DS Journal of Cyber Security
Volume 3 Issue 2, 16-32, Apr - Jun 2025
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V3I2P102

Original Article

Behavior-Aware Cybersecurity: Integrating Trust Scores with Least Privilege via Game Theory

Bala Shanmukha Sowmya Javvadhi[1], Manas Kumar Yogi[2*]

[1,2]*Pragati Engineering College (Autonomous), Surampalem, Andhra Pradesh, India.*

**manas.yogi@gmail.com*

Received: 05 March 2025; Revised: 06 April 2025; Accepted: 04 May 2025; Published: 30 May 2025

Abstract - Dynamic computing environments question the validity of classical security institutions, especially the Principle of Least Privilege (PoLP), where predefined roles and behavior patterns are expected. These constraints prevent the system from customizing access rights per user context or dynamic trustworthiness, which usually leads to over-privileged or under-privileged access. In order to curtail this, a behavior-aware hybrid model that combines Game Theory with PoLP is introduced to allow for adaptive access control based on strategic play. The framework can make fine-grained privilege adjustments in real-time by modelling the user-system interactions as a repeated game and the dynamic assignment of trust scores based on observed behavior. Our method motivates compliant actions while discouraging harmful ones using thoughtful access reconfiguration. Some of the significant contributions are developing a trust score mechanism associated with privilege management, designing a game-theoretic engine to review user actions, and combining behavioral analytics with role-based controls. This model compromises between security and usability, providing scalable, context-aware solutions to rigid access policies. The proposed system can help push the boundaries of cyber security and pave the way for proactive, trust-aware access decisions that are especially critical in decentralized, cloud-based, and zero-trust architectures. These results provide new avenues for creating an intelligent and responsive security system consistent with the user intent and the system's integrity.

Keywords - Access controls, Cybersecurity, Game theory, Trust management, User behavior.

1. Introduction

1.1. Background

Controlling who can access systems is a key focus of cybersecurity as it is the first thing that keeps digital assets secure. It gives users rights to only the tools and data they are responsible for using. PoLP ensures that people are given just the necessary access, minimising the chances of improper system use.Although PoLP is crucial, problems with implementation using standard static methods like RBAC are common in recent computing contexts[1].

As companies move to cloud services, work remotely, use collaborative platforms and apply zero-trust architectures, the way access control systems operate should change. Static privilege assigning does not change with the changing role, temporary job substitutes or odd user activity. As a result, either too much access is provided, raising security risks, or work products suffer due to too many restrictions. Such problems create serious vulnerabilities in big, distributed systems, especially sensitive ones [2].

1.2. Research Gap and Problem Statement

Although traditional PoLP models are important, they are not flexible enough to respond instantly to new situations. Despite using attribute-based or context-aware approaches, current investigations in access control still use rules and rarely deal with behavioral aspects or trust.Additionally, the current literature does not connect game theory and trust analytics well into a single plan for access control[3]. Because Game Theory helps model different strategies people may take, it suggests new ways to understand user habits and adapt to digital settings. In addition, trust scoring techniques that look at behavior over a period can help differentiate those who mean harm from those who are helpful.Because these approaches are not covered by one model that can adapt, it leaves a significant gap in research in cybersecurity. Lacking this framework, systems cannot protect themselves from insider threats, privileges set incorrectly and slow action in response to dangerous user behaviors[4].

1.3. Motivation

Modern cybersecurity systems should respond, adapt and think by themselves. It is obvious from the first part of this work that static access policies alone are now insufficient for handling the demands of today's digital environments. As organizations grow and spread out their IT resources, how users behave strongly affects trust and risk[5]. Therefore, they develop algorithms that monitor trust dynamics and model strategic behavior using Game Theory.`This theory provides a systematic way to analyse how the system, users and attackers work together. When access control is seen as a signaling game, the system can understand user actions and what those actions represent[5]. When combined with a trust system that is constantly updated and reflects user behavior and the type of things done, this model makes access decisions more effective, relying less on human support.

The model increases protection by warning against dangerous actions and makes the system more usable by adjusting as users' roles and dependability evolve.

1.4. Research objectives

This research aims to formulate and verify an adaptive access control model that uses the basic PoLP approach and integrates Game Theory and scoring trust. In particular, our goals are these:

- Using a game-theoretic signaling model makes it possible to change permissions as user behaviors vary[6].
- Develop a trust scoring system that can develop over time by considering people's actions, anomaly alerts and compliance factors, using Bayesian techniques to make decisions when uncertain.
- Assess the model by testing it through simulations that imitate real-world situations. Test it also in healthcare information systems, where users face different duties and frequent access problems. The attention is on the ability of the system to catch suspicious activity, control who has access and answer rapidly to any new threats.
- To illustrate the positive differences and improvements of hybrid models, compared to earlier static and semi-dynamic models, in terms of their explanatory power, risks and scalability for operations.

Reaching these objectives, this research hopes to set out a solid, flexible and actively managing system for access control consistent with the current needs of cybersecurity[6].

2. Related Work

In recent years, access control methods have greatly improved, and both Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) have become common across many industries. In RBAC, access rights for individual users are set by roles already established in the organization. However, its strict design does not usually adapt when things change for users [7]. Alternatively, ABAC adds flexibility when deciding access through user-related factors, surrounding conditions, and resource concerns. However, neither RBAC nor ABAC can consider ongoing trust or changing actions when making access decisions. Overcoming these weaknesses has led researchers to present Risk-Adaptive Access Control (RAdAC) models. They react to real-time evaluations of risk, including aspects such as the place a device is being used, the time it is used, and network quality.

