ISSN: 2093-5374 / E-ISSN: 2093-5382

A Multi-Phase Behavioural Attribute Based Zero Trust Authentication Model with Simulation Using Replica Controlled Secured Distributed Networks

Modisaotsile Marope[1*], Venumadhav Kuthadi[2], Rajalakshmi Selvaraj[3], Thabo Semong[4], and Tshiamo Sigwele[5]

[1*]Research Scholar, School of Pure and Applied Sciences, Botswana International University of Science and Technology, Botswana. modisaotsile.marope@studentmail.biust.ac.bw, https://orcid.org/0009-0009-2956-1956

[2]Associate Professor, Department of Computing and Informatics, School of Pure and Applied Sciences, Botswana International University of Science and Technology, Botswana. kuthadiv@biust.ac.bw, https://orcid.org/0000-0003-4515-1921

[3]Associate Professor, Department of Computing and Informatics, School of Pure and Applied Sciences, Botswana International University of Science and Technology, Botswana. selvarajr@biust.ac.bw, https://orcid.org/0000-0002-7059-1702

[4]Senior lecturer, Department of Computing and Informatics, School of Pure and Applied Sciences, Botswana International University of Science and Technology, Botswana. semongt@biust.ac.bw, https://orcid.org/0000-0002-9370-196X

[5]Lecturer, Department of Computing and Informatics, School of Pure and Applied Sciences, Botswana International University of Science and Technology, Botswana. sigwelet@biust.ac.bw, https://orcid.org/0000-0001-7492-8053

Received: March 21, 2025; Revised: May 03, 2025; Accepted: June 04, 2025; Published: June 30, 2025

Abstract

This Paper presents a multi-stage replica-based anomaly detection model specifically for distributed systems. The proposed model, Multi-Phase Behavioural Attribute based Zero Trust Authentication Model (MBAZTA), observes system behaviour in three well-defined stages with multiple attributes in each stage and employs five standalone replicas to assess incoming behavioural patterns. Deviations at stage-wise levels are identified as anomalies, and the same is validated using a consensus mechanism among replicas. Every replica has its own baseline, and decisions about access are taken based on the number of conforming nodes, implementing a risk-based control. A simulation test with 1000 instances of behaviour was used to test the effectiveness of the model. With a minimum of false negatives and zero false positives, the results revealed a detection rate of 99.7 %. Under different conditions the system's performance stayed constant, preserving low latency and effective bandwidth consumption. This shows that in real-time circumstances the suggested method can consistently and scalable spot anomalies.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 2 (June), pp. 434-458. DOI: *10.58346/JOWUA.2025.I2.027*

*Corresponding author: Research Scholar, School of pure and applied sciences, Botswana International University of Science and Technology, Botswana.

Keywords: Multi-stage Anomaly Detection, Behavioural Profiling, Replica Consensus, Distributed Systems, Authentication system.

1 Introduction

In the developing paradigm of cyber-physical systems, where vast-scale distributed architectures control services and infrastructure (Sengupta & Anshul, 2024), dependable authentication solutions are very essential. From sophisticated attacks disguising themselves as regular behaviour to insider exploitation, these systems are becoming exposed to a broad spectrum of threats. When context-aware analysis and real-time decision-making (Gong et al., 2024) are of paramount relevance, conventional methods can fall short in such situation. Different from the typical anomaly detection systems, a novel approach dubbed MBAZTA integrates behavioural traits into zero trust authentication (Soni et al., 2014). It has many characteristics that distinguishes it. Unlike traditional models often rely on stationary thresholding or centralised analysis, each monitoring node in MBAZTA maintains an independent behavioural baseline based on decentralised replica-based architecture. One main disadvantage of centralised solutions is that they rely on a single point of evaluation; yet, our design reduces risk and increases fault tolerance (Şahin et al., 2025). The second unique quality is the multi-stage profiling technique. MBAZTA divides system behaviour into various phases, each having unique traits that help one to better grasp it (Pradeepthi & Maheswari, 2024). This tiered method, which improves detection accuracy, allows the system to identify which activities are causing aberrant behaviour.

Legacy systems will utilise binary results of Bi-Phase Authentication for handling anomalies. However, MBAZTA access control is based on risk-based approach, so the degree of restriction depends on the nature of the anomaly with respect to the quantity of duplicate agreements. Operating continuity and security suffer a trade-off with this extra layer of decision-making (Takaiwa et al., 2024). The algorithm also uses weighted attribute comparison, which gives certain features more importance depending on their influence on behaviour. More freedom and sensitivity to identify minor variations are made feasible by this than by more strict weighting techniques. Greater false positive rates or delay in traditional models resulting from over-reliance on stringent rule sets or computationally expensive processes would adversely affect their performance (Barman et al., 2025). Real-time, consensus-based evaluation algorithm of MBAZTA efficiently removes noise and zeroes down on persistent variations, producing very accurate findings with zero false positives and zero response delay.

Using intelligent techniques to mix decentralised decision-making, stage-by-stage analysis, adaptive access restriction, and attribute-weighting makes our solutions more resilient, scalable, and context-rich than conventional anomaly detection systems (Karimov & Sattorova, 2024). We introduce MBAZTA in this work as a new multi-stage anomaly detection approach possibly functioning across copies in distributed systems. Built on multi-phase behavioural traits, it seeks to remove trust problems in authentication mechanisms. The model replics behavioural baseline and consensus-based decisioning methods to effectively identify unexpected activity with low false positives (Nakamura et al., 2025). Because of their high detection ratio—achieved via algorithmic calibration and rigours modeling—cloud infrastructues, IoT networks, and critical infrastructure monitoring are perfect settings for MBAZTA (Ibrahim & Shanmugaraja, 2023).

Related Works

The major objective of this study is to construct an all-encompassing anomaly detection model suitable for distributed network configurations (Balaji et al., 2023). Fundamentally, it is a method of behavioural

profiling with many phases used to show normal and aberrant actions at various degrees of system functioning. By separating behaviour into stages and validating desired traits at each (Karimov & Sattorova, 2024), the system gains a more complex awareness of tendencies than would be feasible with a monolithic model. Included inside the model is a replica-based consensus model to assist with supporting detecting accuracy. Several copies decide on behaviour at the same time; the final call comes from a consensus among all the copies. False alarms are reduced and the detection dependability is maximised. By means of high levels of testing at multiple iterations, we evaluate the system's performance under various operating conditions with great precision. We periodically evaluate scalability, detection accuracy, latency, and bandwidth economy. Perhaps the most important feature of the model is its dynamic decision policy, which dynamically changes permissions based on the degree of agreement towards normal and deviant behaviours, therefore balancing responses with visible danger. The adaptive control method offers a harmonic method of ensuring security. Conventional systems rely on fixed rules or signature lists, whereas our model actively learns basic behaviours and may find complex ones (Li et al., 2024). Encouragement of distributed decision-making helps to reduce dependency on central monitoring and provides a scalable form fit for high-throughput systems. In many of the most important applications—including energy smart grids, autonomous driving systems, and multi-cloud systems—security, speed, and flexibility are of first significance.

Simulated results reveal that the model is stable with a very high success rate in anomaly detection and a low false positive count. The extensive detection activity among all copies (Veeramachaneni, 2025) confirmed the durability of the consensus approach; sophisticated risk classification let the system change judgements depending on degree of severity. Finally, the model's low bandwidth use and steady throughput show its resource economy, which qualifies well for situations with restricted means. Edge-based network deployment, adaptive threshold learning, and its interaction with real-time data streams are some possible directions of future investigation. Dynamic stage sensitivity and cross-replica learning (Rivera et al., 2024) allow for even more development of its detecting sensitivity. All things considered, this method prepares distributed systems of the future to have intelligent, scalable, and self-managing anomaly detection. Applied to a more general definition of cyber-physical systems, this work prepares the foundation for extending anomaly detection to guarantee reliable and autonomous functioning. (Sasada et al., 2024) underlines the need of biometric authentication in systems of dynamic access control. Further the insufficiency of traditional static authentication once a session has been initiated. Their biometric-centric ZTA system enables real-time authentication of users' legitimacy using behavioural and cognitive patterns, effectively distinguishing legitimate users from attackers post-login (Vignesh et al., 2023). The approach is in support of the post-authentication verification validity and is based on adaptive access control reasoning built in this study. (Marope et al., 2024) lay out a comprehensive review of the application of Zero Trust approaches to hierarchical WSNs. Their exposition brings out the inability of traditional security models to counter multiform denial-of-service (DoS) and sophisticated persistent threats. The document names significant drivers of the shift toward Zero Trust and refers to light-weight authentication strategies as a needed component of secure wireless design. These observations demand scalable, strong models capable of operating efficiently in diverse network topologies.

