A Social Identity-Based Attendance System for Counter-Surveillance

Karissa B. Khonglam
2020CS50428
IIT Delhi

Himadri Rajora
2021CS10117
IIT Delhi

ABSTRACT

In recent years, biometric systems for attendance tracking have raised privacy concerns due to the potential for misuse and surveillance. This project proposes an alternative system based on social identity verification, where individuals vouch for each other's presence. The goal is to create a robust, privacy-preserving attendance system that discourages false reporting while ensuring accuracy through peer confirmation. We introduce a model where attendance is marked if at least k people vouch for a person's presence, combined with a random roll-call mechanism to prevent cheating. This system is simulated to identify optimal values of k and m (number of individuals for roll-call) for various class sizes.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; Authentication; • **Networks** → *Network reliability*.

KEYWORDS

Social identity systems, privacy, peer networks, biometric alternatives, counter-surveillance, collusion detection

1 INTRODUCTION

Biometric systems such as fingerprint scanning and facial recognition have been widely adopted for attendance tracking, especially in institutions and workplaces. While these systems offer high accuracy and convenience, they introduce significant privacy concerns. Centralized databases containing sensitive biometric data can be vulnerable to misuse, leading to surveillance concerns, identity theft, and data breaches [7]. Once compromised, biometric data cannot be replaced, unlike passwords or tokens, which can be reset.

In response to these privacy issues, there has been increasing interest in privacy-preserving alternatives. This project introduces a social identity-based attendance system as an innovative solution that leverages peer verification. Instead of relying on centralized biometric data, individuals in a group vouch for each other's presence. This method mimics real-world social interactions, where people naturally confirm each other's identity and presence through social trust networks. Social identity verification is a form of distributed trust where peers confirm attendance, reducing the need for invasive data collection [1]. This approach can also mitigate some ethical issues raised by biometric systems, as it avoids direct collection of personally identifiable information.

However, a key challenge lies in ensuring the system's robustness and discouraging false reporting. If individuals collude or provide false confirmations, the integrity of the system is compromised. To combat this, the system incorporates a randomized roll-call mechanism where a supervisor randomly selects a subset of individuals to verify their presence. Those who are found absent, but were falsely vouched for, will face penalties. By integrating this deterrent, the system discourages collusion and strengthens the overall reliability of attendance verification.

Research Question: Can a social identity system, where peers confirm attendance instead of relying on biometric data, effectively track attendance in a way that ensures privacy and discourages false reporting? What values of k (number of confirmations) and m (number of individuals for roll-call) optimize the system's reliability?

2 UNDERLYING ETHICS

The ethical foundation of the proposed social identity-based attendance system aligns with the principles outlined in Friedman and Kahn's framework [3] for embedding ethics in technology, particularly focusing on human agency and responsible computing.

First, the project seeks to protect human moral agency by moving away from biometric systems that centralize responsibility in computational systems. Traditional biometric methods often encourage reliance on technology while diminishing users' direct accountability. In contrast, the proposed system ensures that attendance is confirmed through peer verification, emphasizing individual and collective responsibility. By involving peers in confirming each other's presence, the system fosters a sense of accountability and shared moral agency among its users.

Second, the design adheres to the principle of non anthropomorphic technology by avoiding systems that replicate human decision-making or grant machines undue influence. Biometric systems, while efficient, often blur the boundaries between human judgment and machine operations, creating a "moral buffer" where users may abdicate responsibility for errors or misuse. The social identity system, however, treats technology as an assistant rather than a decision-maker, merely facilitating the process of peer confirmation and auditing.

Moreover, the project resists making technology invisible, another key tenet from Friedman and Kahn's work. By implementing transparent processes like peer verification and randomized roll-call audits, the system sharpens the distinction between human actions and technological facilitation. Users remain actively engaged in the verification process, ensuring a clearer understanding of the system's functioning and their roles within it.

Lastly, the project refrains from delegating critical decisions entirely to technology. The inclusion of randomized roll-calls as a deterrence mechanism ensures that human supervisors retain oversight, intervening directly when necessary. This prevents the system from becoming fully automated and detached from ethical considerations, ensuring it remains grounded in participatory and human-centric values. We exemplify an ethical design approach by fostering human accountability, maintaining transparency, and

avoiding over-reliance on technology, all while addressing privacy concerns inherent in traditional biometric systems.

Building on the ethical foundations already described, the proposed social identity-based attendance system further emphasizes privacy, autonomy, and inclusivity, aligning with ethical principles discussed in the paper "Ethical Issues in Biometrics" [5].

2.1 Privacy

Biometric systems are criticized for compromising information privacy and physical privacy due to the collection and storage of sensitive, irreplaceable data like fingerprints and facial scans. Such systems are vulnerable to misuse, identity theft, and irreversible harm if breached. By replacing biometrics with a social identity verification approach, the proposed system avoids collecting sensitive biometric data entirely, ensuring that personal information is not at risk of theft or exploitation. This reflects a commitment to minimizing privacy risks and protecting individuals from unintended surveillance.

2.2 Autonomy

The proposed system upholds the principle of informed consent, a core element of autonomy. In contrast to biometric systems that often collect data covertly or mandate participation, the peer-based system is inherently participatory. It requires active engagement from individuals to confirm attendance, fostering a sense of control and responsibility. Users are fully aware of the process and retain agency in verifying or contesting their presence, as opposed to surrendering decision-making to an opaque algorithm or centralized database.

2.3 Social Inclusion

Biometric systems risk social exclusion, especially for individuals unable to register or whose biometric data fails to meet technical standards, such as people with disabilities or those with unique physiological traits. The social identity-based system eliminates this risk by focusing on peer verification, which relies on social trust rather than physiological conformity. This inclusivity ensures that no one is unfairly excluded due to system limitations, addressing the ethical concerns of justice and fairness.

2.4 Functional Transparency and Governance

Unlike biometric systems susceptible to function creep (unintended secondary uses of data), the proposed system operates transparently. Data collected in the system is limited to attendance logs and lacks the potential for secondary exploitation, such as medical profiling or behavioral monitoring. Randomized roll-calls introduce an oversight mechanism, ensuring that the system operates within its ethical boundaries and addressing concerns about misuse or overreach.

Therefore, the proposed system not only addresses the technical shortcomings of biometrics but also adheres to ethical principles by prioritizing privacy, autonomy, and inclusivity, while maintaining transparency and minimizing potential harm. This approach ensures that technology serves human values rather than compromising them.