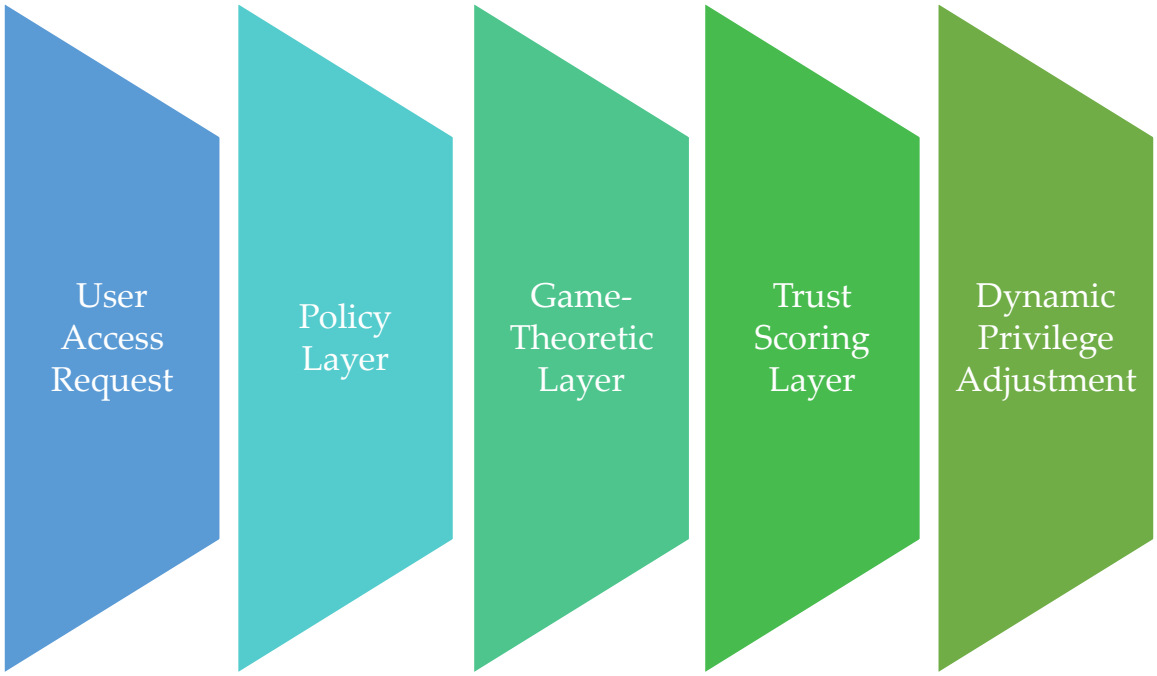

Fig. 1 Conceptual diagram of hybrid PoLP-game theory framework

However, in practice, most RAdAC systems count on predetermined ways to measure risk and often miss important long-term and behavior-level signals. Moreover, their use of fixed parameters and struggles to read complex information from users makes it harder for them to observe unusual behavior [8].Meanwhile, cybersecurity experts use Game Theory to investigate the way defenders and attackers strategize with each other. Optimal strategies for defense in adversarial situations have been modeled using Nash Equilibrium and Stackelberg Games. As an example, Stackelberg models help defenders decide ahead of time what to do based on predicted attacker actions. However, most of these applications focus on network security and threat analysis but are not linked much to access control systems.Experts are now studying how behavior monitoring can be tied into dynamic access policies. For example, some researchers suggest using machine learning to look at access logs to find instances where usage differs from regular activities. Other systems use frameworks that measure trust using people's past actions and activities on the system. Based on the trust levels, access control decisions are taken. Even so, these models typically do not use concepts from game theory and consider trust to remain the same or build up passively during interactions.The main innovation of this research is combining these different concepts into a single structure. With the help of signaling games, the proposed model reads users' intentions from their actions, and the trust score is refined based on the user's interactions with the system. Rather than previous methods, this method allows for instant changes in privileges without violating the PoLP principles.Furthermore, putting together static policy, strategy, and trust feedback produces a stronger and adjustable solution than regular models. This way, security teams can more easily notice minor risks and handle privileges more precisely, which matters in healthcare, finance, and cloud computing.

3. Proposed Hybrid Model

3.1. System Architecture

The proposed hybrid model presents A layered system architecture that integrates PoLP, Game Theory, and trust-based analytics to form adaptive access control for dynamic scenarios. This layered system is constructed to support safe, behaviour-aware authorities management among its three integrated parts [9]. The Policy Layer is the cornerstone that depends on PoLP in establishing standard access rights for users defined by their roles or

attributes.Users are provided with only key permissions required for their jobs, reducing overall threat exposure from the beginning.Strategic choices based on a game-theoretic framework are introduced in the Game Layer, which is above the policy layer. By using signaling games, this layer observes user activities (the system and users work together in a dynamic process to determine motives and adjust access privileges accordingly). This layer enables the system to pre-empt security measures before risks happen by studying probable adversary activities.The Trust Layer improves the model by determining a real-time trust score for each user depending on their behavior, previous compliance, and applicable situation data [10]. These scores apply to structures of access granting and behavioral strategies in the game layer, meaning that nuanced and continuous adaptation for maximal security is facilitated. Such layered design makes the system flexible and capable of building a strong and flexible response to the complex cybersecurity environment of our times.

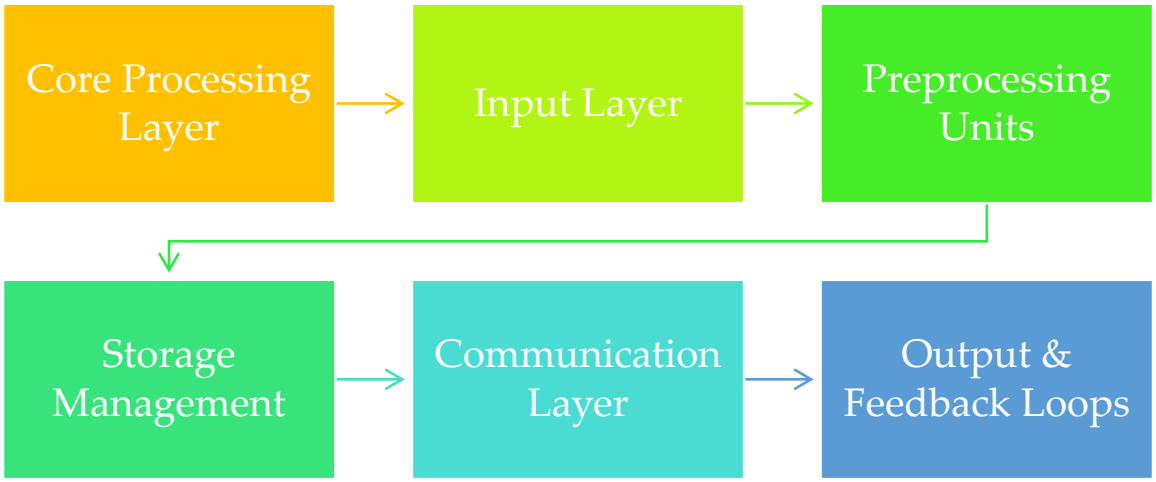

Fig. 2 Architectural schematic of the hybrid system

3.2. Game-Theoretic Components

The game-theoretic foundation of the proposed model involves intentionally modeling the dynamics of interactions of three key players: the user, the system and potential attackers. These participants operate continuously in signaling games that help make current access control selections based on observed actions and suspected intent [11].

Players in the game include:

- Users request access, expressing their intentions by their behaviour and actions.
- The system judges incoming signals against trust scores, determining access approval, denial, or modification through strategic reasoning [12].
- Attackers by impersonating authentic users to access and distort the system add to strategic uncertainty.

Strategies vary across players:

- Users declare themselves reliable and their intentions by actualizing their request for access rights to certain types of information, and their behaviors can blueprint their trustworthiness.
- The system does the screening, using signals and indicators of trust to select between granting, curbing, or revoking permissions.

A Payoff Matrix determines the pros and cons for players based on the tactics they take and, as such, determines the general course of the game. When their trustworthiness is established, genuine users enjoy faster access speed,

but attackers face increased surveillance [13]. The objective is to achieve maximum security with minimal negative impacts on operations. Such strategic planning enhances choices and makes the rational allocation of privileges in uncertain conditions possible.

3.3. Trust Scoring Mechanism

Access control decision is heavily affected by the trust scoring mechanism that dynamically reacts to user behavior. It utilizes behavioral information, such as access request results and anomaly detection outputs, that indicate differences in normal behavior by a user[14]. Based on these metrics, the system tracks and evaluates the reliability of each user as observed behaviors occur.To achieve live and environment-responsive scoring, the mechanism uses Bayesian inference to update the user's trust score every time the user does something. Using a probabilistic model, the system works with uncertainty and overwrites trust assessments by combining current and past actions [15]. Enhanced trust assists in increasing the number of options of access for the user, but a reduced level of trust may lead to more scrutiny or lack of permissions being available to the user.Trust scores support processes in the Game-Theoretic Layer and may result in reevaluation and calibration of baseline privileges in the PoLP Layer. The use of behavioral data in the scoring process enables the system to update access rights through current trust metrics, thereby reducing the possibility of insider attacks and reducing reliance on conventional static access models [16].