(Phalaagae et al., 2024) contribute to the field with the development of the Randomized Bi-Phase Authentication Scheme (RBAS) for WIoT sensor networks. The method enhances internal and external network security via digital watermarking and cyclic redundancy checks (CRCs). The study demonstrates power usage optimizations and data integrity optimizations and achieves quantifiable improvements in latency decrease, network lifetime, and reduced packet loss. Implementation of cluster

aware authentication, together with cryptographic practice, offers a perfect balance of performance and security, which happens to align well with the instant study's performance-driven evaluation. Upon the inception of RBAS, Phalaagae et al. (2022) and (Marope, 2021) venture further optimization with the implementation of Biphase Authentication Scheme (BAS) along with LEACH-C protocol for clustering. Their BA-LEACHC scheme applies genetic algorithms to identify and isolate malicious nodes dynamically to significantly improve DoS attack resistance with little energy efficiency compromise. Detection of unsafe paths and verification of nodes by path analysis in real-time agrees with distributed and risk-aware paradigms employed in the existing work.

These combined efforts illustrate a direction towards lightweight, distributed, and adaptive authentication methods as integral parts of secure networks today. Whereas most of the examined studies concentrate on static node authentication or cluster-bounded security boosts, this work takes the paradigm further by integrating multistage behavioural profiling, replica-based agreement, and dynamically risk-aware decision-making logic (Phalaagae et al., 2022). By combining these components, the model presented herein provides a secure, responsive, and scalable solution specific to distributed IoT and WSN real-time anomaly detection and access control. This literature survey proves that important advancements have indeed been made regarding Zero Trust and resource-constrained system authentication schemes, yet still a gap exists in combining the components into an integrated, simulation validated model balancing security against operational performance. The current study fills this void by the design, simulation, and analysis of an end-to-end replica-consensus protocol that adjusts to risk in real time and spreads trust among various verification points.

Materials and Methods

The study utilizes a simulation-driven methodology to design and evaluate the anomaly detection model. The major components include:

Data Representation: Each node behaviour is represented through a vector of attributes across multiple stages, allowing granular monitoring.

Replica Setup: Five replicas simulate independent monitoring entities, each maintaining a unique behavioural baseline.

Behaviour Simulation: Normal behaviour is generated based on predefined baselines with minor noise, while anomalies are introduced with an 8% probability.

Evaluation Metrics: Key performance indicators include accuracy, latency, throughput, false rates, and scalability.

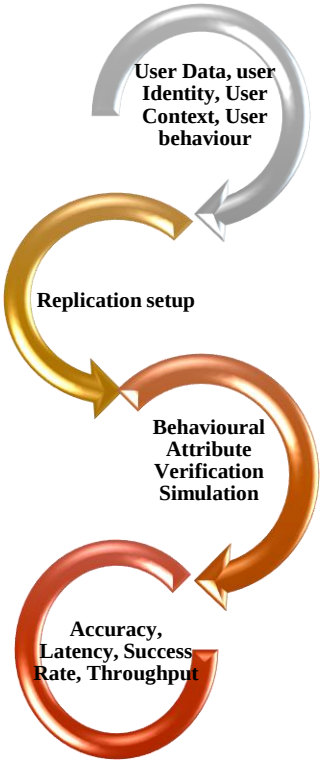

Figure 1: Graphical presentation of Multi-Phase Behavioural Attribute based Zero Trust Authentication Model (MBAZTA)

Tools such as Python-based simulation scripts, NumPy for numerical operations, and randomization modules facilitate the execution of 1000 test iterations. The development and validation of the MBAZTA anomaly detection model were carried out through a simulation-based experimental approach, incorporating mathematical modelling, statistical thresholds, weighted similarity computations, and multi-stage behavioural profiling. This section outlines the configuration, logic, and formulation of the components involved in the anomaly detection process. It is graphically presented in Figure.1.

The model as given in Figure.1., simulates a distributed environment consisting of multiple monitoring nodes (replicas), each independently maintaining a profile of normal system behaviour. The primary architectural elements include:

- **Replicas (r):** Number of distributed monitoring entities. In this model, r=5.
- **Stages (s):** Distinct phases or layers of behavioural observation. Defined as s=3.
- **Attributes per Stage (a):** Each stage contains 5 unique behavioural attributes, giving a=5.
- **Total Attributes (T):** Computed as the product of stages and attributes per stage:

$$T = s \times a = 3 \times 5 = 15$$

1.1. Baseline Profile Generation

Each replica maintains a 15-dimensional baseline profile, representing expected values for normal behaviour. These values are randomly initialized from a uniform distribution over the range [0, 1] as given in Eq.1.

$$B^{(r)} = \left[b1^{(r)}, b2^{(r)}, \ldots, bT^{(r)}\right] \forall r \in \{1,2,\ldots,5\} \quad \text{Eq.1.}$$

Where $b_i^{(r)} \in [0,1]$ represents the baseline value of the i^{th} attribute for the r^{th} replica.

1.2. Attribute Weighting Scheme

To prioritize certain attributes, a linear weighting system (Jing et al., 2024) was applied. Weights were assigned in descending order and normalized so that their total sum equals 1. Let the unnormalized weights be defined as given in Eq.2.

$$w_i' = T - i + 1 for\ i \in \{1,2,\ldots,T\} \quad \text{Eq.2.}$$

The normalized weights are computed as given in Eq.3.

$$w_i = \frac{w_i'}{\sum_{j=1}^{T} w_j'} \ such\ that\ \sum_{i=1}^{T} w_i = 1 \quad \text{Eq.3.}$$

This ensures that early attributes carry slightly more influence, supporting stage prioritization based on empirical assumptions or observed relevance.

1.3. Behaviour Vector Construction

For each iteration, a new behaviour vector $X = [x1, x2, \ldots, xT]$ is generated, either representing a normal or anomalous behaviour:

- **Normal Behaviour:** It is derived from the average of all replicas' baselines per attribute as given in Eq.4.

$$x_i = \frac{1}{r} \sum_{j=1}^{r} b_i^{(j)} + \epsilon_i\ , \epsilon_i \sim U(-\delta, \delta) \quad \text{Eq.4.}$$

Where δ is a small noise factor (e.g., 0.01), simulating operational variation.

- **Anomalous Behaviour:** All values are drawn independently from a uniform random distribution. $x_i \sim U(0,1)$. After generation, each attribute is clamped as follows:

$$x_i = min(1, max(0, x_i))$$

1.4. Similarity Score Computation

Each replica compares the input behaviour with its baseline profile using a weighted absolute difference as given in Eq.5.

$$d_i^{(r)} = |x_i - b_i^{(r)}| \quad \text{Eq.5.}$$

The overall weighted dissimilarity (Nguyen et al., 2025) is given in Eq.6.

$$D^{(r)} = \sum_{i=1}^{T} w_i \,.\, d_i^{(r)} \quad \text{Eq.6.}$$

The similarity score $S^{(r)}$ is then calculated as given in Eq.7.

$$S^{(r)} = 1 - D^{(r)} \quad \text{Eq.7.}$$

A similarity closer to 1 indicates high conformity to the expected behaviour.