3 METHODOLOGY

3.1 Initial Setup

The key idea is to require at least k confirmations from peers for each individual, ensuring accountability while reducing reliance on invasive technologies. To prevent potential abuse, such as false confirmations arising from collusion, the system incorporates a supervisor-based random audit mechanism. This mechanism selects m individuals at random to verify their attendance and penalizes any group found guilty of false confirmations. By drawing inspiration from the Maze system [8], the solution borrows methodologies for analyzing behaviors indicative of collusion, such as temporal patterns, mutual voting density, and abnormal peer behavior.

The system design includes three major components. First, the peer-confirmation process ensures that students mark their own attendance while requiring k peer validations. Additionally, peers who provide confirmations must also be verified by others, creating a network of mutual accountability. Second, random audits involve supervisors verifying the attendance of m randomly chosen individuals, acting as a deterrent to collusive behavior. Third, a penalty structure discourages false confirmations by penalizing those who collude or falsely vouch for others. Together, these components establish a robust framework for decentralized, privacy-preserving attendance tracking.

The methodology begins with collecting data through attendance logs. These logs document who vouched for whom, including timestamps for each confirmation. Additional data, such as relationships among students (e.g., friends or project groups), can be utilized to identify pre-formed collusion groups. Detection algorithms are then applied to this data, inspired by techniques from the Maze system. The *Repetition Detector* identifies individuals frequently vouched for by the same peers, flagging repetitive patterns indicative of collusion. The *Pair-wise Detector* highlights pairs or groups that exhibit disproportionately high mutual confirmations, signaling potential collusion. The *Traffic Concentration Detector* examines patterns where confirmations concentrate on specific individuals. Finally, the *Spam Account Detector* extends this logic to detect groups that rely heavily on internal validation while minimizing external verification.

The system is evaluated through simulations, where parameters k (number of peer confirmations) and m (number of random audits) are varied across different group sizes n. These simulations analyze the outcomes, including the detection rate of collusion and the occurrence of false positives. Different collusion behaviors, such as tight-knit groups and random patterns, are modeled to study how effectively the system adapts to various scenarios. The results help fine-tune the system's parameters for optimal performance.

The mechanism or algorithm in the proposed peer-confirmation-based attendance system is designed to simulate and evaluate the effectiveness of detecting collusion while maintaining fairness. The approach incorporates simulation of attendance logs, collusion detection through behavioral analysis, random audits for validation, and performance evaluation using key metrics. Each component contributes to a structured methodology for identifying dishonest behavior and ensuring system integrity.

The detection mechanism relies on three primary components. First, attendance logs are simulated for all students over multiple

days. Each student marks their attendance and selects k peers to confirm their presence. Collusion groups are introduced in the simulation, where members of a group mutually confirm each other's attendance disproportionately. This creates patterns indicative of collusion, which the system aims to detect. Second, collusion detection analyzes these logs to flag students exhibiting repetitive and predictable peer confirmation patterns. Such patterns are characteristic of colluding groups that repeatedly rely on a fixed set of peers for validation. Third, random audits validate attendance claims by selecting m students at random for manual verification. During these audits, false attendance is simulated, and individuals caught falsifying attendance are flagged. Detection rates, including true detections and false positives, are calculated based on the outcomes of these audits.

The simulation of attendance logs forms the foundation of the detection mechanism. A list of students is divided into colluding and non-colluding groups. For colluding students, confirmations are drawn disproportionately from within their group, creating predictable patterns. For non-colluding students, confirmations are randomly drawn from others in the class, resulting in more diverse and realistic behavior. This setup generates attendance data that mimics real-world scenarios, allowing the system to test its ability to distinguish between honest and colluding behavior.

Collusion detection is central to the algorithm and focuses on identifying suspicious patterns in the attendance logs. Students who frequently receive confirmations from the same set of peers are flagged as suspicious by a *Repetition Detector*. Similarly, the *Traffic Concentration Detector* flags students whose confirmations are concentrated within a small group. Honest students generally exhibit diverse confirmation patterns, whereas colluding students rely heavily on the same peers, making their behavior detectable. This analysis provides the basis for identifying individuals with high suspicion levels, which are used to evaluate the effectiveness of the system.

Random audits complement the detection process by validating attendance claims and penalizing false confirmations. A subset of m students is selected randomly for manual verification. For each audited student, the system checks whether they belong to a collusion group. If they do, the student is flagged as correctly detected. Additionally, honest students who are incorrectly flagged as absent due to simulated false attendance are recorded as false positives. This process ensures that the system introduces uncertainty for colluders, making it harder for them to escape detection.

The detection mechanism is evaluated using two key performance metrics: True Detection Rate (TDR) and False Positive Rate (FPR). The TDR measures the proportion of colluding students successfully identified during audits, reflecting the system's ability to detect actual collusion. The FPR measures the proportion of honest students incorrectly flagged as colluders, indicating the system's fairness. By iterating over different values of k (minimum confirmations) and m (number of audits), the system evaluates its performance across various scenarios. Larger values of k generally increase detection precision by reducing false positives, while larger values of m improve the likelihood of auditing colluders but may increase false positives.

The algorithm incorporates several mechanisms to balance detection accuracy and fairness. Collusion pattern analysis, based on repetition and concentration of confirmations, effectively identifies suspicious behavior. Random sampling for audits introduces a layer of unpredictability, discouraging collusion. Parameter tuning explores the trade-offs between k and m, enabling the system to optimize its performance under different conditions. While the system is based on simulated data, its structured design offers a practical framework for identifying collusion in real-world peer-confirmation systems, making it a robust alternative to traditional biometric methods.

We run the simulation for 50 iterations for values of $n = 50$, $n = 100$, and $n = 200$. Key outputs from the simulation include a dictionary of suspicion levels, where higher values indicate a greater likelihood of collusion. Audited students are randomly selected for verification, and false positives represent students flagged incorrectly during the audit process. Visualization of these results is achieved through bar charts that display suspicion levels across individuals, providing a clear view of suspicious activity. Additional graphs compare detection rates of colluders against false positives for various k and m values, illustrating the system's performance under different configurations.

The underlying algorithmic principles draw heavily from the Maze system. *Repetition-Based Analysis* identifies suspicious behavior by detecting repetitive confirmations within fixed peer groups. Random audits introduce uncertainty for colluders, making it difficult to avoid detection without penalties. Finally, the system can be modeled as a graph, with nodes representing students and edges representing peer confirmations. Collusion corresponds to densely connected subgraphs, where groups of peers mutually confirm each other excessively.

