are improved. After determining the optimal policies, the appropriate one is selected based on user requests. The user then chooses

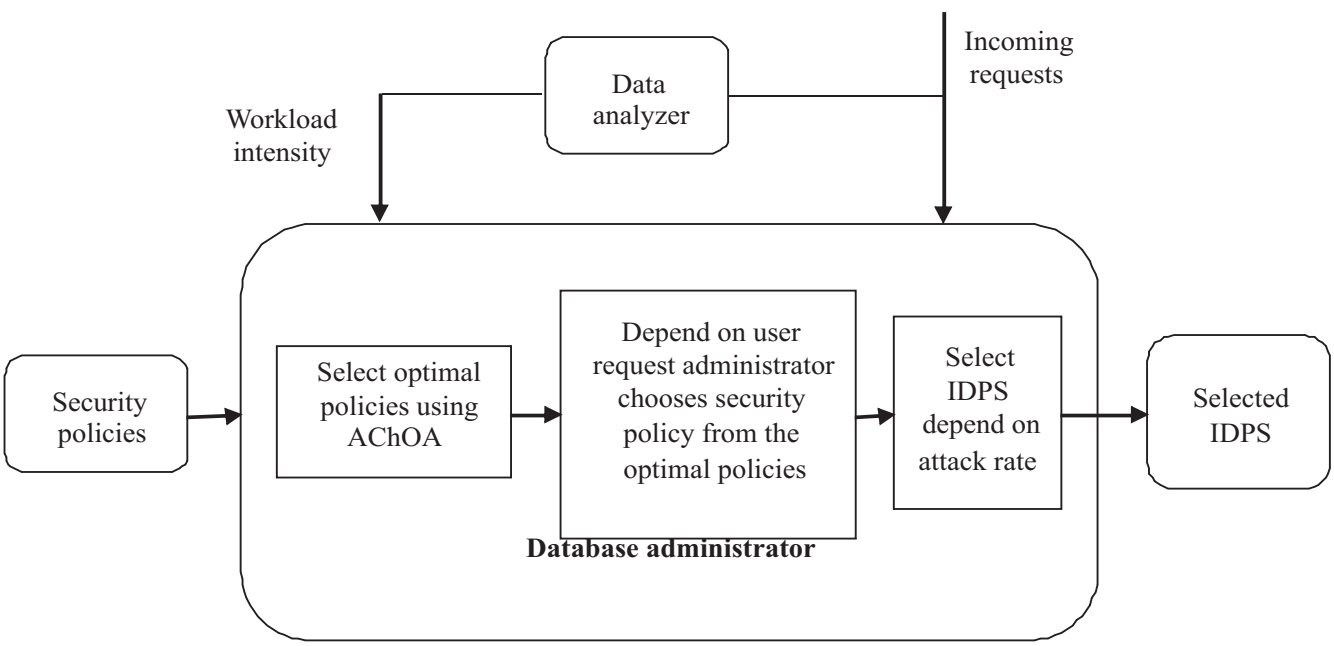

Figure 1. The Overview Diagram of the Proposed Scheme

the IDPS with the highest level of incoming request identification from a set of IDPSs to reduce response time and computational resources. The selected IDPS forwards the incoming request with the optimal security policy to the application server.

2.2. Functions of Database Administrator

Executing DBMS functions falls under the responsibility of the Database Administrator (DBA). The DBA oversees multiple systems rather than relying on a single framework. Instead of using one IDPS, the DBA employs a combination of IDPSs to enhance the system's security. The major functions of the DBA are as follows:

- *Support Users:* The DBA assists users in accessing the requested data.
- *Security and Integrity:* The DBA is responsible for identifying malicious users through authentication and authorization. Additionally, the DBA must maintain database protection and ensure its integrity.
- *Detecting Execution and Response of Requirements Modification:* DBA helps to evaluate the efficiency of system while meeting the system requirements. Besides, it helps to develop the appropriate changes based on requirements modification.

2.3 Functions of Security Mechanism

In this approach, IDPS is considered as the security mechanism. Besides, the IDS is used to identify the policy violation and also used to detect the malicious activities of the framework. Let consider M numbers of security mechanism. U stands for the total amount of user responsibilities while A stands for the total amount of attack types. The DBA policy η_u denotes the policy of the DBA it illustrates how the security methods are assigned to the u^{th} responsibilities of user. The symbols indicate that DBA policy has been assigned to the user role:

$$\eta_u = \{\in u,1,\in u,2,.....,\in u,M\} \quad (1)$$

According to Equation (1) the i^{th} security mechanism is assigned to u^{th} user role if $\in$ u, i it is set to 1 then. If not $\in$ u, i it turns to 0. The vector of a whole framework policy is denoted:

$$\eta = \{\eta_1, \eta_2, ..., \eta_U\} \quad (2)$$

2.4 Calculation of Security Strength and QoS Parameter

The security quality and QoS of the DBA are measured using security strength and response time, respectively. These measures are considered objective functions for selecting the policies of the security mechanism based on user requests. The security strength is estimated based on the number of IDPSs used and their detection rates. To obtain an efficient model, the security strength is estimated using exponential averaging. The security strength of user role u is defined in Equation (3).