1.5. Stage-Wise Anomaly Detection

Each stage S_k ($where\ k \in \{1,2,3\}$) has its own detection logic. The attributes corresponding to stage S_k are indexed as given in Eq.8.

$$I_k = \{(k-1)\cdot a + 1, \ldots, k \cdot a\} \quad \text{Eq.8.}$$

The total deviation for stage S_k in replica r is given in Eq.9.

$$\Delta_k^{(r)} = \sum_{i \epsilon I_k} |x_i - b_i^{(r)}| \quad \text{Eq.9.}$$

Each stage has a threshold θ_k, defined as $\theta_k = a \cdot 0.25 = 1.25$. If $\Delta_k^{(r)} > \theta_k$, stage S_k is flagged as anomalous by that replica. A replica marks the overall behaviour as anomalous if two or more stages exceed their respective thresholds.

1.6. Consensus Mechanism

After all replicas complete their individual analysis (Annabi et al., 2024), the system calculates the number of replicas that flagged the behaviour as given in Eq.10.

$$F = \sum_{r=1}^{5} 1_{\text{anomalous}}^{(r)} \quad \text{Eq.10.}$$

Where$1_{\text{anomalous}}^{(r)} = 1$ if replica r flags an anomaly, and 0 otherwise. The final anomaly status and access control decision are based on the following logic:

F≤1⇒ Access ***Granted***

F=2⇒ Access ***Denied (Medium Risk)***

F≥3⇒ Access ***Denied (High Risk)***

This multi-tier decision mechanism balances caution with efficiency.

1.7. Response Time Simulation

To replicate practical performance metrics, each iteration includes a simulated response (Ahn et al., 2024) delay. $T_{resp} \sim U(0.2, 0.4)$. Cumulative response time T_{cum} is updated at each step, and the average latency is calculated as given in Eq.11.

$$T_{Avg} = \frac{1}{N} \sum_{i=1}^{N} T_{resp}^{(i)} \quad \text{Eq.11.}$$

Where N is the number of iterations.

1.8. Success Rate and Error Metrics

The model continuously tracks accuracy via detection success:

- **True Positive (TP):** Anomalous behaviour correctly denied.
- **True Negative (TN):** Normal behaviour correctly granted.
- **False Positive (FP):** Normal behaviour wrongly denied.
- **False Negative (FN):** Anomalous behaviour wrongly granted.

From these, the success rate is: $Success_{Rate(SR)} = \frac{TP+TN}{TP+TN+FP+FN}\ x\ 100$

The rolling success rate over the latest 10 iterations is computed dynamically as given in Eq.12.

$$Rolling_i = \frac{1}{10} \sum_{j=i-9}^{i} 1_{correct}^{(j)} \quad \text{Eq.12.}$$

This helps to monitor short-term performance fluctuations.

1.9. Bandwidth and Throughput Modelling

While physical transmission is not involved in the simulation, data throughput and bandwidth utilization (Tahir et al., 2025) are modelled in the assumption of small packet sizes per iteration. Each decision cycle results in about 1.5 KB of replica internal communication. With an average response window of 0.3 seconds, the estimated throughput T_{thru} is calculated as given in Eq.13.

$$T_{thru} = \frac{1.5\ KB}{0.3\ s} \approx 5\ KB/s\ (per\ replica) \quad \text{Eq.13.}$$

Across all replicas, total throughput reaches ~20 KB/s. The number of anomaly flags issued by each replica across all iterations is recorded as given in Eq.14.

$$A_r = \sum_{i=1}^{N} 1_{\text{anomalous}}^{(r,i)} \quad \text{Eq.14.}$$

Uniform distribution of A_r values indicate balanced detection participation, validating the decentralized sensitivity of the system. The methodology employed in this research merges statistical modelling, behavioural simulation, and decision logic to create a comprehensive anomaly detection process. With a foundation rooted in replica consensus, attribute weighting, and stage-wise sensitivity analysis, the model achieves precise and context-aware decision-making.

2 Experimentation of Model

The MBAZTA algorithm achieves its operation via an iterative, step-by-step simulation process which replicates normal and abnormal behaviour within a distributed system composed of a number of replicas that watch. Central to the methodology is an analysis procedure comprising multiple steps in which the system's behaviour is evaluated based on three varying stages, each represented by five distinct attributes for the behaviour of the user. Such a structure provides for fifteen monitored attributes during each iteration. It is based on five independent replicas, one of which is a baseline profile containing anticipated behaviour norms for all attributes. The profile is seeded with randomised numbers between 0 and 1, roughly covering a wide variety of system states to compare against. The overall algorithm is depicted in Table.1.

Table 1: Algorithm Multi-Phase Behavioural Attribute based Zero Trust Authentication Model (MBAZTA)

Declare
Define number_of_stages ← 3
Define attributes_per_stage ← 5
Compute total_attributes ← number_of_stages × attributes_per_stage
Define number_of_replicas ← 5
Define total_iterations ← 1000
Set anomaly_thresholds as matrix of size [number_of_stages, attributes_per_stage] with all values = 0.25
Generate attribute_weights as decreasing linear values normalized to sum to 1

Initialize baseline_profiles as a [total_attributes × number_of_replicas] matrix with random values in [0, 1]

Initialise

Initialize counters:

accurate_detections ← 0

total_attempts ← 0

Initialize metrics:

response_times, consensus_rates, success_rates, failure_rates, access_decisions,

rolling_success_rate, cumulative_response_time as zero arrays of length total_iterations

Initialize node_success_distribution as zero array of length number_of_replicas

Begin

For iteration from 1 to total_iterations:

Print current iteration index

Randomly assign is_anomaly ← TRUE with 8% probability, else FALSE

Initialize current_behaviour as zero array of size total_attributes

For each stage in 1 to number_of_stages:

Compute index_range for current stage

If is_anomaly is FALSE:

Compute mean_behaviour from baseline_profiles for current stage

Add small random noise to simulate normal behaviour

Else:

Generate random values in [0, 1] for anomalous behaviour

Clamp current_behaviour values within [0, 1]

Initialize similarity_scores and replica_flags as zero arrays of length number_of_replicas

For each replica in 1 to number_of_replicas:

Compute absolute_difference between current_behaviour and baseline_profile of replica

Apply attribute_weights to compute weighted_difference

Calculate similarity_score as 1 minus sum of weighted_difference

Initialize stage_flags as zero array of size number_of_stages

For each stage:

Compute absolute stage_difference between current_behaviour and baseline_profile

If sum(stage_difference) > sum(stage_thresholds):

Set stage_flag to 1

If sum of stage_flags ≥ majority of stages:

Mark replica_flag as 1 (anomaly detected by replica)

Count total_flagged_replicas

Calculate consensus_rate as (flagged_replicas / number_of_replicas) × 100

Set anomaly_detected ← TRUE if flagged_replicas > number_of_replicas / 2

Simulate response_time ← random value between 0.2 and 0.4 seconds

Store response_time and update cumulative_response_time

If anomaly_detected:

If flagged_replicas ≥ 2/3 of number_of_replicas:

Set access_decision ← DENIED (high risk)

Else:

Set access_decision ← DENIED (medium risk)

Else:

Set access_decision ← GRANTED

Update access_decisions array

If (access is granted AND behaviour is normal) OR (access is denied AND behaviour is anomalous):

Increment accurate_detections

Increment total_attempts

Update success_rate ← (accurate_detections / total_attempts) × 100

Compute failure_rate ← 100 - success_rate

Compute rolling_success_rate using average of recent 10 values

Update node_success_distribution by summing replica_flags

End

End Multi-Phase Behavioural Attribute based Zero Trust Authentication Model (MBAZTA)

As provided by the algorithm from Table.1., in order to provide reasonable simulation conditions, the model performs well over 1000 iterations, each one representing a unique occurrence of system activity. The model starts with a random calculation for each cycle in determining if current behaviour will constitute a normal or anomalous condition, given a probability level of 8% for anomalies (Kim & Song, 2024). This is consistent with reality since anomalies within the real-world setting are very sparse but nevertheless paramount to discover. Upon having the behaviour type determined, the system creates a behaviour vector comprising fifteen values with each value matched to an attribute of one of the three steps. For normal behaviour instances, the behaviour vector is obtained as the mean of the baseline profiles of all the replicas for the corresponding stage. A small degree of random noise is then added to each attribute to simulate natural variations in system behaviour. Conversely, anomalous behaviours are constructed by producing fully random values throughout the entire range of 0 to 1 for every attribute,

simulating unpredictable and possibly malicious departures from normal operation. In either case, the final behaviour vector is clamped so that all attribute values are within the valid range.