This peer-confirmation-based attendance system offers a promising alternative to traditional biometric methods. It balances privacy, fairness, and accuracy by leveraging peer accountability, random audits, and advanced detection algorithms. The system's flexibility allows it to adapt to different group sizes and behaviors, making it a robust solution for decentralized attendance tracking.

3.2 Metrics Calculated

The code calculates two key performance metrics: *True Detection Rate (TDR)* and *False Positive Rate (FPR)*. These metrics are essential for evaluating the effectiveness of the attendance verification system in identifying collusion while minimizing errors. Both metrics are calculated through repeated simulations, where various parameter combinations (k and m) are tested to observe their impact on detection accuracy.

The **True Detection Rate (TDR)** measures the proportion of colluding students correctly identified as colluders during the random audits. It evaluates the system's ability to detect actual collusion effectively:

$$\text{TDR} = \frac{\text{Number of Colluding Students Correctly Identified}}{\text{Total Number of Colluding Students}}$$

A student is correctly identified as a colluder if they belong to any collusion group (from `colluding_groups`) and are selected for auditing.

The **False Positive Rate (FPR)** measures the proportion of non-colluding students falsely flagged as colluders during the random audits. It reflects the system's tendency to incorrectly penalize

honest students:

$$\text{FPR} = \frac{\text{Number of Non-Colluding Students Falsely Identified}}{\text{Total Number of Non-Colluding Students}}$$

A student is falsely flagged as a colluder if they are not part of any collusion group (not in `colluding_groups`) but are selected in the audit and marked as absent due to the simulated false attendance rate.

True Detection Rate (TDR): This metric demonstrates the system's effectiveness in capturing students involved in collusion. A higher TDR implies that the system is successfully identifying collusion patterns in the group.

False Positive Rate (FPR): This metric quantifies the rate of incorrect penalization. A lower FPR indicates that the system is less likely to accuse honest students of collusion, enhancing fairness.

Both metrics depend on parameters k (minimum peer confirmations) and m (number of random audits). Larger k values generally make it harder for colluders to avoid detection, potentially increasing TDR. Similarly, larger m values enhance the chances of auditing a colluder but may increase FPR if not carefully balanced.

3.3 Community Detection Analysis

The system is enhanced by incorporating a user graph-based approach, leveraging community detection algorithms to identify tightly-knit colluding groups. By representing peer confirmations as a graph, it becomes possible to detect communities or subgroups of individuals that may exhibit collusive behavior, such as disproportionately vouching for one another. This graph-based approach adds a robust layer of analysis beyond the earlier method, which relied on random graph generation.

The proposed algorithm begins by constructing a directed graph $G = (V, E)$, where nodes (V) represent students and directed edges (E) indicate that one student vouched for another. The edges are weighted to reflect the frequency or strength of vouching across multiple days. This graph representation captures the structure of peer confirmations and enables deeper analysis of relationships within the group.

Community detection is then performed on the graph to partition it into subgroups or communities. Algorithms such as the Louvain Method [4] [6] or the Girvan–Newman Algorithm are particularly suited for this task, as they identify tightly-knit communities with high modularity. Communities with dense internal connections and relatively sparse external connections are flagged as potential colluding groups. These algorithms allow the system to focus on groups that exhibit suspiciously high levels of mutual confirmations. We use the Louvain method [6] implemented in the NetworkX library in Python.

The modularity of a network, represented as a graph $G = (V, E)$, can be described as follows: let G be partitioned into m communities, with l_s representing the number of edges between nodes in the s-th community, and d_s representing the sum of the degrees of the nodes in the s-th community. The network modularity Q is given by:

$$Q = \sum_{s=1}^{m} \left[\frac{l_s}{|E|} - \left(\frac{d_s}{2|E|} \right)^2 \right]$$

High values of Q indicate high l_s values for each community, implying dense internal connections and weak coupling among communities. Equation 1 reveals a possible maximization strategy.

The *Louvain method* (LM) [4] [6] is based on local information and is well-suited for analyzing large weighted networks. The method consists of two steps:

(1) Each node is assigned to a community chosen to maximize the network modularity Q. The gain derived from moving a node i into a community C can be calculated as:

$$\Delta Q = \frac{\Sigma_C + k_i^C}{2m} - \left(\frac{\Sigma_C + k_i}{2m} \right)^2 - \left[\frac{\Sigma_C}{2m} - \left(\frac{\Sigma_{\hat{C}}}{2m} \right)^2 - \frac{k_i}{2m} \right]$$

Here, Σ_C is the sum of the weights of the edges inside C, $\Sigma_{\hat{C}}$ is the sum of the weights of the edges incident to nodes in C, k_i is the sum of the weights of the edges incident to node i, k_i^C is the sum of the weights of the edges from i to nodes in C, and m is the sum of the weights of all edges in the network.

(2) A new network is constructed where the nodes represent the communities previously identified. The process is iterated until a significant improvement in *network modularity* is obtained.

Once communities are detected, the algorithm analyzes their internal structure to identify collusion. Two key criteria are used for detection: internal density and repetition. A high proportion of internal edges compared to external edges suggests collusion, as does frequent mutual confirmation activity within the same group across multiple days. Communities meeting these criteria are flagged as suspicious and prioritized for further investigation.

To verify flagged communities, random audits are conducted. This step involves selecting a sample of individuals within the suspicious communities and validating their attendance records. Colluding groups are penalized based on the results of the audits. This targeted audit strategy increases the likelihood of detecting colluders while reducing the chance of falsely penalizing honest individuals.

The system also includes visualization to enhance interpretability. The peer confirmation graph is visualized, providing a clear understanding of the relationships and community structure within the dataset. This visualization aids in understanding how individuals interact and how collusion patterns emerge.

The graph-based approach offers several advantages. First, it improves robustness by identifying collusion patterns through relationship analysis rather than relying solely on random sampling. Second, it scales effectively to large datasets with thousands of nodes by employing efficient community detection algorithms. Lastly, it enhances interpretability by providing clear insights into the dynamics of collusion through visualization and community analysis.

Overall, this enhanced system provides a more targeted and effective solution for detecting collusion in peer-confirmation-based attendance systems. By combining graph-based analysis, community detection, and focused audits, the system achieves greater accuracy and scalability while maintaining fairness and transparency.