$$S_u(\vec{\eta}_u) = \sum_{l=1}^{A} a_{u,l}\left(\ln \sum_{i-1}^{M} e^{r_{u,l} * \in_{u,j}}\right)/10 \quad (3)$$

Here, $a_{u,l}$denotes an assault likelihood associated with a user responsibilitiess u. $r_{u,l}$ denotes the detection rate of security mechanism assigns to user role u. The total use of security policy is defined in Equation (4).

$$S_{Total}(\vec{\eta}) = \sum_{\forall u} \omega_u S_u(\vec{\eta}_u) \quad (4)$$

Here, ω_u denotes the weight factor of user role u.

The average response time of IDPSs which associate to the user role u is obtained as:

$$T_u = T_{NA} + T_{IDPS} \quad (5)$$

Here, T_{IDPS} denotes the response time of IDPS and T_{NA} denotes the response time of network applications.

The total response time of all user roles is defined as:

$$T_{Total} = \sum_{\forall u} \omega_u T_u \quad (6)$$

Here, $\omega_u$denotes the weight factor of user role u.

The user role request includes the DBA measures and the performance of the IDPSs, which are executed by the security policy and application service.

2.5 Selection of Security Polices using AChOA

This approach employs the AChOA algorithm to optimize security policies such as password control, user security regulations, auditing policies, confidentiality regulations, and system protection guidelines based on user requests. According to this algorithm, chimpanzees, referred to as chimps, are a type of large ape native to Africa. The Brain-to-Body Ratio (BBR) of chimpanzees most closely resembles that of humans. Therefore, if a mammal has a higher BBR, it is assumed that its intelligence is comparable to that of humans. Given that both

chimpanzees and humans are descended from hominoid creatures that existed millions of years ago, their DNA may be related. Chimpanzees typically live in fission-fusion communities, where the size of the group can change over time as individuals move around. Each chimpanzee group independently seeks out hunting grounds using its own methods. Although intelligence and skills vary significantly among chimpanzees in different groups, they all fulfill their roles within the colony. Each individual possesses skills that can be useful in specific situations.

In addition, there are four different types of chimps in the colony, which are

- *Drivers:* They do not attempt to catch the victim; they merely pursue it.
- *Barriers:* To block the progress of the prey, they position themselves in a tree.
- *Chasers:* They pursue the prey rapidly in order to hunt it.
- *Attackers:* They predict the prey's escape route in order to direct it downward into the lower refuge or back toward the pursuers.

Chimpanzee hunting is typically divided into two basic stages, "Exploration," which involves driving, obstructing, and chasing the prey, and "Exploitation," which involves attacking the victim. Figure 2 shows the exploration process and Figure 3 shows the exploitation process. Additionally, a chaotic sequence based on a tent map is introduced in this study to improve the initial population quality and searchability of ChOA. A deterministic framework is a type of chaotic framework. Numerous map functions are used in chaotic frameworks, with the tent map and logistic map being among the most popular. However, because the logistic map has uneven traversal characteristics and the tent map has more uniform features, the tent map is used in this paper.

The description of the most effective route selection process applying the AChOA algorithm.

Initialization: The placement of the chimpanzees in ChOA corresponds to the location of the solutions inside the search area. Sets of security policies (η) are taken into account possible solution in this study. The initiation of the solutions' population,

$$P_N = \{y_1, y_2, ..., y_N\} \quad (7)$$

Where as employing (8), y_N shall be referred to as the chimp's position or the N^{th} solution.

$$y_N = \{\eta_1, \eta_2, ..., \eta_i\} \quad (8)$$

Chaotic Sequence Based on Tent Map: Equation (9) determines the tent mapping function.

$$q_{k+1} = \begin{cases} 10\,q_k/7 & q_k < 0.7 \\ 10\,(1-q_k)/3 & q_k \geq 0.7 \end{cases} \quad (9)$$

Where, q_k stands for the chaotic sequence, as its starting value is selected at random from the range [0, 1]. For each iteration, chaotic sequences $\{q_1, q_2, ...q_m\}$ are