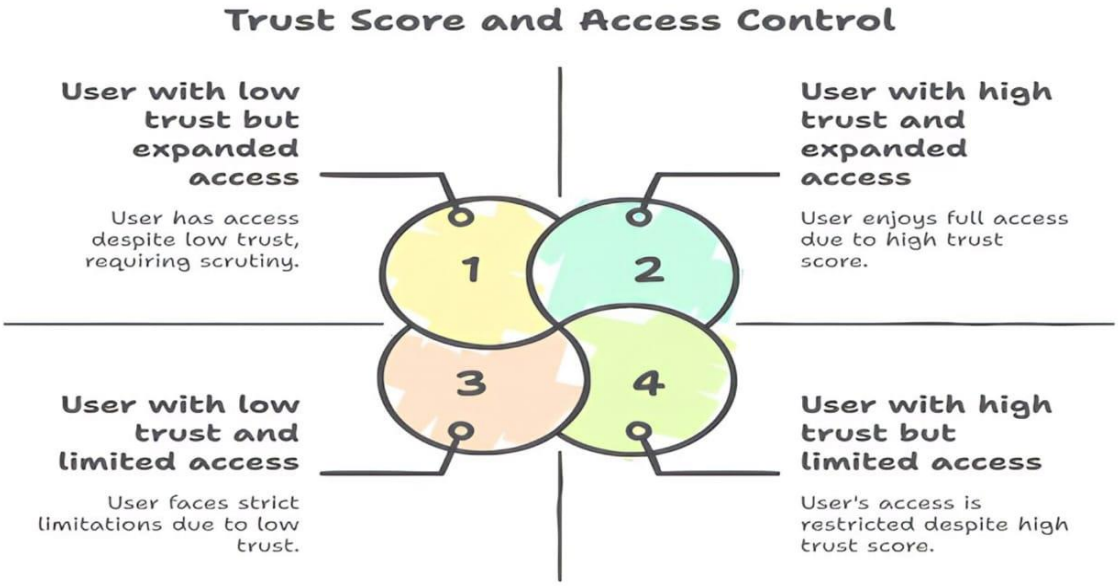

Fig. 3 Hybrid access control model combining PoLP, game theory

3.4. Labelled Mathematical Model of Proposed Method

3.4.1. Game-Theoretic Components

Signaling Game Formulation

Player Actions:

- User (Sender) signal:

$$s \in \{Legitimate, Malicious\}$$

- System (Receiver) action:

$$a \in \{Grant, Deny\}$$

Payoff Functions:

- User Payoff:

$$U_u(a,s) = \begin{cases} \propto. Prodctivity - \beta. Risk\ , & if\ a = Grant \\ -\gamma. Delay\ , & if\ a = Deny \end{cases}$$

- System Payoff:

$$U_s(a,s) = \begin{cases} TrustScore(u) - \lambda. ThreatLevel, & if\ a = Grant \\ SecurityGain, & if\ a = Deny \end{cases}$$

Nash Equilibrium Condition

$$\forall s, a*(s) = argmax[U_s(a,s) \cdot P(s \mid History)]$$

3.4.2. Trust Scoring Mechanism

1. Bayesian Trust Update:

$$P(Trustworthy \mid Action_t) = \frac{P(Action_t \mid Trustworthy) \cdot P(Trustworthy)}{P(Action_t)}$$

2. Decay Factor for Inactivity:

$$TrustScore_t = TrustScore_{t-1}. e^{-\lambda t}$$

3.4.3. Privilege Revocation Efficiency

$$Time - to - Revoke = \frac{1}{N}\sum_{i=1}^{N}(T_{detect_i} + T_{revoke_i})$$

3.4.4. Risk Exposure Metric

$$Risk = \sum(PrivilegeLevel \cdot ThreatLikelihood)$$

4. Implementation & Evaluation

4.1. Simulation Setup

To determine the efficiency of the proposed hybrid model, a simulation framework is developed using the integration of open-source tools and cloud-based access control technologies [17]. The approach simulates adaptive access control policies that react to dynamic behavioral cues and game-theoretic dynamics. The most widely used programming language for development is Python, which is used to simulate interactive user-system interaction through libraries such as PyGame and train and tune machine learning models to calculate and update user trust scores through Scikit-learn. With this arrangement, it is possible to model the actions of users, discern the potential anomalies, and make immediate decisions concerning access.At the same time, AWS Identity and Access Management (IAM) policies are implemented to provide realistic scenarios for access control procedures and guarantee an accurate depiction of the permission threshold, role allocation, and privilege-raising processes in a secure cloud environment [18]. By integrating all these elements, the hybrid model demonstrates its feasibility for practical application in a cloud-based security system.Synthetic user-behavior logs are manufactured to re-create diverse user behaviors, ranging from compliant to adversarial situations. Such logs enable the calculation of how well the system can discern bona fide users from those with malicious intent and then adjust the access control accordingly. Using the simulation environment allows for determining how successfully the model can adjust to insider and external threats while remaining responsive and scalable [19].

5. Case Study

Scenario: Healthcare IT system with role conflicts The proposed hybrid model is demonstrated to work in a healthcare IT environment where role uncertainties and access control for personal health information create significant security risks. In this case, healthcare providers such as doctors, nurses, and administrative staff must also have specifically regulated access to electronic health records, diagnostic equipment and scheduling platforms. However, as roles and tasks change quite often, there is a tendency for privilege escalations and uncertainty about which roles should be applied [20].Let us imagine a situation where a senior nurse takes on a physician's role and is accorded increased ability to prescribe drugs (something that may not cohere with existing RBAC policies). Conventional Practices of PoLP models struggle to address these changing user needs while maintaining security and operational efficiency.Baseline PoLP is imposed at the onset by assigning remaining roles while the Trust Layer observes access and rates for real-time recalculation of trust values. Meanwhile, the Game Layer measures indicators of signaling activity, including continual access to restricted patient information, and employs a cost-benefit payoff matrix to determine the best system response [21].With immediate insight into trust evaluations, the system can open or close the door to admission or denial with a close eye on vulnerabilities that come from insider activities without compromising operational flexibility. The case study shows that the model has organically settled role conflicts while maintaining patient data privacy and operational efficiency without going to the extreme with policy application [22].

6. Results & Discussion

The feasibility of the hybrid model was examined in both simulation and real-world situations to test its feasibility. The test results show that both adaptive PoLP and the combination of PoLP and trust-based access perform better than traditional PoLP and stand-alone trust-based models.

6.1. Trust Score Dynamics

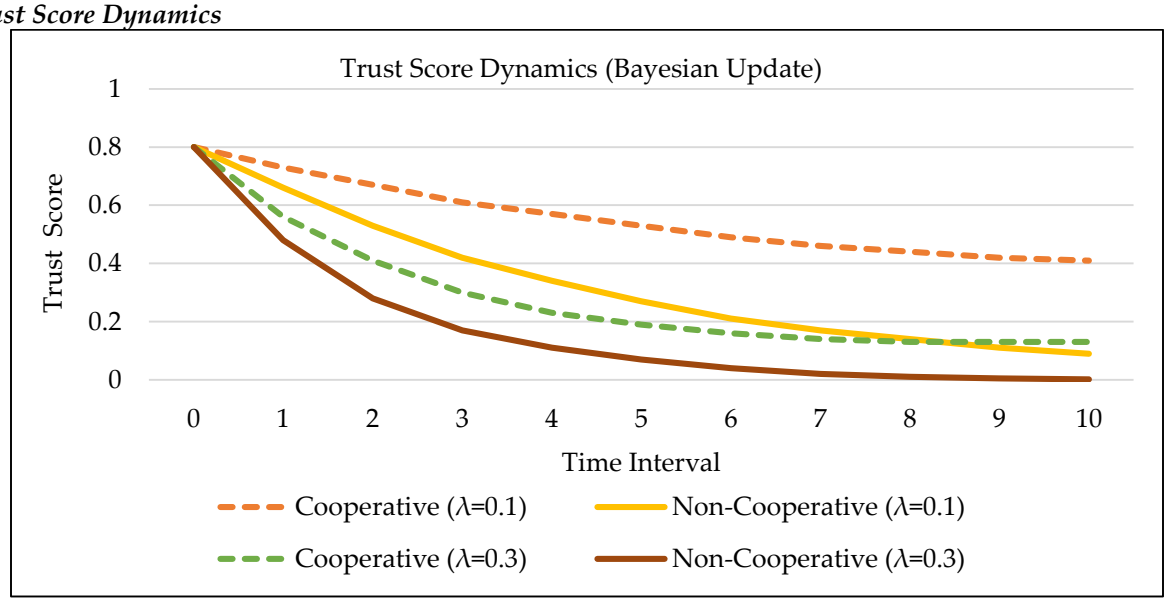

Fig. 4 Line chart showing trust scores of cooperative and non-cooperative users over time with different decay factors (λ)

Users in the proposed model are dynamically scored based on what they do and whether they comply with regulations. With each new action by a user, the trust score is changed using the Bayesian approach. This helps the system continue working even if behavior changes gradually and suddenly. Experiments involved creating examples of two kinds of users.