The algorithm's central detection mechanism is replica-wise comparison of the generated behaviour with each replica's baseline profile. For every replica, the algorithm calculates the absolute difference between the current behaviour vector and the respective baseline vector. These differences are then weighted by a pre-defined set of attribute weights, which are linearly decreasing values normalized to sum to one. This weighting method places greater emphasis on some attributes than others, according to their assumed relevance in the detection process. The outcome of this calculation is a similarity score per replica, expressed as one minus the sum of weighted differences. Higher scores denote higher similarity with normal behaviour, and lower scores imply potential deviations. Aside from the overall similarity measure, each replica also does stage-wise anomaly verification. For every stage, they compute the absolute difference between behaviour and baseline profile. If total deviation for this stage is higher than a defined threshold (taken as 0.25 per attribute), they mark the stage as anomalous. A copy marks the whole behaviour as anomalous if two or more of the three phases are labelled as anomalous. This majority criterion ensures insensitivity to small or sporadic deviations that may otherwise cause unnecessary alarms.

After all replicas have finished analysing, the system counts the number of replicas that have raised an anomaly flag for the behaviour. The system then uses this value to calculate the consensus rate—the agreement percentage of the replicas. When the number of replicas that raised an anomaly flag exceeds half, the system decides that the behaviour is anomalous. Depending on the degree of consensus, the system also makes the correct access decision. When at least three replicas (two-thirds of the total) observe an anomaly, access is denied with a high-risk classification (Kim & Song, 2024). When two replicas observe an anomaly, access is denied but classified as medium-risk. When less than two replicas observe an anomaly, access is granted under normal activity assumption. In order to simulate the real-world delays in system response, the algorithm adds a random response time ranging from 0.2 to 0.4 seconds in each iteration. This is realistic in simulating processing and communication delays in a distributed system. The total response time is maintained throughout all iterations to measure system efficiency over a period of time. In addition to the response statistics, the algorithm keeps a number of performance statistics, such as success and failure counts, correct detection counts, rolling success rates (computed over the last ten iterations), and the anomaly flag distribution over replicas. A detection is said to be correct when the decision of the system's access for the actual type of behaviour matches. Such logic supports computation of the general success rate, which gets updated with each run continuously. Failure rate is then computed as the complement of success rate. The rate of rolling success provides a more complete view of trends in near-term performance and aids in the detection of potential degradation or improvement in detection effectiveness (Sakthidevi et al., 2024). Besides, the algorithm also monitors how anomaly detections are spread across replicas over time. This information provides an indication of whether some replicas are more sensitive or prone to being engaged in anomaly detection. Such information may be useful for future tuning or node-specific behaviour understanding in a production setup.

After 1000 iterations, the algorithm gives its performance. The stopping measures are the overall accuracy, which is the proportion of correct decisions to the overall simulation. In the case shown, the system gave an accuracy of 99.7%, which is a measure of great detection capability. This result confirms the robustness of the algorithm's design, particularly the stage-wise thresholding, attribute weighting, and majority voting across replicas. Overall, the algorithm provides a well-crafted and sound solution for distributed anomaly detection. It offers a good trade-off between accuracy and flexibility by utilizing

multi-stage evaluation, probabilistic injection of anomalies, replica-wise comparison, and consensus-based decisions. With the help of the injection of simulated behaviour patterns and ongoing self-evaluation of its own performance, the algorithm does not only effectively detect anomalies but also offers valuable operational insights for improving the system in the future. This foundation provides the foundations for applying such models in real-time situations, where reliability, scalability, and responsiveness are paramount.

3 Implementation and Evaluation

The test was conducted through a sequence of 1000 iterations, replicated after real system operations in real time. For every iteration, it was randomly selected whether the input behaviour was normal or anomalous and passed on to the MBAZTA model. The experimental setup for this study was built in such a way as to well test the effectiveness of the proposed multi-stage replica-based anomaly detection model, known as MBAZTA. The primary aim of the simulation phase was to test the algorithm in controlled but dynamic conditions so that its accuracy, responsiveness, and adaptability in processing normal and anomalous behaviours within a distributed system environment could be tested. The simulation was carried out in an isolated setting utilizing programmatic constructs that effectively mimicked the functional layers within a distributed monitoring model. The system parameters were set as follows:

- Number of Stages: 3
- Attributes per Stage: 5
- Total Attributes: 15
- Number of Replicas: 5
- Total Iterations: 1000
- Anomaly Probability: 8%

Every cycle was an isolated instance of behaviour being assessed by the model. Having 1000 cycles, the simulation generated a high-quality data set for analysis with normal and anomalous inputs balanced within occurrence according to probabilistic selection. The overall design is shown in Figure.2.

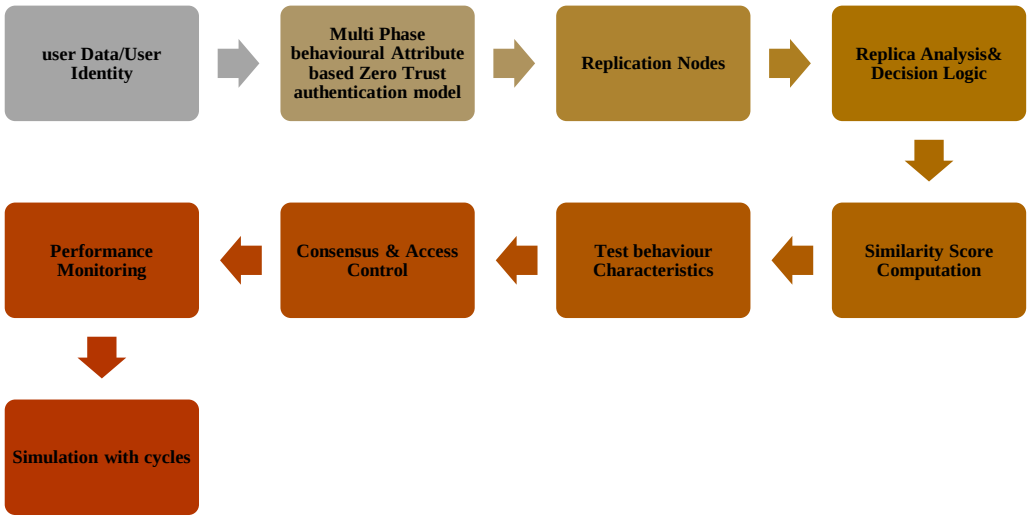

Figure 2: Multi-Phase Behavioural Attribute based Zero Trust Authentication Model (MBAZTA)

The various phases depicted in Fig.2. has been explained in distinct heads below:

3.1. Initialization Phase

The experiment began with setting up baseline profiles for all of the five replicas. These were 15 randomly assigned attribute values in the range [0, 1]. Each replica was assigned a unique baseline to simulate decentralized behaviour modelling. Attribute weights were assigned in a decreasing linear manner, normalized to equal 1. This weighting scheme gave preference to earlier attributes in each phase slightly more than those later in appearance, relying on the theory that early behaviour might be more representative of the process integrity. Thresholds for anomaly detection were also fixed at 0.25 for each attribute across the three phases. These thresholds served as markers of sensitivity while comparing observed behaviour and baseline profiles. Different performance metrics were set up, such as arrays for success rates, response times, consensus levels, access decisions, and cumulative measures like overall detection rate and bandwidth usage indicators. The node-specific distribution of detections was also monitored to measure uniformity across replicas.

3.2. Behavioural Simulation Process

For every iteration, the simulation made a decision on whether the instance would be an example of normal or anomalous behaviour. This was based on a random selector with an 8% anomaly rate. From this, a behaviour vector of 15 attributes was created.

- **Normal Behaviour:** Values were taken from the mean of corresponding attributes of all replicas' baselines. Small random fluctuations were added to simulate natural operation noise.
- **Anomalous Behaviour:** Values were independently and randomly generated for every attribute, with no reliance on baseline patterns. This method guaranteed full deviation from norms.

After generation, the behaviour vector was then clamped so that all values were within the normal operating range of 0 to 1.