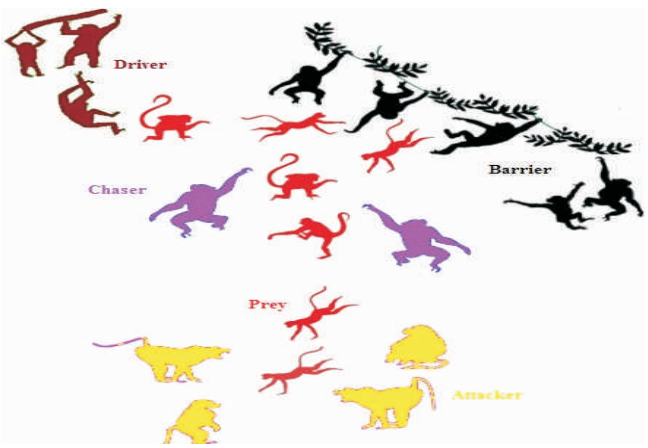

Figure 2. Exploration Process

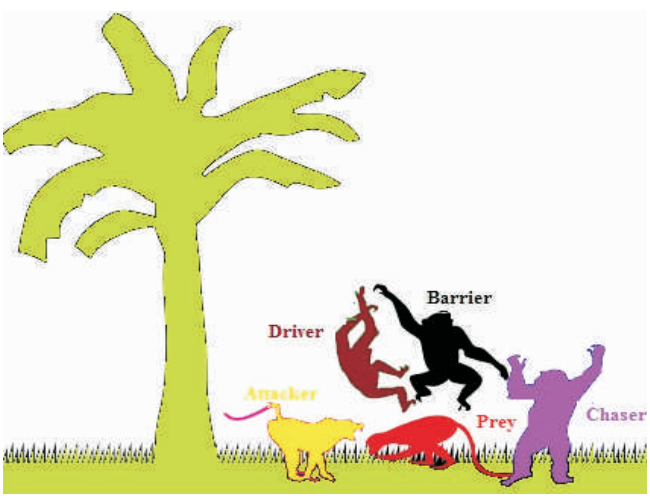

Figure 3. Exploitation Process

generated using (9). By utilizing (10), an initial response is created by mapping each step into the solution.

$$y_d = y_{d,\min} + \left(y_{d,\max} - y_{d,\min}\right) q_d \quad (10)$$

Where, $y_{d,min}$ and $y_{d,max}$ stand for the dth dimension upper boundary as lower boundary of y, respectively. By mapping the population's solutions utilizing (9) and (10), chaotic population is created at initiation.

Fitness Calculation: Fitness of every solution is estimated using security strength and response time of DBA. Employ (11) to define this.

$$Fit_N = Max\left(c_1 * S_u(\eta_u) + c_2 * \frac{1}{T_u}\right) \quad (11)$$

Here, $S_u(\eta_u)$ and T_u represent the security strength and response time respectively. These parameters are calculated using (3) and (5).

The best set of security policies is determined by (11), which states that the solution or set of security policies with the highest fitness is selected. The prey's location is indicated by the position of the algorithm's best solution. If the required fitness cannot be achieved, the solution is adjusted according to chimpanzees' hunting behaviors.

Update the Solution: The steps describe how chimps hunt or update a solution.

Driving and Chasing the Prey: Equations (12) and (13) describe the mathematical definitions of chasing and driving a target.

$$z = \left| y_{prey}(t) * c - y_{chimp}(t) * n \right| \quad (12)$$

$$y_{chimp}(t+1) = y_{prey}(t) - b * z \quad (13)$$

Here, t stands for the iteration, y_{prey} stands for the position of the prey, and y_{chimp} stands for the position of the chimpanzee. The coefficient vectors, denoted by b, c, and n, are calculated as :

$$b = 2 * f * rand_1 - f \quad (14)$$

$$c = 2 * rand_2 \quad (15)$$

$$n = Chaotic\_value \quad (16)$$

Here, rand 1 and rand 2 indicate the random vectors in the range [0, 1], and f is the coefficient vector that has been reduced nonlinearly from 2.5 to 0 during the iterative procedure. The chaotic vector n represents the influence of chimpanzees' sexual desire on the hunting process, with its estimation based on various chaotic maps.

Exploitation or Attacking Stage: Barrier, chaser chimps, and driver assist the attacker chimps in hunting the victim. Typically, the chimps who are attacking carry out the act of hunting. Using the mathematical equation, the most suitable answer or the first attacker, driver, barrier, and chaser is used to determine the position of the prey. The top four solutions are found and retained. The placement of other chimpanzees is updated based on the locations of the best chimps. Figure 4 shows that the chimps update the position. This is determined in Equations (17), (18), and (19).

$$Z_{Attacker} = \left| y_{Attacker} * c_1 - y * n_1 \right|, \quad Z_{Barrier} = \left| y_{Barrier} * c_2 - y * n_2 \right|$$
$$Z_{Chaser} = \left| y_{Chaser} * c_3 - y * n_3 \right| \quad Z_{Driver} = \left| y_{Driver} * c_4 - y * n_4 \right| \quad (17)$$

$$y_1 = y_{Attacker} - Z_{Attacker} * b_1 \quad y_2 = y_{Barrier} - Z_{Barrier} * b_2$$
$$y_3 = y_{Chaser} - Z_{Chaser} * b_3 \quad y_2 = y_{Driver} - Z_{Driver} * b_4 \quad (18)$$

$$y(t+1) = \frac{y_1 + y_2 + y_3 + y_4}{4} \quad (19)$$

Prey Attacking Stage: These apes will assault the victim at this point, stopping the procedure of hunting because the animal has stopped moving. In this stage's calculation, the value of the coefficient f shall be reduced. Aside from that, the range of b is also decreased by lowering the value of f. In particular, the range of b is altered between [-2f, 2f], where f value is reduced from 2.5-0 during iteration. Whenever a value of b falls between [-1, 1], a chimpanzee selects between its current location and the