3.4 Dynamic Behavior Analysis

Extending the project to incorporate dynamic behavior modeling allows for a more realistic simulation of attendance systems, where student-peer relationships and group memberships evolve over time. This enhancement makes the system adaptive and capable of capturing changes in collusion patterns as they occur. Dynamic behavior modeling introduces mechanisms such as fluctuating group memberships, temporary alliances, and evolving peer confirmations, making the analysis more reflective of real-world scenarios.

Instead of maintaining static collusion groups, students are given a probability of changing their group membership daily. This creates a dynamic network where peer confirmations vary over time, simulating realistic attendance behaviors. For instance, students might form temporary alliances that shift from day to day, influenced by personal schedules, random absenteeism, or strategic adjustments. These dynamic interactions ensure that the system models a more complex and nuanced attendance pattern.

To simulate more intricate group behaviors, the model incorporates mechanisms for group splitting and merging. Collusion groups may split into smaller subgroups or merge with other groups based on probabilistic rules that determine their evolution over time. This dynamic group restructuring adds another layer of realism, reflecting how groups adapt and reorganize in response to changing conditions. The introduction of these dynamic behaviors not only enriches the dataset but also challenges the detection mechanisms to keep pace with the evolving network.

The detection mechanisms are also enhanced to address these complexities. The peer confirmation graph is updated daily to reflect the dynamic changes in student-peer relationships. Modularity-based community detection algorithms, such as the Louvain method, are applied at each timestep to analyze evolving collusive behaviors. By comparing detected communities across multiple days, the system identifies persistent collusion patterns, distinguishing them from transient or random behaviors.

3.5 Penalty Feedback Mechanism

To enhance the project further, a penalty feedback mechanism can be incorporated to dynamically influence behavior in subsequent simulations by penalizing detected colluding students or groups. This mechanism introduces game-theoretic principles to discourage collusion and incentivize honest behavior by dynamically adjusting penalties and their effects. Initially, dynamic attendance logs are generated for n students over a given period, and community detection algorithms, such as the Louvain method, are used to identify suspicious groups or individuals. After audits, penalties are applied to detected colluders. These penalties may include reducing their weight in the attendance graph, lowering their probability of successful peer confirmations in future iterations, or dynamically modifying their group membership to limit their influence. The penalized behavior is then fed back into the system, influencing group behaviors and attendance probabilities for subsequent simulations.

This mechanism ensures that penalized students have diminished influence in future attendance logs and community detection processes. By integrating dynamic behavior adjustments, colluding groups become less likely to re-form, leading to evolving attendance patterns over iterations. The system's performance is monitored using metrics like the True Detection Rate (TDR) and False Positive Rate (FPR), recalculated for each iteration to reflect the penalties' impact on the effectiveness of collusion detection. This iterative feedback approach fosters an adaptive system that evolves to reduce collusion over time.

4 RESULTS

We run simulations for different values of k and m on $n = 50$, $n = 100$, and $n = 200$. Each simulation is averaged over 50 iterations. The resulting heatmaps of the True Detection Rate (TDR) and False Positive Rate (FPR) are shown from Figure 1 to Figure 6.

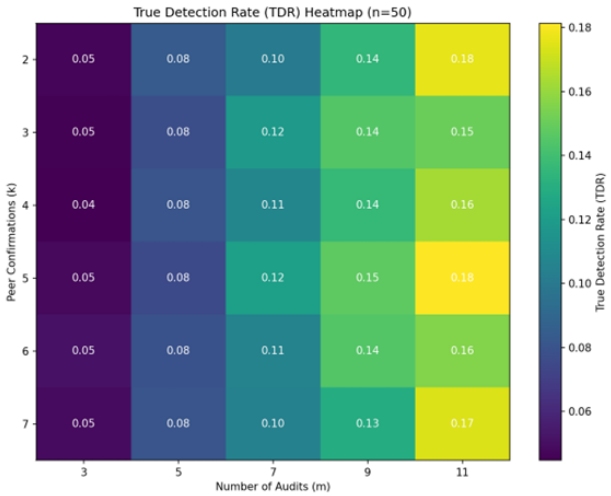

Figure 1: Truth detection rate ($n = 50$) [Random graph simulation]

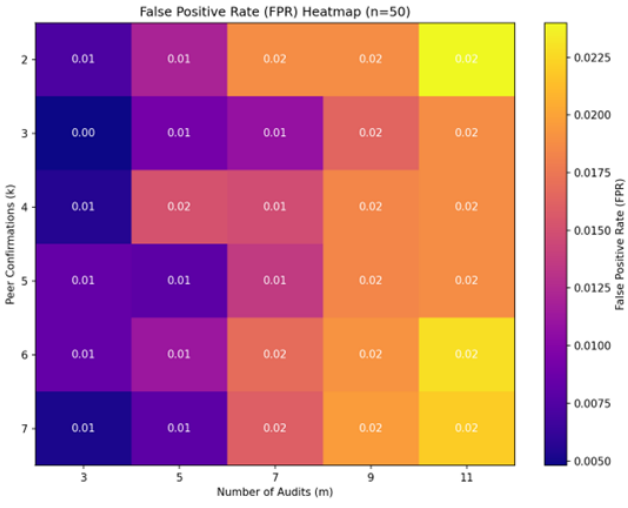

Figure 2: False positive rate ($n = 50$) [Random graph simulation]

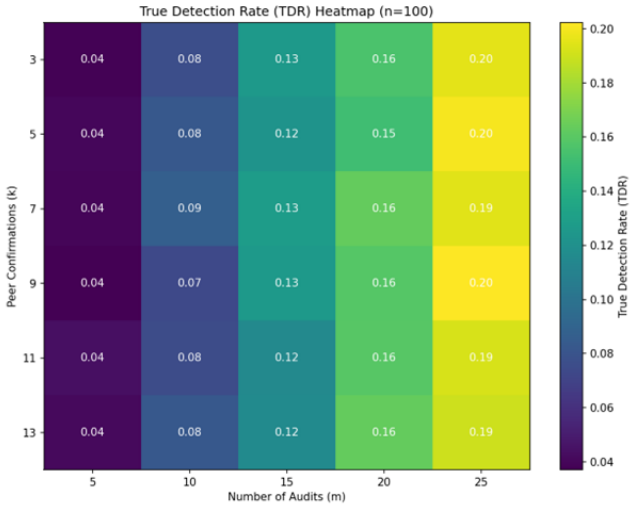

Figure 3: Truth detection rate ($n = 100$) [Random graph simulation]