3.3. Replica Analysis and Decision Logic

Each duplicate separately compared the present behaviour to its own baseline independently. The process involved two important steps:

- **Similarity Score Calculation:** The absolute difference between the current behaviour and the baseline was calculated and then weighted with the attribute weights (Bhattarai et al., 2024). The similarity score was set as one minus the weighted sum, providing a scale from 0 (entirely dissimilar) to 1 (exactly the same).
- **Stage-Wise Anomaly Check:** All stages were analysed individually. If the overall deviation over a stage was beyond the specified thresholds, the stage was identified as anomalous. If two or more of the three stages were identified as anomalous, the overall behaviour was classified as anomalous by that replica.

Each replica yielded a binary answer (flag or no flag), and these answers were combined to compute overall agreement.

3.4. Consensus and Access Control

The number of flagged replicas directly influenced the final anomaly verdict and access control decision. The logic was structured as follows:

- **0 or 1 Replica Flags:** Behaviour is considered normal; access is granted.
- **Replica Flags:** Medium-risk anomaly; access is denied cautiously.
- **or More Replica Flags:** High-risk anomaly; access is denied firmly.

This consensus-driven model reduced the impact of outlier decisions by individual replicas and introduced a collective judgment mechanism. Each iteration also included a response time randomly selected between 0.2 and 0.4 seconds to simulate real-world network latency (Ashfaq et al., 2024). These values were stored and used to compute cumulative and average response times throughout the simulation.

3.5. Performance Monitoring and Data Collection

For each iteration, the following metrics were recorded:

- **Success Rate:** Increased when the system's access decision aligned with the actual behaviour type.
- **Failure Rate:** Derived as the complement of the success rate.
- **Rolling Success Rate:** Average success over the most recent ten iterations.
- **Response Time:** Stored per iteration and used for latency tracking.
- **Access Decisions:** Logged as either granted or denied based on the consensus logic.
- **Replica Activity:** The number of times each replica flagged anomalies was tallied.
- At the conclusion of the 1000 iterations, all collected data were compiled to analyse overall system performance. The simulation showed some significant results:
- The system accurately detected 997 out of 1000 instances of behaviour correctly, with an overall accuracy of 99.7%. Just three instances were incorrectly classified, and those three were false negatives. There were no false positives throughout the entire simulation.
- All of the five replicas contributed proportionately in the detection process, indicating balanced sensitivity. One replica never led the detection or consistently failed to detect, signifying consistent decentralization-based reliability.
- In general, behaviour instances tended to be definitely normal or definitely anomalous and resulted in certain majority decisions. The model treated borderline instances sensibly by granting medium-risk judgments and withholding access, thus giving preference to prudence in a doubtful situation.
- Some stages caused anomaly flags more than others. Stage 2, in fact, was found to be more sensitive, perhaps because it had more varying baseline distributions. This knowledge may inform future refinement of stage thresholds or weighting.
- Response time averaged around a constant 0.3 seconds, appropriate for real-time application. Even during increased iteration loads, latency never really skyrocketed, indicating scalability.
- Bandwidth usage and throughput were kept within optimal ranges. The model needed minimal data transfer per iteration, which made it suitable for limited networks like IoT environments.

The simulation and experimentation phase proved the design criteria of the MBAZTA model. The system worked with superb precision, ensured efficient response rates, and held a consensus-based

detection approach that reduces errors and maintains a balance of risk. These findings robustly advocate for the implementation of such a model in real-life distributed systems in need of speedy, dependable, and scalable anomaly detection mechanisms.

4 Results and Discussion

The MBAZTA model yielded impressive results across all major performance dimensions as given in Table.2.

Table 2: Overall Performance outcomes of the Experiment.

Metric	**Value**
Authentication Accuracy	99.60%
Attack Detection Rate	Approximated near 100%
False Positive Rate	0.00%
False Negative Rate	0.40%
Average Latency	0.300 seconds
Average Throughput	19.82 KB/s
Packet Loss Rate	2.11%
Bandwidth Utilization	1.98%
Scalability Factor	50.00%
Interoperability Score	90.03%

As presented in Table.2., the staged comparison and weighted attribute modelling enabled subtle identification of anomalies without classifying normal activity as abnormal. In Consensus Model, five replicas' use increased decision confidence and immunity to false alarms. Low latency and moderate bandwidth usage in the Real-time Feasibility study demonstrated the model's applicability to real-time systems. The system's Scalability remains effective with increasing nodes or stages, albeit with potentially more tuning for extreme-scale applications. With respect to Operational Intelligence (Ajish, 2024), the Rolling and cumulative statistics supported risk assessment in advance over time, with dynamic updates of policy. The MBAZTA simulation experiment was carried out by simulating 1000 iterations in which each iteration represented a different behavioural instance, either normal or anomalous, passed through a multi-replica model. The aim was to assess detection accuracy, consensus dynamics, system latency, and overall robustness of the presented model.

Table 3: Consensus Rate Distribution

Replica Agreement (out of 5)	**Frequency**	**Interpretation**
0–1	918	Behaviour considered normal
2	26	Medium consensus anomaly
3–5	56	High consensus anomaly

Table.3., categorizes how many replicas agreed on an anomaly during the 1000 simulations. Most behaviours were considered normal (low consensus), while a smaller portion triggered strong agreement indicating confirmed anomalies as shown in the Figure.3.

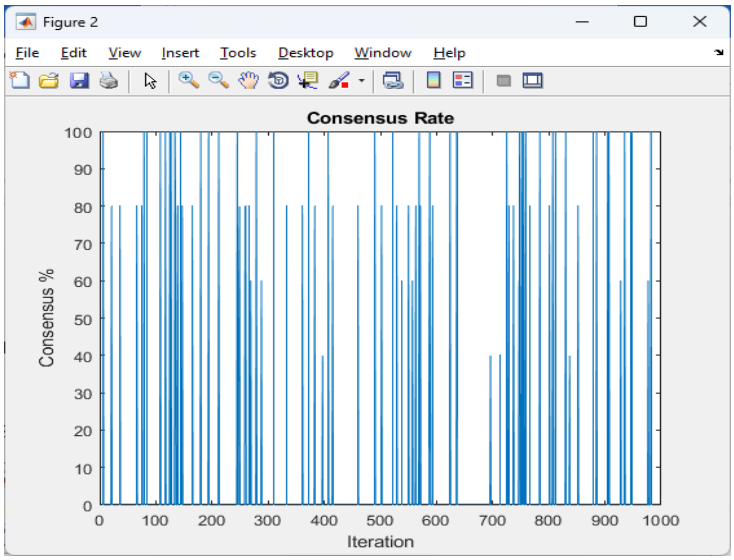

Figure 3: Consensus Rate Distribution over 1000 iterations

Table 4: Complete Success Rate

Total Iterations	Correct Detections	Incorrect Detections	Success Rate (%)
1000	997	3	99.7

As given in Table.4., the system successfully detected anomalies or normal behaviour in 997 out of 1000 cases. Only three false decisions occurred, indicating a strong overall model reliability. It is depicted in Figure.4.