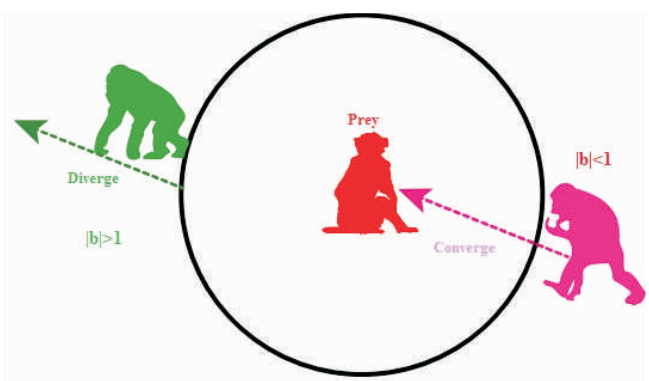

Figure 4. Chimps Update the Position Depend on |b|

location of its prey for its nest. If, the chimpanzees must assault the prey if $|b|<1$.

Exploration Stage: Chimpanzees get separated from their prey during this stage and made to look for the better feed. The apes are compelled to separate from prey when a value of b is larger than 1 or less than -1, according to the mathematical representation of divergence behaviors. The universal search strategy is made possible by this technique. Finding the best prey is placed upon the chimpanzees. Additionally, inside the range [0, 2], the c factor is utilized to prevent local minima. Additionally, this element gives prey random weights.

Social Motivation: At this point, chimpanzees' social incentive causes them to quit their hunting obligations. They then make a powerful chaotic effort to acquire meat. Chimpanzees' chaotic behaviour during their final stage helps to offset the two problems of capture in local optima and the slow speed of convergence when dealing with high-dimensional problems. The use of chaotic maps has improved ChOA's performance. These chaotic maps are loops with predetermined properties that also exhibit randomized behaviour. It will be a 50% chance of choosing either the chaotic model or the standard updating position approach to update the chimpanzees' position in order to show this concurrent behaviour. Equation (20) defines the behaviours' mathematical formulation.

$$y_{Chimp}(t+1)=\begin{cases} y_{prey}(t)-b*z & if\ \eta<0.5 \\ Chaotic\_value & if\ \eta>0.5 \end{cases} \quad (20)$$

Where, η represents a random number between 0 and 1.

Termination: Up until the best solution is found, the solutions are changed according to chimpanzee hunting behaviour. The algorithm concludes after the answer has been found.

Depending on a user's preferences, a DBA chooses one security policy from the best possible set of security policies.

Algorithm: Selection of optimal set of security policies using AChoA algorithm.

Input: Set of security policies (η),b, f, n, and c are coefficient factors.

Output: Optimum set of security policies.

- Consider the population of solutions P_N and coefficient factors initiated.
- Calculate chaotic sequence based on tent map for each solution using (9) and (10).
- Determine the location of each chimp.
- Group the chimpanzees at random.
- Evaluate each chimp's level of fitness.
- Save the greatest four search agents, $y_{Attac\ ker}$, y_{Chaser}, $y_{Barrier}$, y_{Driver}.
- While (Max number of iterations > t).

To Each Chimpanzee

- Take the chimps out of the group.
- Utilizing chimp's group technique, update f, c, and n.
- Determine b and z by using f, c, and n.

For Each Chimp Search

- If $\eta<0.5$

  If $|b|<1$ Utilizing (13) update the search agent's current position.

  Else if $|b|>1$ Select a randomized search agent.
- Else if $\eta<0.5$ Use (20) to update the search agent's current location.
- End if
- End for
- Update n, b, c and f
- Update $y_{Attac\ ker}$, y_{Chaser}, $y_{Barrier}$ and y_{Driver}.
- t=t+1
- End while
- Return $y_{Attac\ ker}$
- Up until the ideal solution is found, steps are repeated.
- Once the best solution has been found, stop the algorithm.

2.6 Selection of IDPS From the Combination of IDPSs

Due to an increase in consumer requests for privacy regulations, the database framework becomes corrupted because of the high attack rate. To enhance the security of the database framework, a mix of Intrusion Detection and Prevention Systems (IDPSs) is used in this

approach. Additionally, according to the security policy, the response time can be assessed by the Database Administrator (DBA) using the queuing network model shown in Figure 5.

IDPSs allow genuine users and characteristics for enhancing the system's performance. However, the selection of IDPSs by all users leads to increased response time and greater complexity. Therefore, in this work, an appropriate IDPS is selected based on how frequently user requests are detected. Specifically, if the attack rate of user requests is low, the detection rate is high. Consequently, the IDPS with the highest detection rate is chosen for incoming user requests. The DBA then forwards the user request, along with the selected IDPS and security policy, to the application server.