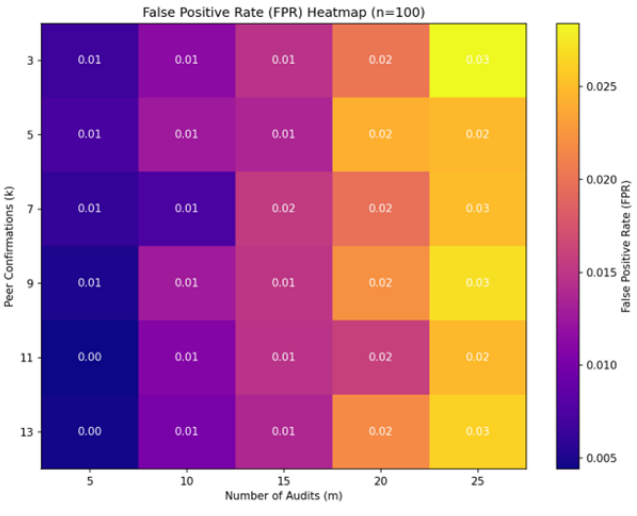

Figure 4: False positive rate ($n = 100$) [Random graph simulation]

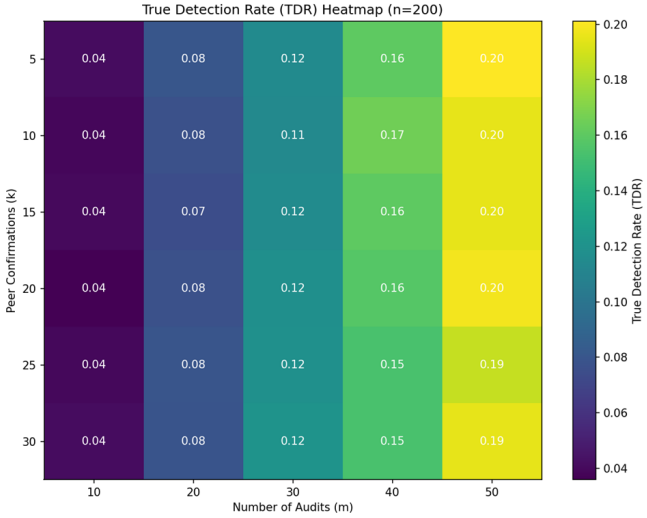

Figure 5: Truth detection rate ($n = 200$) [Random graph simulation]

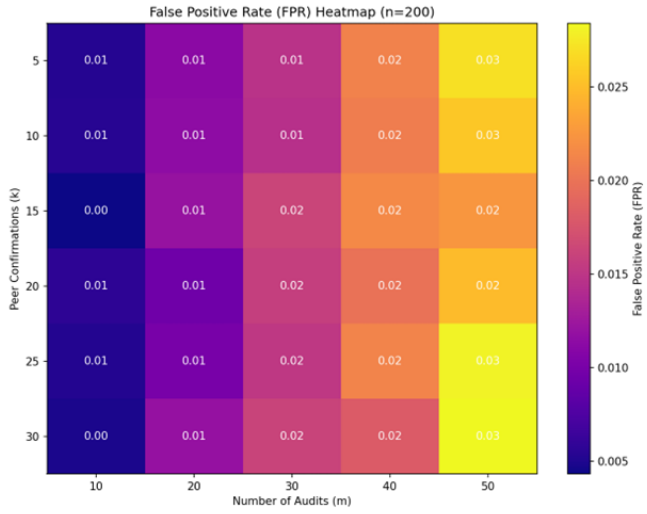

Figure 6: False positive rate ($n = 200$) [Random graph simulation]

Simulation results of the initial setup reveal important insights. The results obtained for $n = 50$, $n = 100$, and $n = 200$, as visualized through the heatmaps of True Detection Rate (TDR) and False Positive Rate (FPR), provide significant insights into the performance and scalability of the peer-confirmation-based attendance system. The findings reveal that the system maintains consistent performance across varying population sizes, demonstrating robustness and scalability.

For the TDR, the values remain remarkably consistent across different population sizes, stabilizing around a maximum value of 0.20 in all cases. This indicates that the algorithm's ability to detect colluders scales well with larger groups. As the number of audits (m) increases, the TDR shows a noticeable improvement. This is expected since more frequent random audits provide greater coverage of the population, increasing the chances of detecting colluders. For instance, at $k = 5$, the TDR improves from approximately 0.08 at $m = 5$ to 0.20 at $m = 25$ or $m = 50$. However, the TDR remains relatively unaffected by changes in the peer confirmation requirement (k), with only minor variations observed. This suggests that increasing k neither significantly enhances nor diminishes the system's ability to detect collusion. The overall results highlight that

the algorithm adapts effectively to larger group sizes without any notable degradation in performance.

The FPR, on the other hand, remains consistently low across all experiments, ranging between 0.00 and 0.03, irrespective of population size. This demonstrates that the system is highly robust in avoiding false accusations against honest students. The FPR values show a slight increase with a higher number of audits (m), which can be attributed to the increased likelihood of random selection errors during audits. However, this increase is minimal, showcasing the system's fairness even as the frequency of audits grows. Similar to the TDR, the FPR is relatively unaffected by changes in k, further emphasizing the stability of the system across varying peer confirmation requirements.

When comparing the results across different population sizes, it becomes evident that both TDR and FPR exhibit minimal variation. This consistency underscores the scalability of the algorithm, as it maintains performance levels irrespective of the group size. Additionally, the results show that the TDR reaches a saturation point for higher values of m, typically around 0.20, indicating that increasing the number of audits beyond a certain threshold yields diminishing returns in terms of detection rates. Similarly, the FPR stabilizes around 0.02–0.03 for larger values of m, reflecting diminishing effects on fairness. These findings emphasize the importance of parameter tuning and penalty structures. Optimal values of k and m depend on the class size and expected collusion rate. Larger classes may require higher m values for effective oversight, while smaller classes can operate effectively with lower thresholds.