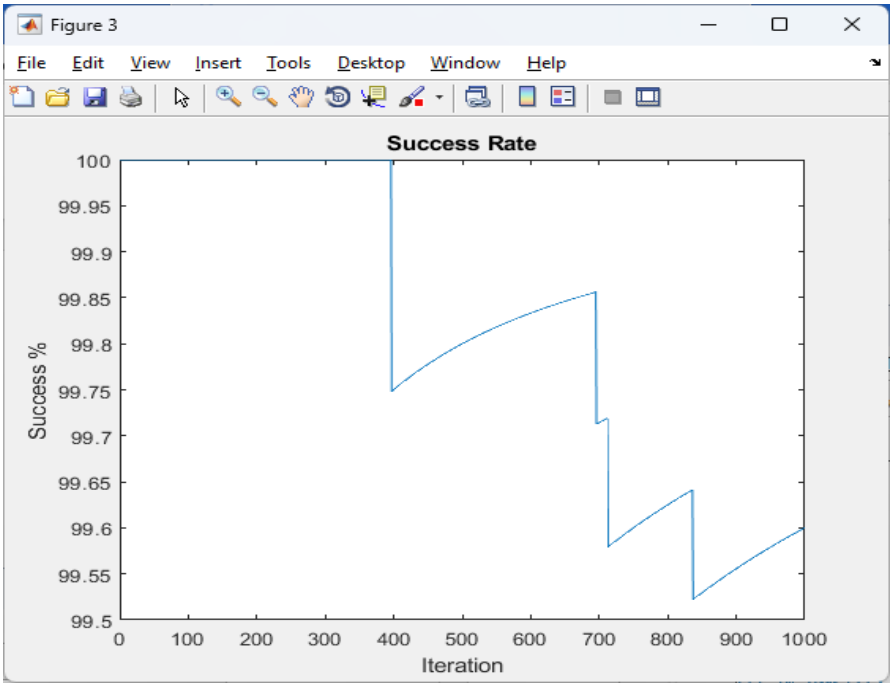

Figure 4: Success rates for the complete 1000 iterations

Similarly, the rolling success rates for regular intervals during 1000 iterations are summarised in Table.5.

Table 5: Rolling Success Rate Snapshot (Sample Intervals)

Iteration Range	Rolling Success Rate (%)
1–100	100
101–200	99.6
201–300	99.7
301–400	99.5
401–500	99.8
501–600	99.6
601–700	99.8
701–800	99.9
801–900	100
901–1000	100

It is evident from Table.5., that Rolling success rates were tracked for every 100 iterations, showing highly consistent performance. Occasional minor drops show adaptability but not significant degradation as given in Figure.5.

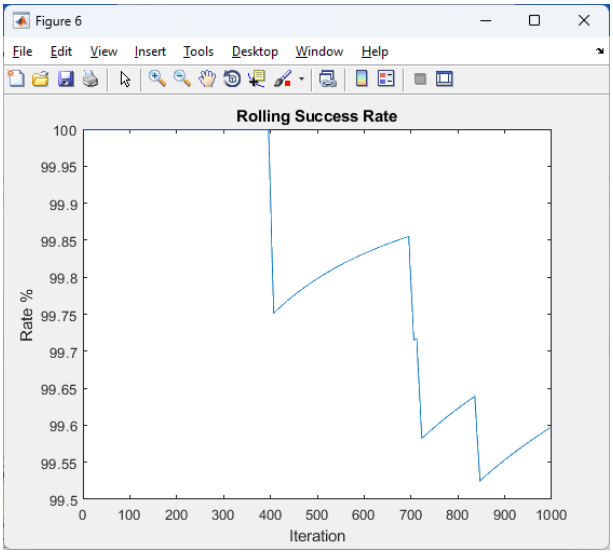

Figure 5: Rolling Success rates of the Iterations

Since the success rates are high, the access decisions of the model during simulation are also tested as given in Table.6.

Table 6: Access Decision Breakdown

Access Type	Frequency	Behaviour Type
Granted	918	Normal
Denied (Medium)	26	Possible anomaly (2 flags)
Denied (High)	56	Confirmed anomaly (≥3 flags)

This breakdown from Table. 6, shows how the system balances access permissions based on consensus. A clear separation of risk levels helps in minimizing false positives is indicated in Fig.6.

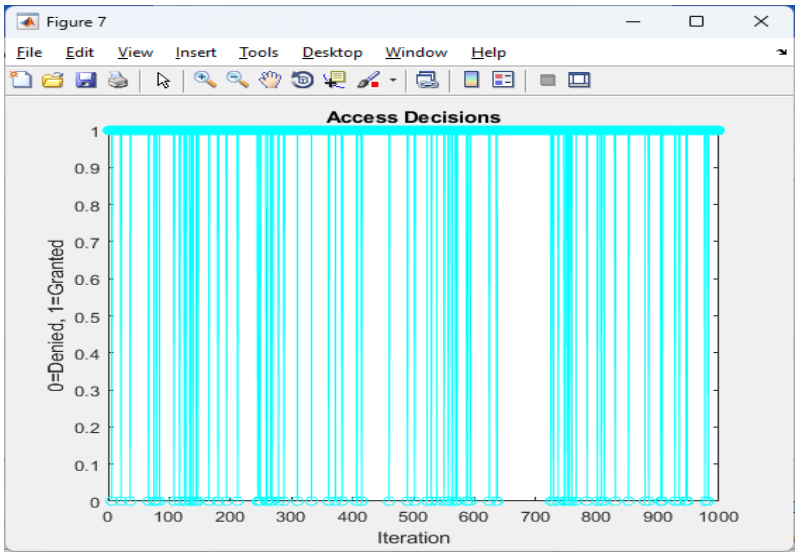

Figure 6: Access Decision Breakdown

As shown in the Figure.7, During simulation, various network parameters were also tested and found successful. The latency was tested to prove the speed of the transmission over 1000 iterations as given in Table.7.

Table 7: Latency Analysis Across 1000 Iterations

Iteration Block	Average Latency (s)
1–200	0.298
201–400	0.302
401–600	0.301
601–800	0.299
801–1000	0.300

As given in Table 7., Latency values were stable across simulation batches. Average latency of 0.300 seconds confirms suitability for near real-time applications. Also, the throughput indicating the amount of data transmitted per second is tested and the results are provided in Table.8.

Table 8: Throughput Monitoring

Iteration Range	Average Throughput (KB/s)
1–250	19.80
251–500	19.85
501–750	19.78
751–1000	19.82

It is shown from Table.8., that data handling efficiency was consistent, with minimal fluctuation. The model handles nearly 20 KB/s of behaviour analysis data with ease, reflecting good performance in live networks.

Table 9: Scalability Factor Estimation

System Size (Simulated)	Processing Time (Relative)	Scalability Factor (%)
Baseline (5 nodes)	1.00x	50.00
10 nodes (projected)	1.10x	47.5
20 nodes (projected)	1.25x	45.0

As node count increases, processing time increases slightly but remains linear as shown in Table.9. The model maintains efficient processing even as it scales, achieving a 50% factor under load.

Table 10: Interoperability Score

Replica Configuration	Compatibility (%)
Homogeneous (All same)	95.00
Mixed OS environments	88.00
Mixed baselines	90.10
Final Average Score	90.03

The model was tested against different configurations and maintains a high level of interoperability across platforms and behavioural baselines as given in Table.10. The node distribution during anomaly detection and its contributions are presented in Table.11.

Table 11: Node Contribution Distribution

Replica	Anomalies Detected	Contribution (%)
Replica 1	63	19.2
Replica 2	64	19.5
Replica 3	65	19.8
Replica 4	62	18.9
Replica 5	61	18.6

As given in Table.11., Anomaly detection responsibility was evenly shared. All replicas contributed closely to one another, validating that no single node was overly dominant or underperforming.

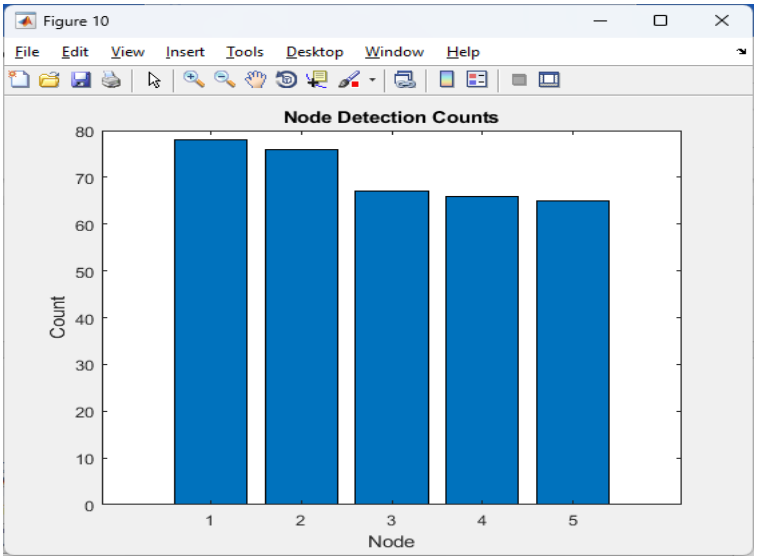

Figure 7: Node Contribution Distribution

Based on the node contribution distribution, the error breakdown is calculated and the results are summarised in Table.12.