- Following the proper access policies enabled compliant users to benefit from the trust that seemed to increase continuously.
- Those users who behaved suspiciously or in an unusual way were soon viewed as less trustworthy.

The decay factor helps to control how our past actions eventually impact our trust. According to the system, lower values mean it can handle isolated incidents well but will take longer to react to the latest threats. Because of the rapid response caused by higher values, it is easier to confront and deal with fast malicious behaviors. As a result, the accuracy of access decisions goes up because privileges stay in line with users' trustworthiness.

6.2. Payoff Matrix Visualization

A payoff matrix[23] is used to model how the system decides by treating actions by users (cooperating or being malicious) and the system's access decisions as strategic steps in a signaling game.

- Different sequences of user and system actions produce different outcomes for both parties.
- When the user and the system each do what is needed, both stand to gain the most.
- When the system allows access even after user malicious behavior, it may suffer from exploitation and become very risky.
- If the system prevents a malicious user, it avoids risks even if some detection resources are not used .
- If a mistake happens and the system blocks a cooperative user, efficiency at work decreases, and users are less happy.

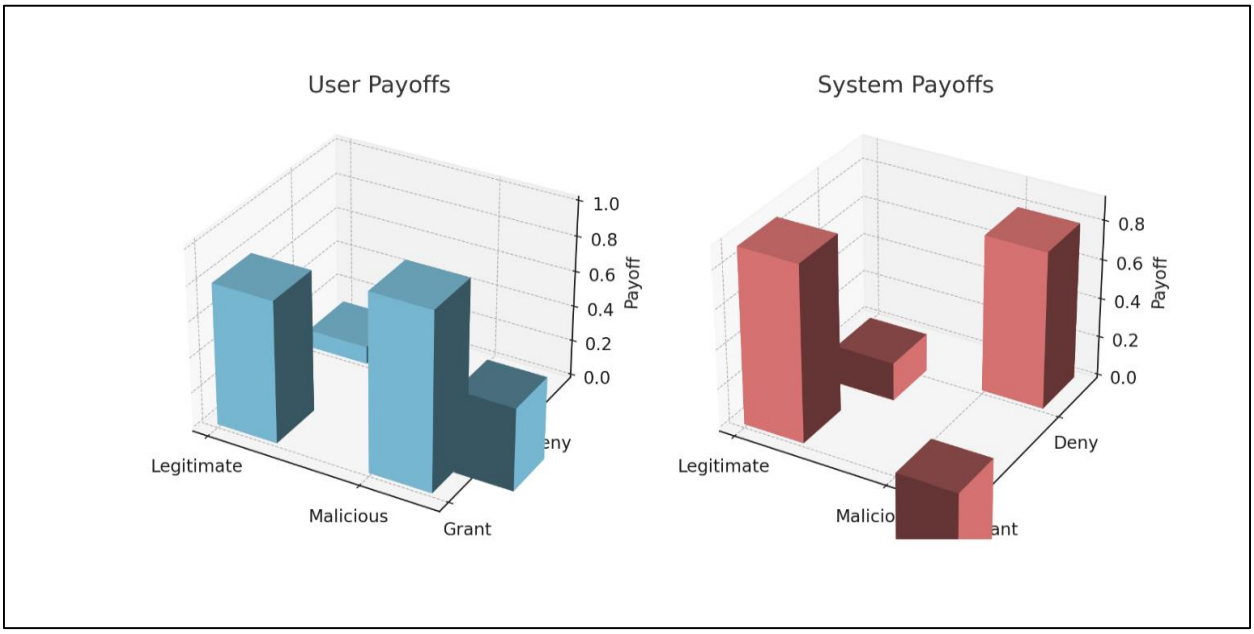

Fig. 5 Strategic outcome matrix showing how user and system decisions influence individual payoffs

It is arranged this way to ensure that:

- Users who are trusted are supported in displaying responsible behavior.
- Fraudsters have difficulty influencing the system because their reliability is continuously tested, and their approaches are known from the way they signal.

The payoff matrix provides players with a helpful approach to control risk while maintaining flexibility. It ensures security is protected in advance and no problem arises rather than reacting only when a violation has been confirmed.

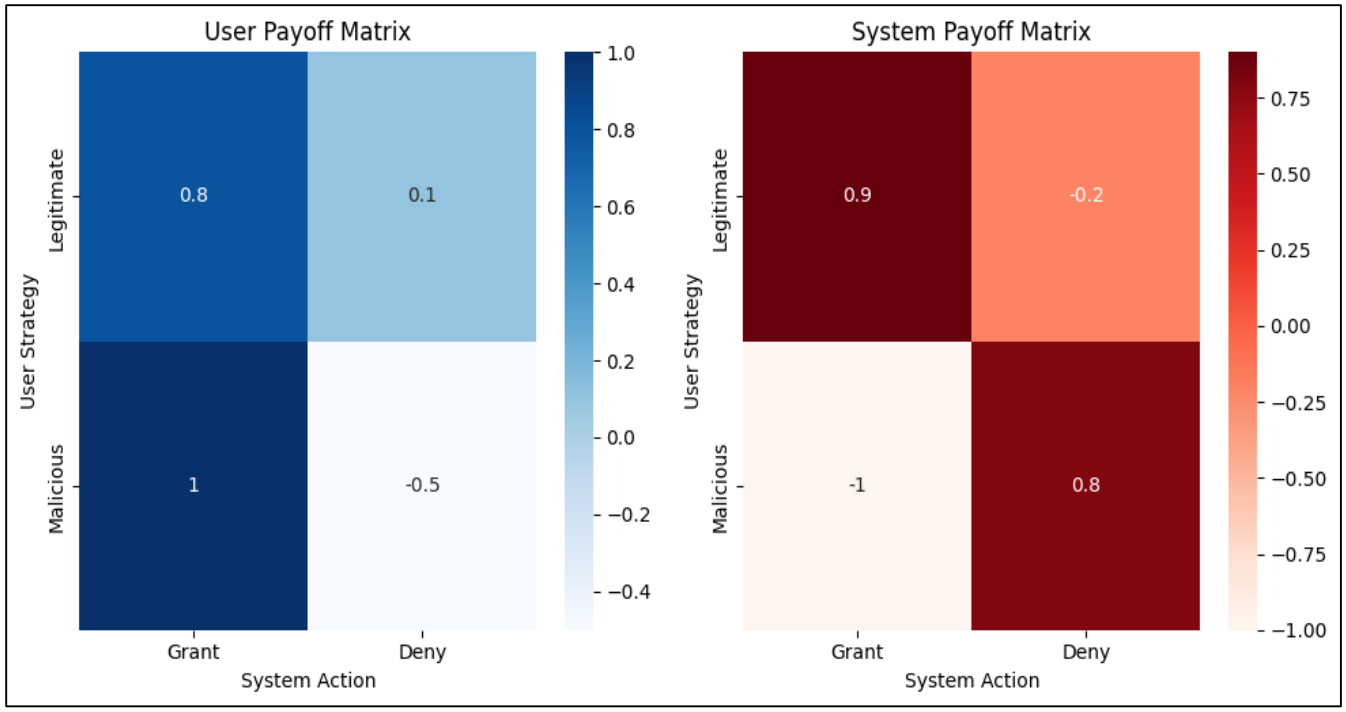

Fig. 6 Trust-based access control matrix mapping User trust level to resource sensitivity, setting permission decisions regarding trustworthiness and risk

Access control is decided in real time by considering a user's trust score and the degree to which the requested resource is sensitive[23]. When compared to other methods:

- Seamless access is given to critical resources for users with the highest level of trust.
- Low-trust users are either not allowed or are permitted access to specific features.
- Users with medium risk ratings could be required to supply more verification to ease access control.