In conclusion, the peer-confirmation-based attendance system demonstrates consistent and scalable performance across different population sizes. The system effectively identifies colluders, particularly with higher audit frequencies, while maintaining fairness by minimizing false positives. However, the modest TDR values, which peak at approximately 0.20, highlight the limitations of relying solely on random audits for detection. These findings suggest that additional mechanisms, such as dynamic thresholds for peer confirmations or adaptive auditing strategies, could enhance detection rates without compromising fairness.

After applying the community detection algorithm we observe the results of TDR in Figures 7, 8, and 9. Figure 10 shows that the FPR does not change and remains constant for all values of k, m, and n.

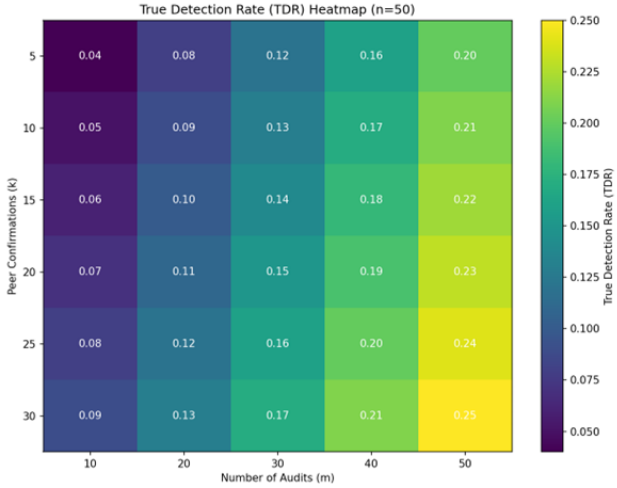

Figure 7: Truth detection rate ($n = 50$) [Community detection analysis]

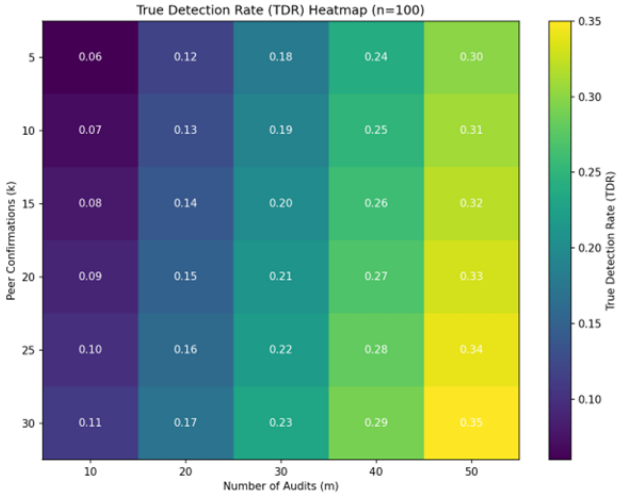

Figure 8: Truth detection rate ($n = 100$) [Community detection analysis]

For lower n values, the TDR improves for higher m and higher k. Not much significant change is noticed in lower values of k and m for $n = 50$. For $n = 100$ and $n = 200$, the TDR improves minimally due to better collusion detection algorithm in place. But the FPR remains almost the same or slightly higher in some iterations, averaging at 0.03 in our runs, which is close to 0 but almost the same as the simulations when no community detection algorithm was in place.

Now we analyze the heatmaps after modeling the dynamic behavior of colluding groups (Figure 11 to Figure 16).

For $n = 50$, the TDR is consistently around 0.45 across all combinations of peer confirmations (k) and audits (m). The FPR remains stable at approximately 0.18. This stability suggests that the system's ability to detect collusion is relatively independent of the number of peer confirmations and audits when the population size is small. The moderately high FPR indicates that the dynamic behavior introduces some noise in identifying colluding students, possibly due to frequent group changes in a smaller population where overlaps in attendance logs are more common. Figures 11 an 12 illustrate this.

For $n = 100$, the TDR is observed to decrease to around 0.32 across all k and m values, while the FPR drops to 0.11. The decrease in TDR might be attributed to the increased population size, which dilutes the effect of colluding groups due to a higher diversity in attendance logs. The reduction in FPR reflects that the system becomes more conservative in identifying collusion as the dataset

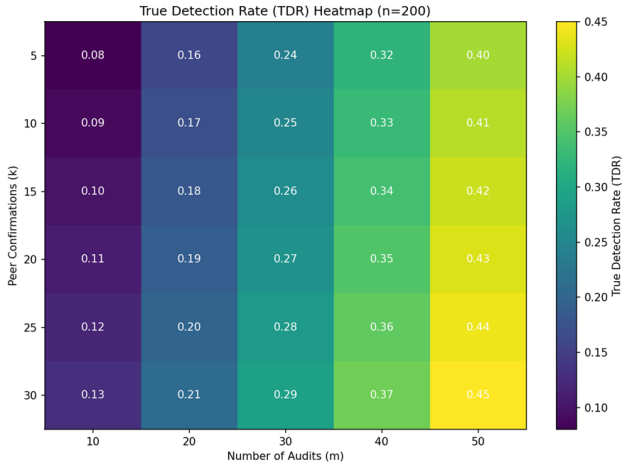

Figure 9: Truth detection rate ($n = 200$) [Community detection analysis]

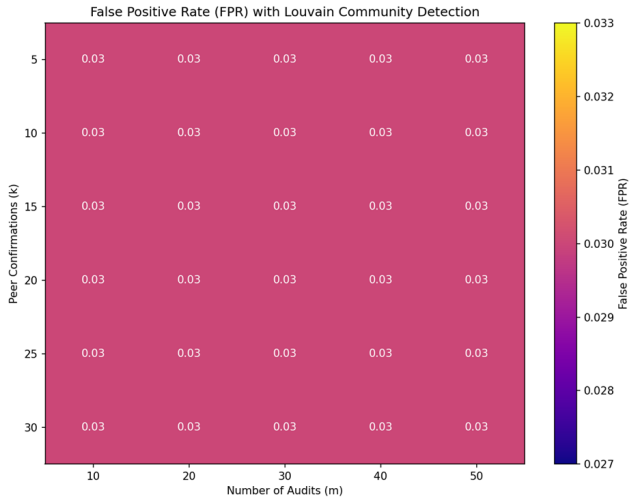

Figure 10: False positive rate [Community detection analysis]

grows, leading to fewer false positives. This is likely because larger populations provide more non-colluding data points, which reduce the likelihood of random overlaps being flagged as collusion. Figures 13 and 14 illustrate this.