3. Results and Discussion

The Windows 7 OS and a 2 GHz dual core PC with 4 GB of primary RAM are used to carry out the suggested technique. Java is used for implementation. Fewer than two scenarios, the efficacy of the suggested scheme can be evaluated. In the first scenario, 5 different IDPSs are used for varying number of user requests 100, 200, 300, 400 and 500. In the second scenario, 8 different IDPSs are used for varying number of requests. The efficacy of AChoA is compared to that of ChOA, Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) in each scenario. Inverted generational distance, reaction time, protection capacity, and fitness measurement are also used to evaluate the effectiveness of the suggested approach. Table 1 shows the total number of security policies used in this work. Table 2 shows the optimal security policies.

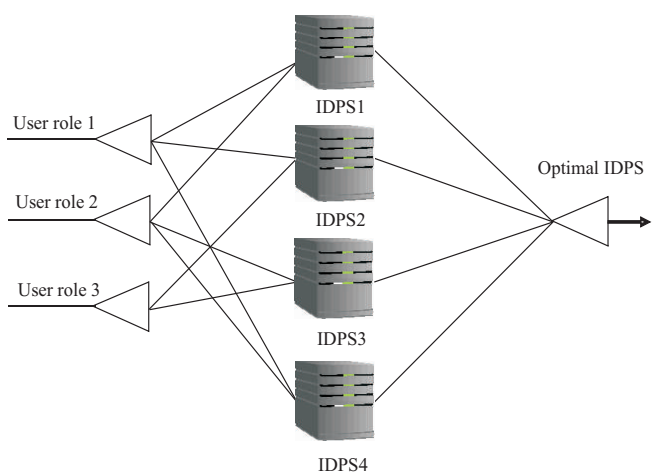

Figure 5. Queuing Network Model of IDPS

3.1 Performance Analysis Depend on 5 Different IDPSs

This analysis analyzes the effectiveness of the suggested scheme using 5 distinct IDPSs for 100, 200, 300, 400, and 500 user requests, respectively. Figure 6 shows the comparison of security strength of different schemes for varying number of user requests. As shown in Figure 6, compared to PSO and GA, security strength of RTDMS is

Total security polices	
Automatically forwarded email policy	Minimum requirements for network access policy
Acquisition assessment policy	Application service provider (ASP) policy
Acceptable use policy (AUP)	Personal communication device policy
Account access request policy	Acceptable encryption policy
Analog and ISDN line policy	Employee records retention policy
Audit policy	Database credentials coding policy
Dial-in access policy	Server security policy
Email policy	Network access standards
Global web server policy	Extranet policy
Information sensitivity policy	Interprocess communications policy
Password policy	Project security policy
Remote-access policy	Electronic communication retention policy
Risk-assessment policy	Source code protection policy
Spam policy	Router and switch security policy
VPN security policy	Financial retention policy

Table 1. The Total Number of Security Policies Used

Optimal security policies	
Account access request policy	Personal communication device policy
Acquisition assessment policy	Acceptable encryption policy
Automatically forwarded email policy	Network access standards
Acceptable use policy (AUP)	Analog and ISDN line policy
Dial-in access policy	Electronic communication retention policy
Email policy	Router and switch security policy
Global web server policy	Minimum requirements for network access policy
Information sensitivity policy	Application service provider (ASP) policy
Password policy	Inter process communications policy
Risk-assessment policy	Extranet policy
Spam policy	Server security policy
VPN security policy	

Table 2. Optimal Security Policies

increased to 22.5% for 100 numbers of user requests while that of RTDMS is increased to 63.5% for 500 numbers of user requests by selecting security policies using ChOA. However, in this approach, security strength of RTDMS is increased to 27% for 100 numbers of user requests and is increased to 67.5% for 500 numbers of requests because of presenting AChOA. The comparison of response time of different schemes is shown in Figure 7. For 100 numbers of user requests, response time of AChoA based RTDMS is decreased by 15%, 25% and 33% than that of ChOA, PSO and GA based RTDMS respectively. Likewise, compared to ChOA, PSO and GA, response time of AChoA based RTDMS is decreased by 7%, 11%, 19% for 500 numbers of requests. Figure 8 shows the analysis of inverted generational distance of the proposed scheme. Inverted generational distance is the measure to estimate the Euclidean distance between the actual solutions and approximate solutions in the algorithm. As shown in Figure 8, the average inverted generational distance of AChOA is decreased by 30%, 47% and 55% than that of ChOA, PSO and GA respectively. As shown in Figure 9, fitness measure of AChOA is increased to 47% for 100 numbers of user requests and that of AChOA is increased to 97% for 500 number of user requests than existing algorithms.