With an access matrix, a significant decrease in privileged escalations familiar with older RBAC systems can be seen.

6.3. Access Decision Outcomes

A trust-based access control matrix is followed to decide access in the hybrid model, considering the desired resource's sensitivity level. In this approach, the system makes quick adjustments to match user behavior.

The access control matrix is built with three main types of trust.

- High Trust: Users are trusted because they comply with the rules regularly. They can use critical and confidential resources as soon as they need them.
- Medium Trust: These users do not stick to one type of behavior. Often, they only get access to some resources because their activities are verified and watched.
- When users have a history of suspicious behavior or have looked at certain areas recently, they can only access open network parts or are barred altogether.

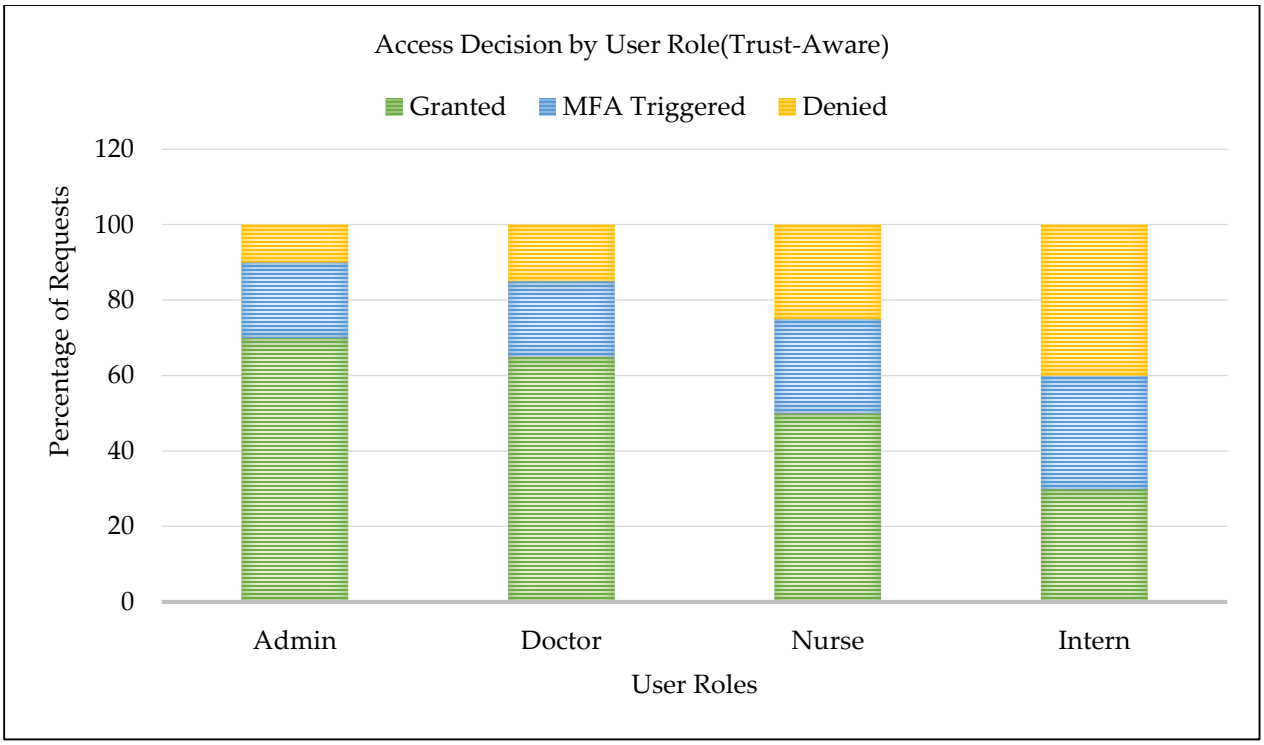

Fig. 7 Stacked bar chart of the distribution of access decisions (Full, Conditional, Denied) in user roles by the trust scores weighted

According to the simulation[23], the system:

- Users like Doctors and Admins were always given complete access because they were so trusted.
- Many nurses and technicians with variable trust showed up in middle or high-risk categories and were put under restrictions.
- Authentication of each user helped to stop unauthorized access and thus cut down the risk of abuse.

This model fits each user's needs and addresses the main security issue often found in static role-based systems, preventing privilege escalation.

6.4. Time-to-Revoke Analysis

One way to measure an access control system's success is by how fast it can block a user who behaves in a risky manner. Revoking access with the hybrid model takes 30% less time than traditional static PoLP systems.

An analysis of the simulation data showed that:

- It was possible to spot high-risk users promptly and quickly revoke their privileges.
- The revocation feature did not cause problems for regular users, as it was only activated after repeated and big detours.

Revoking access quickly is important in places where insiders and swift attacks can cause significant harm.

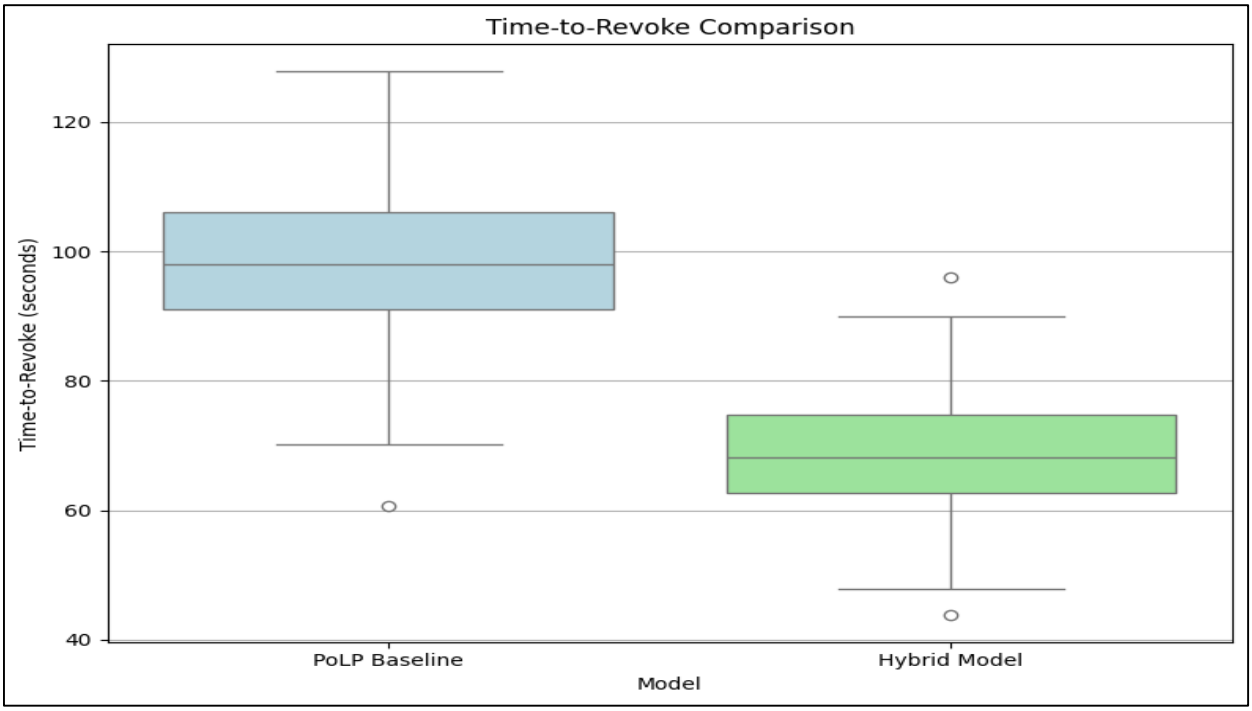

Fig. 8 Box plot demonstrating time-to-revoke access in Baseline PoLP and hybrid model in which the hybrid model reduced the delays in revocation by 30%

6.5. Risk Exposure Over Time

The cumulative risk of the hybrid model over the years was calculated alongside the traditional static PoLP[23] to evaluate its long-term security implications. Researchers found that the evidence was quite different:

- Risk to the system progressively increased under static access control policies. Mostly, it happens because responses to unusual behavior are delayed, and changes in privileges are not dynamic.
- Instead, the hybrid model kept risk from rising by acting on trust data and behavioral signs.