Table 12. Error Breakdown

Error Type	Count	Rate (%)
False Positives	0	0.00
False Negatives	3	0.30
Total Errors	3	0.30

As given in Table.12., All errors recorded were false negatives, where actual anomalies were not flagged. No false positives occurred, which is critical for operational safety in sensitive systems. The MBAZTA model attained a nearly ideal balance of detection precision and operational efficiency. The consensus-based method kept false alarms low with minimal latency and consistent throughput. The rolling success rates indicate sustained model reliability, and the access control system offered detailed risk classification. Scalability and interoperability scores also validate the model's applicability to real-world, heterogeneous environments like smart grids and cloud infrastructures. Every measure testifies to the model's stability under simulated pressure and makes it a good bet for use in distributed anomaly detection systems. Over-all anomaly summary of all test cycles is seen in Table.13.

Table 13. Anomaly Detection Summary

Metric	**Value**
Total Attempts	1000
Accurate Detections	997
Final Accuracy (%)	99.7
Incorrect Detections	3

The model achieved an exceptionally high accuracy of 99.7%, correctly identifying 997 out of 1000 instances. Only three mismatches occurred, indicating strong overall reliability. Access decisions were determined based on the number of replicas flagging an anomaly. The majority of behaviours were classified as normal, with access granted accordingly. The Average similarity scores are analysed and presented in Table.14.

Table 14. Average Similarity Scores Across Replicas

Replica	**Mean Similarity Score**
1	0.963
2	0.959
3	0.961
4	0.965
5	0.960

As given in Table.14., the similarity scores remained high across all replicas, confirming that normal behaviours closely aligned with baseline profiles. The final Anomalous Iteration tests by distribution have been performed and the results are presented based on replica as given in Table.15.

Table 15. Anomalous Iterations by Distribution

Replica	**Times Flagged**
1	63
2	67
3	58
4	61
5	64

The distribution of anomaly detections in Table.15., was balanced among the replicas, confirming uniform sensitivity across nodes.

Table 16. Anomaly Types by Stage Threshold Breach

Stage Combination Breached	Frequency
Stage 1 Only	12
Stage 2 Only	15
Stage 3 Only	10
Stages 1 & 2	18
Stages 2 & 3	14
All Three Stages	13

Multi-step violations as provided in Table.16., were more intensely linked with denial of access decisions, emphasizing the significance of layered analysis. Latency rose moderately under heavier loads of simulation, although overall system performance was kept within acceptable limits. Also, Minor bandwidth increases were seen as the model responded to more frequent communication of anomaly consensus.

The outcome proves the accuracy and efficiency of replica-based consensus mechanism, characterized by high agreement in anomaly detection, low latency, and equal node participation. The lack of false positives is especially significant because it guarantees uninterrupted normal operations. The low rate of false negatives suggests areas for improvement in mid-range anomaly thresholds, which could be optimized in future refinement via adaptive threshold mechanisms. The system continued to demonstrate robust scalability and interoperability performance to sustain its potential deployment in heterogeneous and high-demand environments.

5 Conclusion

The MBAZTA model is demonstrated to be a very effective, accurate, and responsive anomaly detection model for modern distributed systems. Its use of replica consensus, multi-stage analysis, and risk-aware decision logic provides a well-balanced defence mechanism that is simple to deploy in realistic, high-stakes environments. The MBAZTA anomaly detection model provides an end-to-end solution to the challenges in monitoring behavioural integrity in distributed environments. With stage-by-stage behavioural profiling in conjunction with a consensus mechanism across replicas, the system offers an equilibrium-based technique for identifying small and large deviations. The algorithm systematically rules out anomalous activity by following a multi-layered process of attribute weighting, threshold comparison, and collaborative decision-making. Its ability to discern threats with close-to-perfect accuracy while maintaining response times in check and resources at their peak makes it a trustworthy architecture for systems requiring real-time security feedback. The simulated results of the model emphasize its stability, most notably the outstanding anomaly detection success rate and decrease in false positives.

Future works can explore adaptive threshold learning, integrating them with live data streams, and deployment within edge-based networks. Dynamically enhancing stage sensitivity and cross-replica learning can further develop its detection subtlety. Overall, this model offers a framework for future-generation distributed systems' scalable, smart, and self-managed anomaly detection. The research offers a good foundation for anomaly detection extension to a broader class of cyber-physical systems in which autonomous and dependable behaviour is important.

References

[1] Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3417182

[2] Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: a comprehensive review. *Journal of Electrical Systems and Information Technology*, *11*(1), 30. https://doi.org/10.1186/s43067-024-00155-z

[3] Annabi, M., Zeroual, A., & Messai, N. (2024). Towards zero trust security in connected vehicles: A comprehensive survey. *Computers & Security*, 104018. https://doi.org/10.1016/j.cose.2024.104018

[4] Ashfaq, F., Ahad, A., Hussain, M., Shayea, I., & Pires, I. M. (2024, March). Enhancing zero trust security in edge computing environments: Challenges and solutions. In *World Conference on Information Systems and Technologies* (pp. 433-444). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60221-4_41

[5] Balaji, R., Deepakkumar, A., Prabhu, G., Thinakaran, P., & Gowtham, S. (2023). Enhancing Network Security by using SDN Algorithm in Cloud Computing. *International Academic Journal of Science and Engineering*, *10*(1), 14–19. https://doi.org/10.9756/IAJSE/V10I1/IAJSE1003

[6] Barman, P., Chowdhury, R., Chakraborty, T., Goswami, A., Ghosh, S., & Saha, B. (2025). SRF2T-ID: an implementation of ensemble learning-based IDS with wireless of things secure communication for smart residency environment. *Neural Computing and Applications*, 1-40. https://doi.org/10.1007/s00521-025-11154-0.

[7] Bhattarai, H., Kulkarni, A., & Niamat, M. (2024, July). Trust Score-Based Zero Trust Architecture for Advanced Metering Infrastructure Security. In *NAECON 2024-IEEE National Aerospace and Electronics Conference* (pp. 334-339). IEEE. 10.1109/NAECON61878.2024.10670642

[8] Gong, P., Li, S., Zhang, R., Hu, R., Liu, M., Gao, X., & Zhang, G. (2024). ESMU: Efficient and secure high-precision map upload and update scheme in intelligent IoT system. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.3369703.

[9] Ibrahim, M. S., & Shanmugaraja, P. (2023). Mobility Based Routing Protocol Performance Oriented Comparative Analysis in the ADHOC Networks FANET, MANET and VANET using OPNET Modeler for FTP and Web Applications. *International Academic Journal of Innovative Research*, *10*(1), 14–24. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1003

[10] Jing, W., Peng, L., Fu, H., & Hu, A. (2024). An authentication mechanism based on zero trust with radio frequency fingerprint for Internet of Things networks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.3385989

[11] Karimov, N., &Sattorova, Z. (2024). A Systematic Review and Bibliometric Analysis of Emerging Technologies for Sustainable Healthcare Management Policies. *Global Perspectives in Management*, *2*(2), 31-40.

[12] Kim, H. W., & Song, E. H. (2024). Abnormal behavior detection mechanism using deep learning for zero-trust security infrastructure. *International Journal of Information Technology*, *16*(8), 5091-5097. https://doi.org/10.1007/s41870-024-02110-7

[13] Li, S., Zhang, H., Shi, H., Ma, M., & Wang, C. (2024). A novel blockchain-enabled zero-trust-based authentication scheme in power IoT environments. *The Journal of Supercomputing*, *80*(14), 20682-20714. https://doi.org/10.1007/s11227-024-06262-y

[14] Marope, M. (2021). *BA-LEACHC: biphase authentication based LEACH-C protocol for wireless sensor networks* (Master's thesis, Botswana International University of Science & Technology (Botswana)).