3.2 Performance Analysis Depend on 8 Different IDPSs

This analysis analyzes the effectiveness of the suggested scheme using 8 distinct IDPSs for 100, 200, 300, 400, and 500 user requests, respectively. Figure 10 shows the

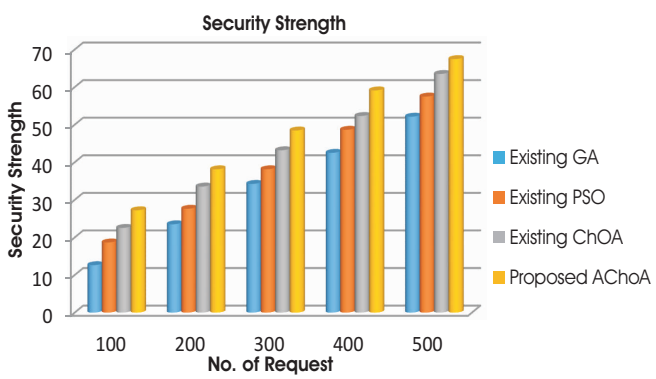

Figure 6. Analysis of Security Strength When RTDMS Uses 5 Different IDPSs

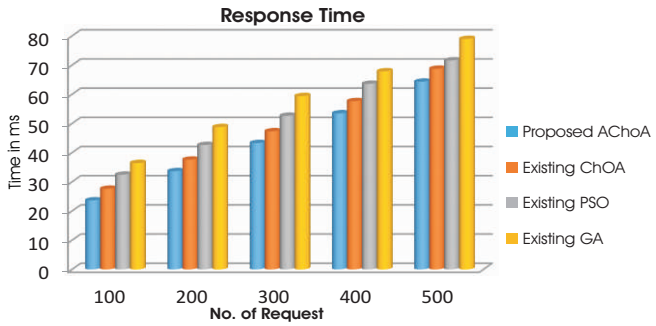

Figure 7. Analysis of Response Time When RTDMS Uses 5 Different IDPSs

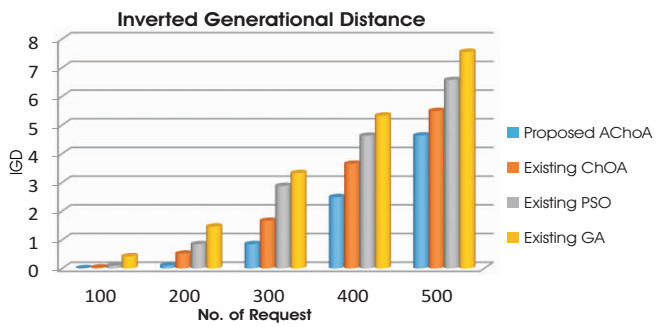

Figure 8. Analysis of Interleaved Generational Distance When RTDMS Uses 5 Different IDPSs

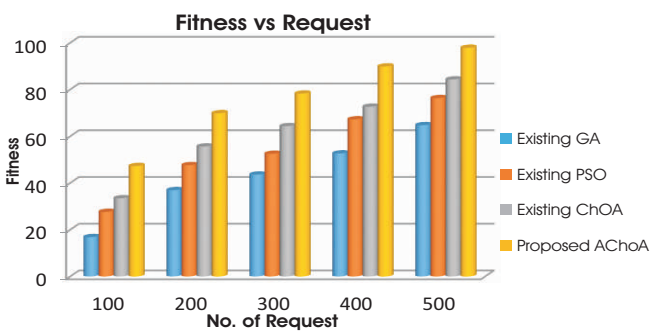

Figure 9. Analysis of Fitness Measure When RTDMS Uses 5 Different IDPSs

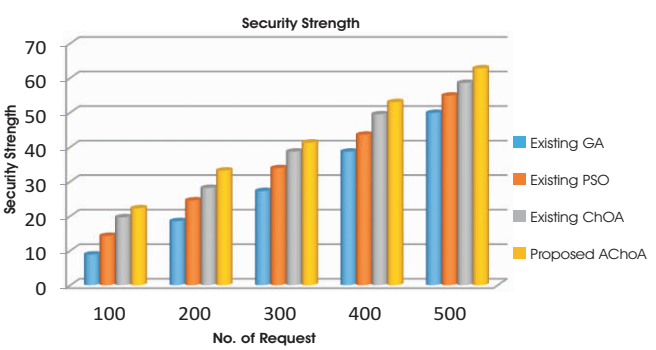

Figure 10. Analysis of Security Strength When RTDMS Uses 8 Different IDPSs

evaluation of the suggested method protection capability. Figure 10 shows the AChOA based RTDMS achieves 22% of security strength for 100 numbers of requests and it achieves 63% of security strength for 500 numbers of requests than the existing schemes. Figure 11 shows a response time analysis of various methods. According to Figure 11 a typical response time of AChOA based RTDMS is reduced to 9%, 17% and 28% that of ChOA, PSO and GA respectively. Figure 12 shows the comparison of inverted generational distance of different algorithms. Inverted generational distance of AChOA is reduced to 0.0014 for 100 numbers of requests and that of AChOA is reduced to 1.8754 for 500 numbers of requests than the existing algorithms. Figure 13 shows the fitness measurement for several algorithms. AChOA maximizes the fitness measure to 98.6% compared to existing algorithms.