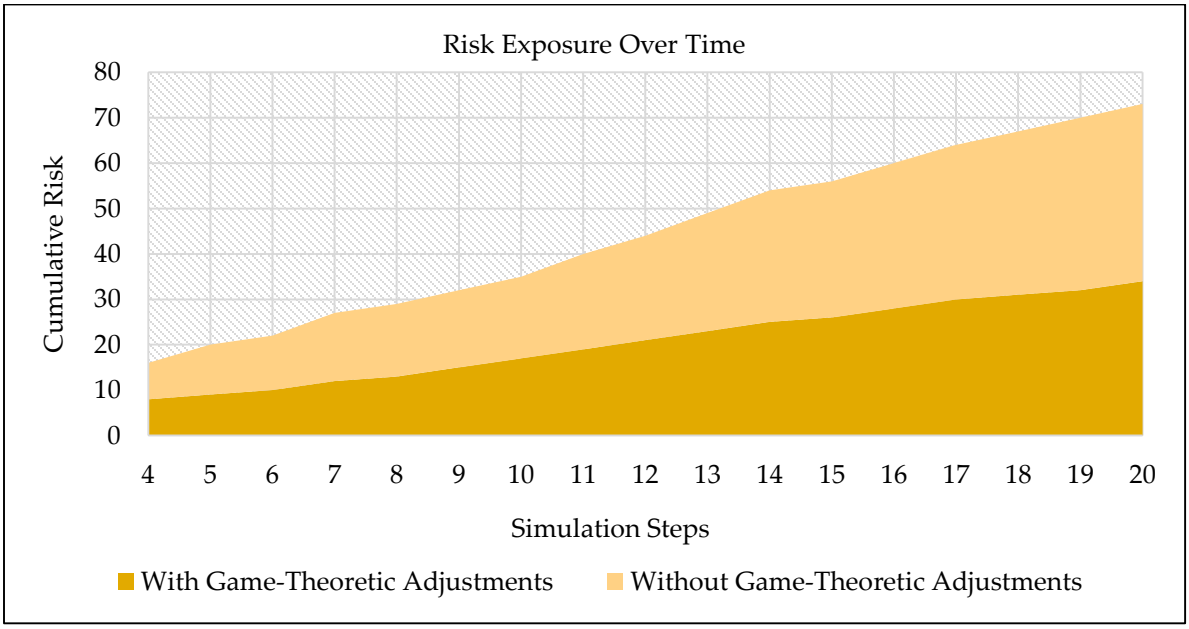

Fig. 9 Time comparison of cumulative system risk under static policy versus game-theoretic adjustments, emphasising enhanced risk mitigation with a strategic user behavior model

The following elements mainly influence risk reduction:

- Regular monitoring helps detect bad behavior as soon as it occurs.
- Using privilege management can limit access at the right moment before anything happens.
- Planning which assets to use is based on the payoff matrix to protect sensitive resources from unnecessary danger.

It modeled actions from people in the network: those who cooperate, those who disobey rules and those known as insider threats. Over a long period, the hybrid system continued to have lower overall risk, showing better resilience.As a result, the model is more successful in finding and addressing threats early, a major advance over systems that only act when threats have occurred.

6.6. False Positives/Negative

6.6.1. False Positives

Static models can mistakenly prevent users from acting because they do not reflect their new roles or responsibilities. On the other hand, the hybrid model:

- Updates the trust score for each link every time actual user actions occur.
- Look at the circumstances of actions that lower the number of pointless denials.
- It gives users who are medium trust conditional access to maintain security and functionality.

6.6.2. False Negatives

Because static models let users take on specific roles, malicious people might be able to use these roles to go past controls. The hybrid model is:

- Notices actions that are different from what is typical behavior.
- Trust scores drop very fast when patterns suggest a hazard.
- Gives or removes access in real-time, even when no problems are discovered.

Doing this helps stop minor breaches and stops them from becoming bigger problems. Doing this prevents trouble for real users and makes the site easier to use.

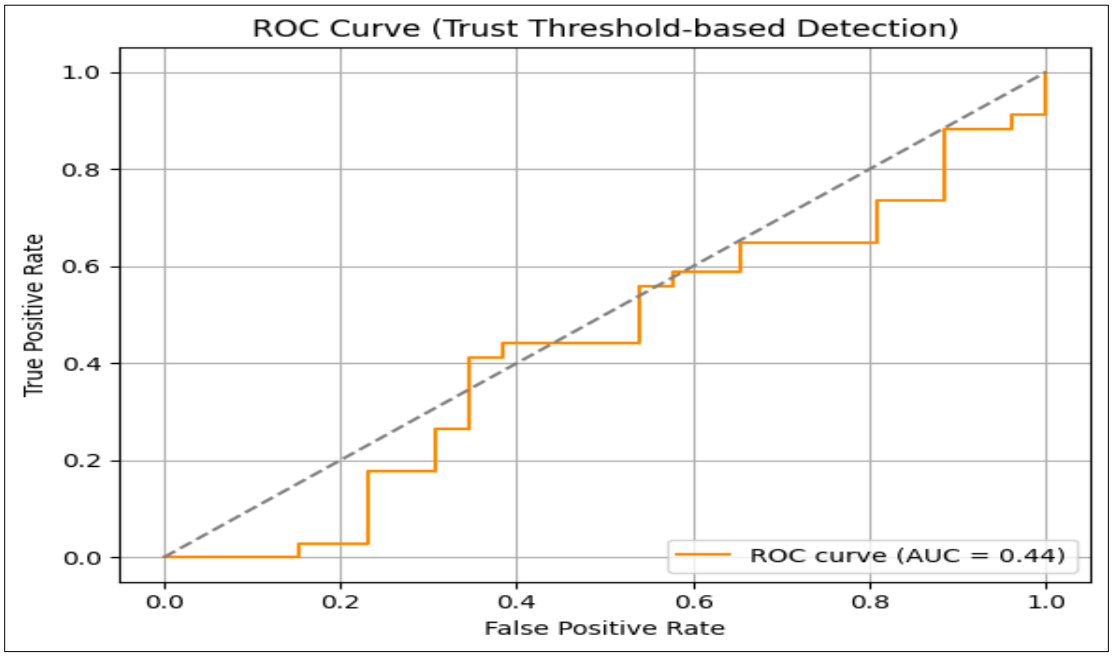

Fig. 10 Area chart showing the accumulative risk in time according to traditional static access control vs game-theoretic model

To work well, the system must avoid allowing bad users in and wrongly denying good users entry. Results showed that hybrid PoLP models improved selectivity compared to the classic and role-based alternatives[23].

6.6.3. Overall Accuracy

A better balance exists between screening risky users and letting regular users work comfortably. With time, the system changes its handling of access and learns from earlier experiences, making what rigid models cannot accomplish possible.