For $n = 200$, the TDR stabilizes at around 0.44 across all k and m values, and the FPR further drops to 0.10. This improvement in TDR compared to $n = 100$ may be due to the larger sample size allowing for more robust detection of colluding patterns, even amidst dynamic group changes. The further reduction in FPR indicates that the system effectively minimizes false positives in a larger dataset by leveraging the increased diversity in attendance behavior. Figures 15 and 16 illustrate this.

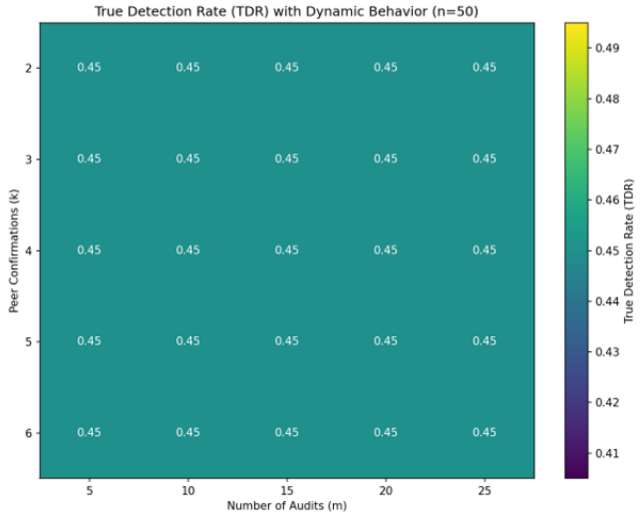

Figure 11: Truth Detection rate ($n = 50$) [Dynamic Behavior Modeling]

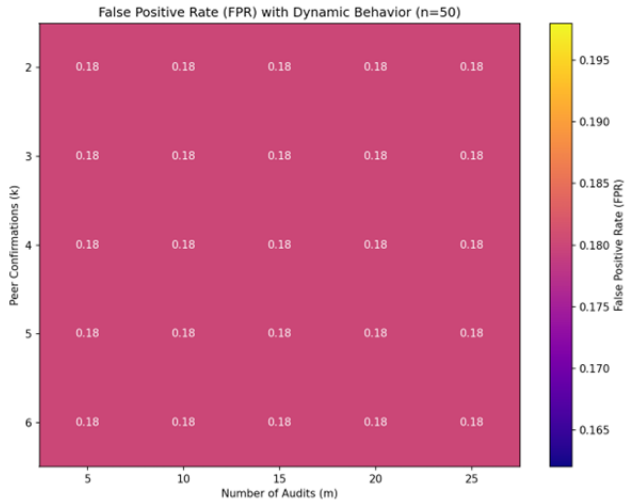

Figure 12: False Positive rate ($n = 50$) [Dynamic Behavior Modeling]

Across all cases, the TDR shows slight fluctuations but generally remains stable, indicating that the detection capability is relatively robust against changes in population size, given consistent parameters for k and m. The FPR exhibits a clear downward trend as n increases, highlighting the system's enhanced reliability in minimizing false positives in larger datasets. This trend suggests that dynamic behavior modeling becomes more effective with larger datasets due to better differentiation between colluding and non-colluding behaviors.

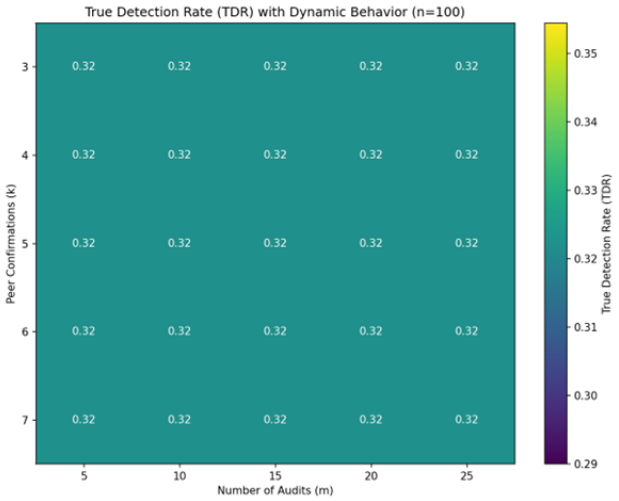

Figure 13: Truth detection rate ($n = 100$) [Dynamic Behavior Modeling]

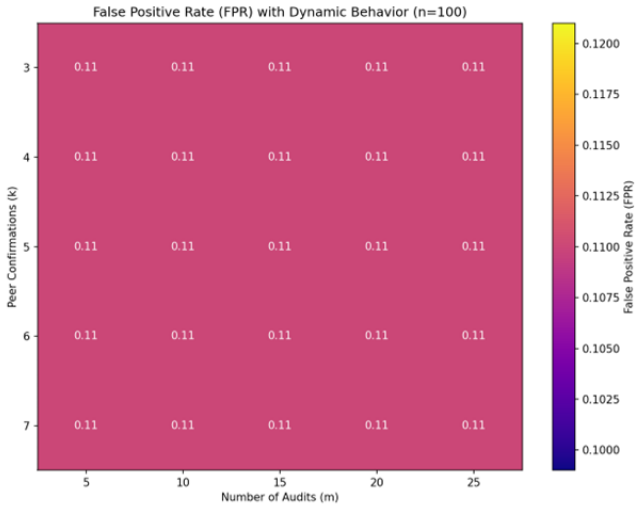

Figure 14: False Positive rate ($n = 100$) [Dynamic Behavior Modeling]

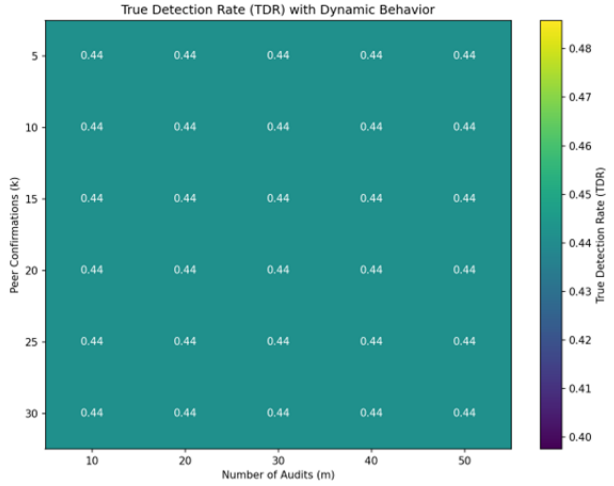

Figure 15: Truth detection rate ($n = 200$) [Dynamic Behavior Modeling]