Conclusion

To achieve secure workload strategy in RTDMS, an

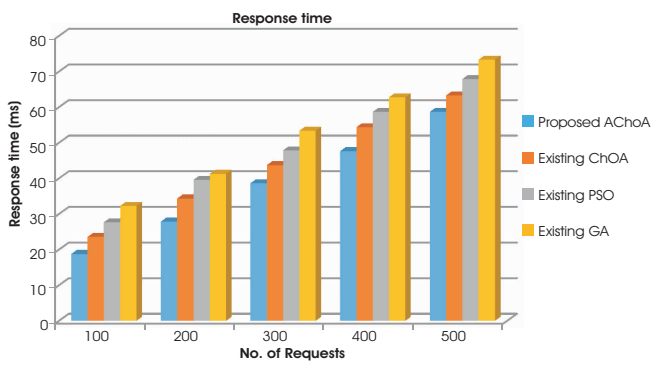

Figure 11. Analysis of Response Time When RTDMS Uses 8 Different IDPSs

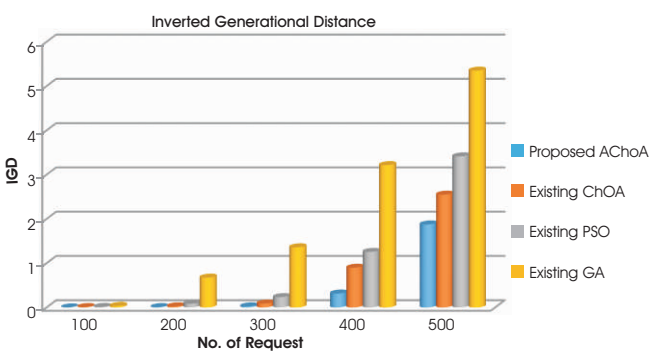

Figure 12. Analysis of Interleaved Generational Distance When RTDMS Uses 8 Different IDPSs

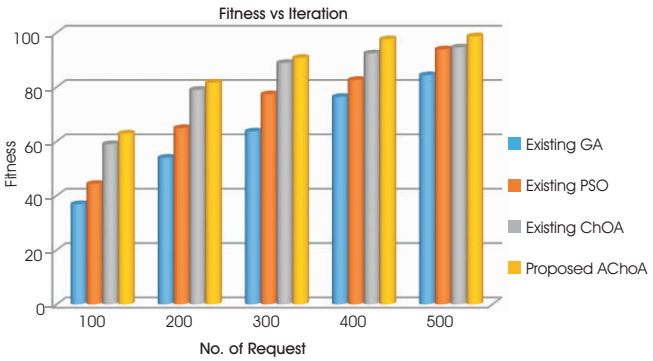

Figure 13. Analysis of Fitness Measure When RTDMS Uses 8 Different IDPSs

adaptive chimp optimization algorithm based RTDMS has been presented in this paper. In this approach, depend on user's requests, optimal security policies has been selected utilizing AChOA algorithm. By modifying the chaotic sequence generator according to the shelter mapping, the ChOA algorithm's search capabilities have been improved. From an optimal set of security policies, one policy is chosen based on the user's request. Additionally, among the various IDPSs, the one with the higher detection rate is selected to enhance QoS parameters such as response time. The final step is to forward the user's request to the application server along with the selected protection rules and IDPS. The efficacy of the suggested strategy was assessed under two scenarios: one with 5 different IDPSs and another with 8 different IDPSs, varying the number of user requests. As discussed in the results, the proposed AChOA-based RTDMS achieved better security strength, response time, and interleaved generational distance compared to the existing ChOA, PSO, and GA-based RTDMS.

References

[1]. Ali, R., Liu, R., Awan, S. A., Qayoom, A., Mahmood, S., ur Rehman, S., & Umer, M. (2020, February). Improvisation the security and privacy in real time database system. In *2020 International Conference on Information Science and Communication Technology (ICISCT)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICISCT49550.2020.9080027

[2]. Bu, S. J., & Cho, S. B. (2020). A convolutional neural-based learning classifier system for detecting database intrusion via insider attack. *Information Sciences*, 512,

123-136.

https://doi.org/10.1016/j.ins.2019.09.055

[3]. Chauhan, N., & Tripathi, S. P. (2019). QoS aware replica control strategies for distributed real time database management system. *Wireless Personal Communications,* 104(2), 739-752.

https://doi.org/10.1007/s11277-018-6047-0

[4]. Deng, C., Li, G., Zhou, Q., & Li, J. (2020). Guarantee the quality-of-service of control transactions in real-time database systems. *IEEE Access,* 8, 110511-110522.

https://doi.org/10.1109/ACCESS.2020.3002335

[5]. Ge, J. K., Chai, Y. F., & Chai, Y. P. (2021). WATuning: A workload-aware tuning system with attention-based deep reinforcement learning. *Journal of Computer Science and Technology,* 36(4), 741-761.

https://doi.org/10.1007/s11390-021-1350-8

[6]. Gunjal, B., & Koganurmath, M. M. (2003). *Database System: Concepts and Design*. Researchgate.