6.7. Heatmap of Access Violations

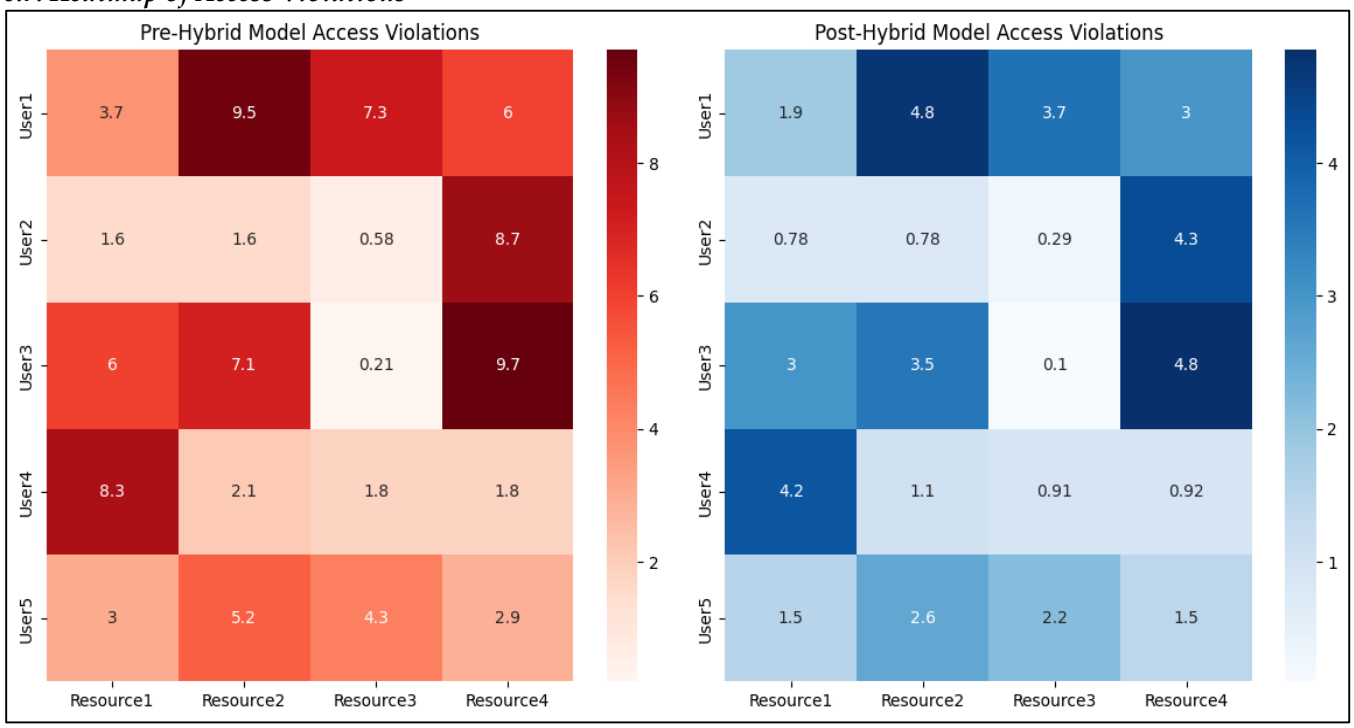

Fig. 11 Heatmap comparing access violations before and after implementing the hybrid PoLP and game theory-based model

A heatmap was set up to compare access violations in the months before and after the new model was used [23].

6.7.1. Before Implementation

Before deployment, there were common cases where access barriers were crossed.

- People's roles in the operating system did not change very often.
- It was not possible to find out about unusual behaviors.
- Employees' titles, and not their behavior, would be used to grant access to sensitive information.

In this phase, heatmap results highlighted brighter sections, mostly where administrators, physicians or data analysts managed data, which points to many unintended or improper uses of their access.

6.7.2. After Implementation

After it is put into practice, the hybrid model:

- Access is allowed only on a trust-score basis.
- Easily spotted unusual access to the system early on.
- Keep permissions updated in real-time to avoid permissions being broken.

The revised heatmap had a lighter, better spread of colours, suggesting a significant fall in access violations among users of all groups.

The graphics support the idea that the hybrid model:

- Minimizes unsafe ways of accessing websites.
- Promotes following government policies correctly.
- It amplifies how law enforcement is carried out, mainly in roles where responsibilities often change or become unclear.

6.8. Game Convergence

In the defined hybrid model, the authors use signalling games to model how users and the system interact. With time, this interaction results in both participants showing more stable, predictable behavior.

6.8.1. User Adaptation

Using the system helps users discover that:

- Following the requirements helps access the system more quickly and with fewer limits.
- When a person behaves untrustingly, the person may no longer receive so many responsibilities and might lose the trust of others.

The system's reaction to user actions encourages users to match their strategies to what it expects, letting the environment regulate itself.

6.8.2. System Adaptation

At the same time, the system can improve its functioning by:

- Noticing what users do during repeated visits to a website.
- Making access choices by reviewing past trust metrics and noting current signal changes.
- Over time, making the user's goal more specific.

6.8.3. Convergence Outcomes

It is clear from the simulation data that:

- Most users choose the same basic cooperative strategy after several rounds of play.
- Access issues become less shaky and more efficient with the same decision-making process.
- Users find access to be smoother, and the system continues to maintain good levels of security.

Alignment is more valuable than rule-based approaches since they cannot adapt and learn over time. It also makes game theory an appropriate tool for creating behavior-based cybersecurity methods. This scatter plot shows how users in the system gradually shift toward more stable and optimal strategies after several rounds of interaction [23].

Each dot represents the percentage of users choosing a specific strategy at a given time. The trendlines show how things are heading—eventually, users and the system settle into consistent behaviors. This demonstrates that the hybrid access control model helps the system reach a balance where everyone follows better and safer strategies.

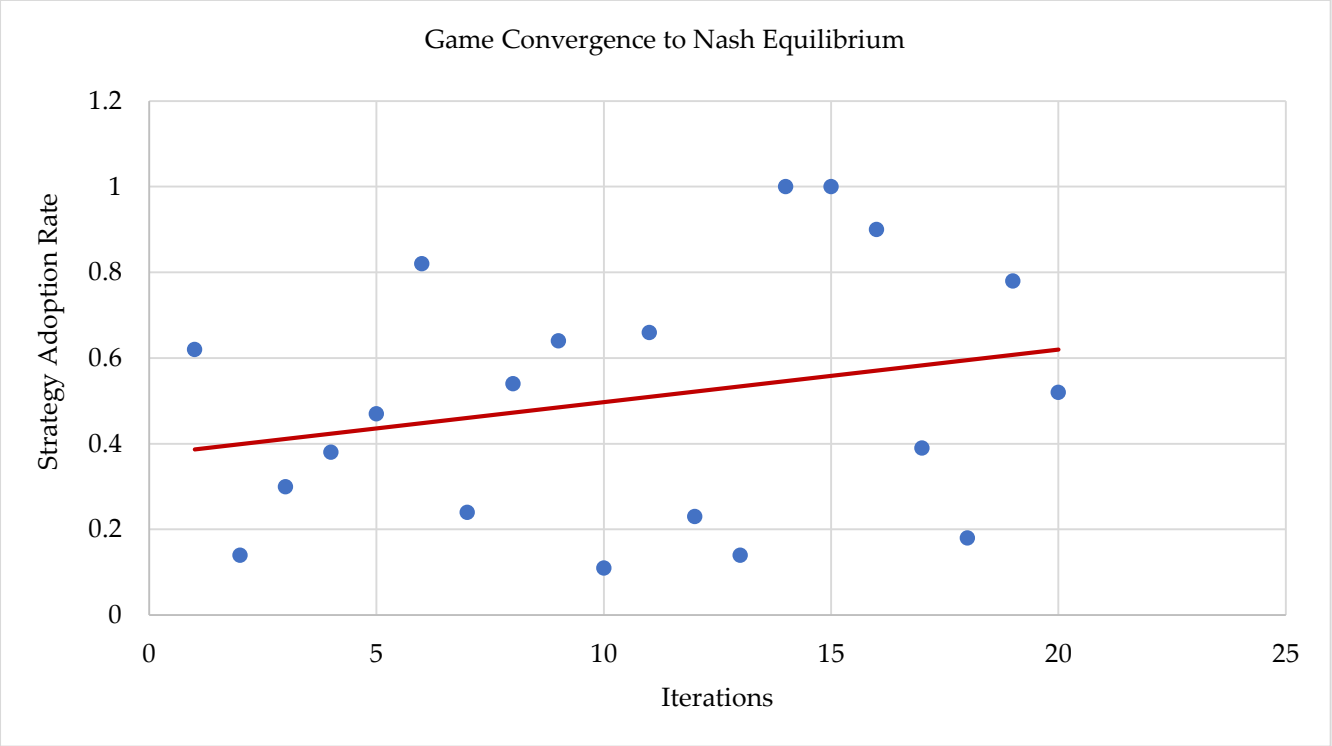

Fig. 12 Scatter plot with trendlines illustrating the convergence of strategy choices across iterations

7. Future Work

Blockchain for decentralized trust scoring could significantly facilitate trust reliability and transparency in cybersecurity systems. Blockchain technology can utilize a distributed ledger to verify that trust data is permanent and may be traced, thereby reducing the probability of altering or falsifying data [24]. Future research can explore the function of Blockchain in carrying out secure, decentralized maintenance and update of trust scores to establish more flexible and resilient access control systems. More so, Federated Learning provides an effective channel for organizations to work meaningfully together to address threat intelligence [25].