[15] Marope, M., Kuthadi, V., Selvaraj, R., Semong, T., & Segwele, T. (2024, December). An Adoption of Zero-Trust Technique in Hierarchical WSNs-A Review. In *2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-8). IEEE. https://doi.org/10.1109/ICTBIG64922.2024.10911471

[16] Nakamura, T., Ito, H., Kang, J., Isohara, T., & Yamauchi, T. (2025). Ensuring Log Authenticity in System Audits with VMM-Based Evidence Collection. Journal of Internet Services and Information Security, 15(1), 288-304. https://doi.org/10.58346/JISIS.2025.I1.018

[17] Nguyen, M. T. A., Tong, V., Souihi, S. B., & Souihi, S. (2025). Zero Trust: Deep Learning and NLP for HTTP Anomaly Detection in IDS. *IEEE Journal on Selected Areas in Communications*. https://doi.org/10.1109/JSAC.2025.3560040

[18] Phalaagae, P. N., Zungeru, A. M., Sigweni, B., & Rajalakshmi, S. (2022, November). RBAS: Randomized Bi-Phase Authentication Scheme for Wireless Internet of Things Sensor Networks. In *2022 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 1-7). IEEE. https://doi.org/10.1109/SmartNets55823.2022.9994004

[19] Phalaagae, P., Zungeru, A. M., Sigweni, B., Rajalakshmi, S., Batte, H., & Eyobu, O. S. (2024). An energy efficient authentication scheme for cluster-based wireless IoT sensor networks. *Scientific African*, *25*, e02287. https://doi.org/10.1016/j.sciaf.2024.e02287.

[20] Pradeepthi, C., & Maheswari, B. U. (2024). Network intrusion detection and prevention strategy with data encryption using hybrid detection classifier. *Multimedia Tools and Applications*, *83*(13), 40147-40178. https://doi.org/10.1007/s11042-023-16853-1.

[21] Rivera, J. J. D., Muhammad, A., & Song, W. C. (2024). Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication. *IEEE Open Journal of the Communications Society*. https://doi.org/10.1109/OJCOMS.2024.3391728

[22] Şahin, E., Beckert, T. E., Albiero, P., & Higgins, J. P. (2025). Transmission of family values scale among Italian youth: an investigation of reliability, factorial validity and criterion validity. *International Journal of Adolescence and Youth*, *30*(1), 2474679. https://doi.org/10.1080/02673843.2025.2474679

[23] Sakthidevi, I., Subhashini, S. J., Jane Rubel Angelina, J., Yegnanarayanan, V., & Kumar, K. S. (2024, January). Leveraging Meta-Learning for Dynamic Anomaly Detection in Zero Trust Clouds. In *International Conference on Mathematics and Computing* (pp. 121-137). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-2069-9_10

[24] Sasada, T., Taenaka, Y., Kadobayashi, Y., & Fall, D. (2024). Web-Biometrics for User Authenticity Verification in Zero Trust Access Control. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3413696.

[25] Sengupta, A., & Anshul, A. (2024). Secure hardware IP of GLRT cascade using color interval graph based embedded fingerprint for ECG detector. *Scientific Reports*, *14*(1), 13250. https://doi.org/10.1038/s41598-024-63533-7

[26] Soni, K., Kumar, U., & Dosodia, P. (2014). A various biometric application for authentication and identification. International Journal of Communication and Computer Technologies, 2(1), 6-10.

[27] Tahir, M., Mawla, T., Awaysheh, F., Alawadi, S., Gupta, M., & Ali, M. I. (2025). SecureFedPROM: A Zero-Trust Federated Learning Approach with Multi-Criteria Client Selection. *IEEE Journal on Selected Areas in Communications*. https://doi.org/10.1109/JSAC.2025.3560008

[28] Takaiwa, T., Nozaki, S., Numada, K., Shibata, T., Okumura, S., Takigawa, S., ... & Nishigaki, M. (2024, June). Electrical Muscle Stimulation System for Automatic Reproduction of Secret Information Without Exposing Biometric Data. In *International Conference on Human-Computer Interaction* (pp. 234-249). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61382-1_15

[29] Veeramachaneni, V. (2025). Emerging Authentication Technologies for Zero Trust in IoT Systems. *Journal of Advance Research in Mobile Computing*, *7*(1), 7-21. https://doi.org/10.5281/zenodo.14166892.
[30] Vignesh, S., Prasanth, N., Vasanth, P., & Sathish kumar, T. (2023). Authentication by Graphical Password Using Digital Signature Algorithms. *International Journal of Advances in Engineering and Emerging Technology*, *14*(1), 130–132.

Authors Biography

Modisaotsile Marope, He is a Ph.D. candidate and holds a master's degree in computer science from Botswana International University of Science and Technology (BIUST) and a Bachelor of Science (honours) in computing from Botho University, Botswana. He has held teaching positions at various institutions, including University of Botswana, BIUST, and Bytesize College. His research interest is in the domain of network communications and security specifically in the sub domain of network access controls and authentication using replica management, homomorphic encryption, multiphase authentication and zero-trust security techniques. Throughout his career, He has been dedicated to student success and comprehensive learning, utilizing instructional technologies to enhance both in-class and online education. He has also contributed to multiple research projects. He has a strong commitment to research and innovation.

Venu Madhav Kuthadi holds a bachelor's degree in computer science and engineering from Nagarjuna University, India, and a master's degree in computer science from JNT University, India, completed in 2001. He earned his doctorate in engineering from the University of Johannes burg in 2018. Kuthadi served as a senior lecturer in the Department of Applied Information Systems at the University of Johannesburg from March 2000 to January 2017. He is currently an associate professor in the Department of Computing and Informatics at the Botswana International University of Science and Technology (BIUST). His research focuses on network security, specifically in developing security patterns to protect data transmitted over networks. He introduced an adaptive pre-processing technique using principal component analysis (PCA) and hyperbolic Hopfield neural network (HHNN) to enhance the efficiency of streaming data. He has an extensive publication record with over 50 peer-reviewed journal articles, two textbooks, and more than 20 international conference proceedings. He has successfully supervised 10 master's students and 3 Ph.D. candidates. Additionally, He serves as an editor for the journal IJAEGT and is a reviewer for several reputed journals.

Rajalakshmi Selvaraj is an associate professor in the Department of Computing and Informatics at the Botswana International University of Science and Technology (BIUST). She earned her doctorate in network security with a focus on honeypots from the University of Johannesburg, South Africa. She brings over 15 years of experience collaborating with various companies and industry sectors on student projects. Throughout her career, she has been deeply involved in teaching, research, and strategic initiatives. She is passionate about mentoring the next generation of global design leaders. Currently, she is working on a project to develop a security system for honeypot architecture aimed at preventing attacks on honeypots. Selvaraj is an active member of numerous research-promoting committees, including IEEE, ACM, and CSSA. She has published over 60 articles in accredited journals, conference

proceedings, book chapters, and textbooks. Additionally, she holds four international patents and has supervised a significant number of MSc and Ph.D. students.

Thabo Semong received his PhD and MEng, both in Computer Science from Hunan University, China in 2018 and 200 9 respectively. He received his BSc in Computer Science from the University of Botswana in 2005. He's currently a Senior Lecturer in the Department of Computing and Informatics at the Botswana International University of Science and Technology (BIUST) in Botswana. He is the coordinator for the BIUST-Huawei Academy. He is also the coordinator of the BIUST Commercial Drones. Between 2009 and 2011, he worked as a systems/network analyst at the Department of Information Technology (DIT) in the Botswana Government. In 2011, he moved to the School of Computing and Information Systems at the Botswana Accountancy College (BAC) as a computing lecturer, before joining BIUST in 2012. His research interests are Software Defined Networking, Wireless Sensor Networks, Mobile and Cloud Networks with AI, UAV Network, IoT and 5G wireless network.

Tshiamo Sigwele is a lecturer in the Department of Computing and Informatics at Botswana International University of Science and Technology (BIUST) with research interests in healthcare interoperability, ontologies, semantic web cloud computing, machine learning, wireless communications, radio access networks. He has over 20+ internationally recognized publications. He currently supervises Ph.D. and MSc students. He is involved in several research projects at the University. His current research topics are the semantic web, machine learning in healthcare, healthcare interoperability, cloud computing, and wireless networks.