[7]. Maté, A., Peral, J., Trujillo, J., Blanco, C., García-Saiz, D., & Fernández-Medina, E. (2021). Improving security in NoSQL document databases through model-driven modernization. *Knowledge and Information Systems,* 63, 2209-2230.

https://doi.org/10.1007/s10115-021-01589-x

[8]. Mozaffari, M., Nazemi, E., & Eftekhari-Moghadam, A. M. (2020). Feedback control loop design for workload change detection in self-tuning NoSQL wide column stores. *Expert Systems with Applications,* 142, 112973.

https://doi.org/10.1016/j.eswa.2019.112973

[9]. Pandey, S., & Astya, P. (2017, May). Real time database management in mobile computing. In *2017 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 825-828). IEEE.

https://doi.org/10.1109/CCAA.2017.8229909

[10]. Raza, B., Kumar, Y. J., Malik, A. K., Anjum, A., & Faheem, M. (2018). Performance prediction and adaptation for database management system workload using case-based reasoning approach. *Information Systems,* 76, 46-58.

https://doi.org/10.1016/j.is.2018.04.005

[11]. Samaiya, S., & Agarwal, M. (2018, January). Real time database management system. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 903-908). IEEE.

https://doi.org/10.1109/ICISC.2018.8398931

[12]. Toapanta, S. M., Quimis, O. A. E., Gallegos, L. E. M., & Arellano, M. R. M. (2020). Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks. *IEEE Access,* 8, 169367-169384.

https://doi.org/10.1109/ACCESS.2020.3022746

[13]. Vadivoo, D. S., Shanthini, S., Vinora, A., & Priya, G. M. (2017). An overview of database management systems and their applications along with the queries for processing the system. *International Journal of Computer Science and Engineering,* 4 (3), 1-4.

https://doi.org/10.14445/23488387/IJCSE-V4I3P101

[14]. Wickramasinghe, S., & Raza, M. (2021). *DBMS: Database Management Systems Explained*. Retrieved from

https://www.bmc.com/blogs/dbms-database-management-systems/

[15]. Xu, Z., Tu, Y. C., & Wang, X. (2015). Online energy estimation of relational operations in database systems. *IEEE Transactions on Computers,* 64(11), 3223-3236.

https://doi.org/10.1109/TC.2015.2394309

ABOUT THE AUTHORS

Dr. Somasundara Rao M. serves as an Assistant Professor in the Department of Computer Science and Engineering at K L University, Vijayawada, Andhra Pradesh, India. He holds a Bachelor's degree in Computer Science and Technology from Andhra University, Visakhapatnam, Andhra Pradesh, India. He further pursued a Master's degree in Computer Science and Technology, specializing in Artificial Intelligence and Robotics, from the same university. He has completed his Ph.D. in Computer Science and Engineering at Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India. His primary research interests lie in the fields of Network Security and Database Security, where he actively contributes to advancing knowledge and innovative solutions.

Dr. Koduganti Venkata Rao holds the position of Director and Professor of Computer Science and Engineering at Guru Nanak Institutions Campus, Ibrahimpatnam, Telangana, India. He has served in various roles, including Lecturer, Assistant Professor, and Associate Professor, at multiple institutions since 1998. He obtained his B.Sc. degree in 1991 and an M.Sc. degree in 1994 from Nagarjuna University, Andhra Pradesh, India. He later earned his M.Tech and Ph.D. degrees from Andhra University, Visakhapatnam, India, in 1999 and 2008, respectively. His research interests include Networks, Security, and Database Security. He has contributed extensively to the academic community, with over 30 research papers published in leading international journals and conferences. Additionally, he has participated in numerous national and international conferences, both in India and abroad.

Dr. M.H.M. Krishna Prasad serves as the Principal and Professor in the Department of Computer Science and Engineering at the University College of Engineering Kakinada (Autonomous), JNTUK, Andhra Pradesh, India. He earned his B.Tech. degree from Chaitanya Bharathi Institute of Technology (CBIT), Osmania University, Hyderabad, India, and went on to obtain both his M.Tech. and Ph.D. in Computer Science and Engineering, with a specialization in Data Mining. He has distinguished himself through international academic experiences, including the successful completion of a two-year MIUR fellowship (January 2007-December 2008) at the University of Udine, Italy. He has published over 50 research papers in reputed international journals and conferences and has presented his work at numerous national and international conferences both in India and abroad. He is an active member of professional organizations such as the Association for Computing Machinery (ACM), the Indian Society for Technical Education (ISTE), and the International Association of Engineers (IAENG), Germany. Additionally, he serves as a member of the board of reviewers for various international journals and conferences. His research interests span across Data Mining, Big Data Analytics, and High-Performance Computing, where he continues to contribute to the advancement of knowledge in these critical areas.