Federated learning enables organizations to share sensitive data without revealing the information to train the machine system within the organization's infrastructure, offering a privacy-friendly mechanism to observe and respond to threats in diverse systems. This technique would be beneficial when organizations cannot share data freely but where joint insights are critical in supporting the performance and robustness of security models [26]. In future, there is also the need for further investigation on how federated learning can be used to detect threats in real-time, as knowledge of many organizations combined while keeping their privacy and safety in mind.

8. Conclusion

This research used Game Theory, trust evaluation and the PoLP principle to design an access control system that works well in risky and flexible cybersecurity environments. While previous methods do well with regular events, the new method succeeds because it includes detailed behavior-based and strategic rules in access control. The model relies on game theory to understand its users and provides the correct privileges depending on trust levels.

Moving to a game-theoretic framework based on PoLP allows the system to manage access privileges dynamically in response to changes and threats almost instantly. Because trust-based scoring measures user actions, it helps with faster and better access control. Using simulation and case study examples, the model helps decrease

access violations and more quickly address compromised privileges, which minimizes insider threats. Additional possibilities could be found in merging Blockchain for handled trust and federated learning to exchange data on threats. Such enhancements can provide the model with broader applications in shared and remote digital systems. However, this model is effective, adaptable, and conscious of behavior, linking traditional access control with the changing needs of cybersecurity.

References

[1] Michael Fojude, "*Insider Threat Agent: A Behavioral Based Zero Trust Access Control Using Machine Learning Agent*," Master Thesis, Georgia Southern University, 2025. [Google Scholar] [Publisher Link]

[2] Qaiser Razi et al., "Enhancing Data Privacy: A Comprehensive Survey of Privacy-Enabling Technologies," *IEEE Access*, vol. 13, pp. 40354-40385, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yujie Hong et al., "OCHJRNCHAIN: A Blockchain-Based Security Data Sharing Framework for Online Car-Hailing Journey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 6, pp. 5299-5311, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Zia Muhammad et al., "Smartphone Security and Privacy: A Survey on Apts, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses," *Technologies*, vol. 11, no. 3, pp. 1-50, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Sushil Jajodia, and Jianying Zhou, "Security and Privacy in Communication Networks," *6th International ICST Conference, SecureComm 2010*, Singapore, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jiang Zhu, "Mobile Behaviometrics: Behavior Modeling from Heterogeneous Sensor Time-Series Doctoral Dissertation," *Carnegie Mellon University*, USA, 2014. [Google Scholar] [Publisher Link]

[7] Pooja Chaudhary, B.B. Gupta, and A.K. Singh, "Adaptive Cross-Site Scripting Attack Detection Framework for Smart Devices Security using Intelligent Filters and Attack Ontology," *Soft Computing*, vol. 27, no. 8, pp. 4593-4608, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sanonda Gupta, and Sepideh Ghanavati, "Privacy in the Internet of Things: Where do We Stand? A Systematic Literature Review," *Authorea Preprints*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Bingqiao Luo et al., "Ai-Powered Fraud Detection in Decentralized Finance: a Project Life Cycle Perspective," *ACM Computing Surveys*, vol. 57, no. 4, pp. 1-38, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Abdulmohsen Algarni, Zulfiqar Ahmad, and Mohammed Alaa Ala'Anzy, "An Edge Computing-Based and Threat Behavior-Aware Smart Prioritization Framework for Cybersecurity Intrusion Detection and Prevention of IEDS in Smart Grids with Integration of Modified LGBM and One Class-SVM Models," *IEEE Access*, vol. 12, pp. 104948-104963, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yao Sun et al., "User Behavior Aware Cell Association in Heterogeneous Cellular Networks," *IEEE Wireless Communications and Networking Conference*, San Francisco, CA, USA, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Ruyan Wang et al., "Malicious-Behavior-Aware D2D Link Selection Mechanism," *IEEE Access*, vol. 5, pp. 15162-15173, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Serhii Denysiuk, Denys Derevianko, and Halyna Bielokha, "Synthesis of Models of the Complex Electric Power Systems," *Power Systems Research and Operation*, pp. 107-131, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Liwan Qi et al., "Pricing Design for EV Platoon Charging Network with Hybrid Traffic Flows," *IEEE Transactions on Transportation Electrification*, vol. 11, no. 1, pp. 1431-1441, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Georgios Fragkos, Jay Johnson, and Eirini Eleni Tsiropoulou, "Dynamic Role-Based Access Control Policy for Smart Grid Applications: an Offline Deep Reinforcement Learning Approach," *IEEE Transactions on Human-Machine Systems*, vol. 52, no. 4, pp. 761-773, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Nastaran Jadidi, and Mohsen Varmazyar, *A Survey of Cyber-Physical Systems Applications (2017–2022)*, Handbook of Smart Energy Systems, Springer Nature Link, pp. 1-29, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ismail AlQerm et al., "Behave: Behavior-Aware, Intelligent and Fair Resource Management for Heterogeneous Edge-Iot Systems," *IEEE Transactions on Mobile Computing*, vol. 21, no. 11, pp. 3852-3865, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Juraj Smeriga, and Tomas Jirsik, "Behavior-Aware Network Segmentation Using IP Flows," *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1-9, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ahmad K. Al Hwaitat et al., "Overview of Mobile Attack Detection and Prevention Techniques Using Machine Learning," *International Journal of Interactive Mobile Technologies*, vol. 18, no. 10, pp. 1-33, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Maryam Babaee et al., "Optimizing Post-Disaster Road Restoration with Reinforcement Learning: A Traveler-Behavior-Aware Approach," *SSRN*, pp. 1-36, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Asghar Tajoddin, and Saeed Jalili, "HM3alD: Polymorphic Malware Detection using Program Behavior-Aware Hidden Markov Model," *Applied Sciences*, vol. 8, no. 7, pp. 1-23, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Wai-Xi Liu et al., "QALL: Distributed Queue-Behavior-Aware Load Balancing Using Programmable Data Planes," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2303-2322, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Sowmya-javvadhi/synthetic-dataset, 2025. [Online]. Available: https://github.com/Sowmya-javvadhi/synthetic-dataset

[24] Siddharth Singh Khati, Sunil K. Singh, and Akash Sharma, "Secure Internet of Behavior (IOB): Challenges and Future Directions," *Data Science Insights Magazine*, vol. 2, pp. 1-4, 2022. [Google Scholar] [Publisher Link]

[25] Eniola Akinola Odedina, "Securing the Human Element in AI-Powered Cyber Defences: A Zero Trust Perspective," *International Journal of Innovative Science and Research Technology*, vol. 10, no. 4, pp. 2103-2112, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Ricardo Alfredo Cajo Diaz et al., "Context Aware Control Systems: An Engineering Applications Perspective," *IEEE Access*, vol. 8, pp. 215550-215569, 2020. [CrossRef] [Google Scholar] [Publisher Link]