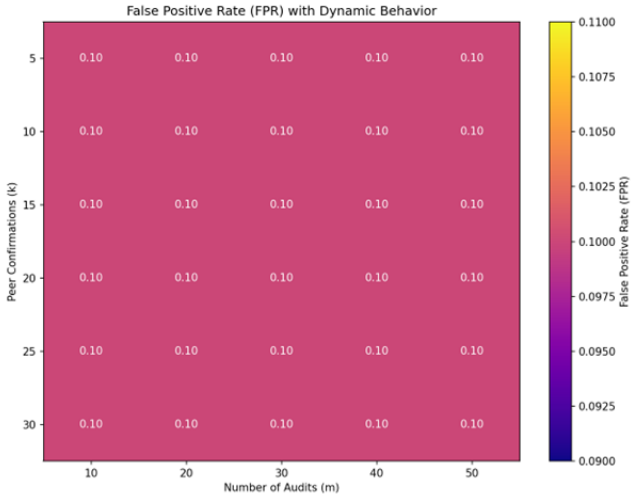

Figure 16: False Positive rate ($n = 200$) [Dynamic Behavior Modeling]

The consistency of the TDR across different n values implies that the system effectively adapts to dynamic group changes, maintaining its detection capability regardless of population size. However, the slight drop in TDR at $n = 100$ reflects a transitional phase where the system adjusts to increased complexity in attendance patterns. The steady decline in FPR with increasing n can be explained by the fact that larger populations provide a broader base of legitimate attendance behaviors, reducing the impact of random overlaps and enhancing the precision of the detection mechanism.

Now we observe the results after applying a penalty feedback mechanism. TDR remains similar for most values of k and m, but for $n = 50$, for higher values of m and low values of k, the TDR improves further than no mechanism in place (random) or community detection algorithm but not higher than when dynamic behavior is modeled. This can be attributed to the increased focus on smaller, more tightly-knit collusion groups. With lower k, collusion networks are smaller and easier to identify, and higher auditing rates (m) amplify the chances of exposing these groups. The penalty feedback mechanism further discourages repeated collusion by dynamically reducing the influence of penalized individuals in subsequent iterations, allowing the system to adapt and focus its detection efforts more effectively. However, this improvement is less pronounced than when dynamic behavior is modeled, as the

penalty mechanism does not inherently restructure group dynamics, which limits its ability to uncover new collusion patterns that evolve over time. Figure 17 shows this.

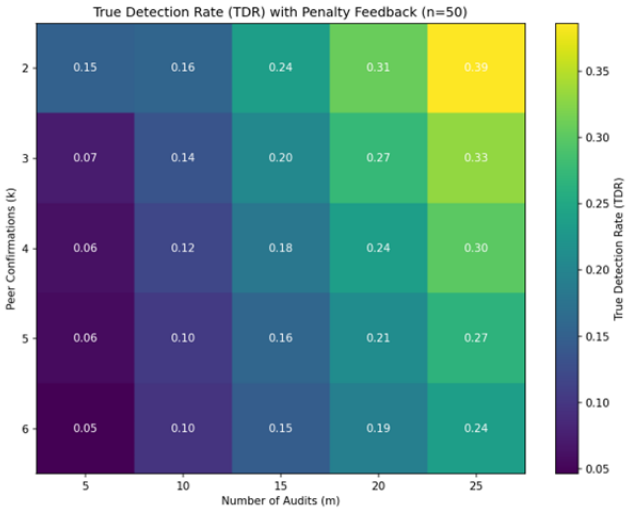

Figure 17: Truth detection rate ($n = 50$) [Penalty Feedback mechanism]

For $n = 50$, we observe upon a penalty feedback mechanism that the FPR remains consistently low, as with the other methods, but generally lower than the dynamic behavior mechanism for greater values of k. (Figure 18).

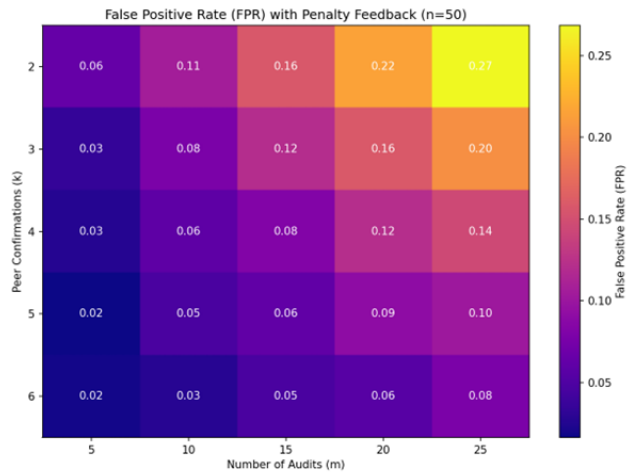

Figure 18: False positive rate ($n = 50$) [Penalty Feedback mechanism]

For $n = 100$, Figure 19 shows the TDR following a similar trend as $n = 50$. The penalty feedback mechanism improves TDR more than the random or community detection algorithm mechanism and less than the dynamic behavior mechanism for most values of k and m, except for high values of m and low values of k, just like for $n = 50$. Figure 20 shows that the FPR remains relatively low and similar to all other mechanisms.

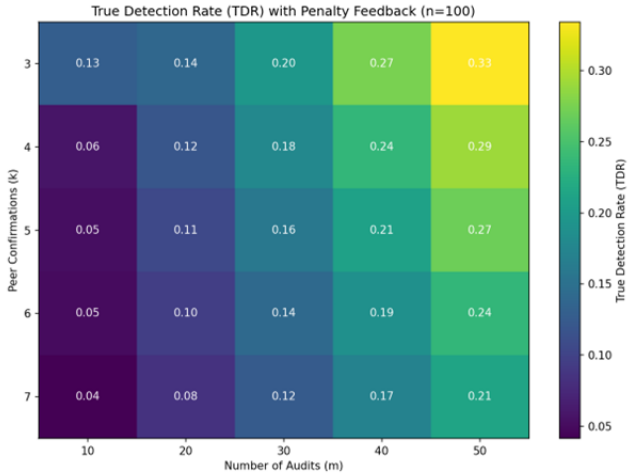

Figure 19: Truth detection rate ($n = 100$) [Penalty Feedback mechanism]

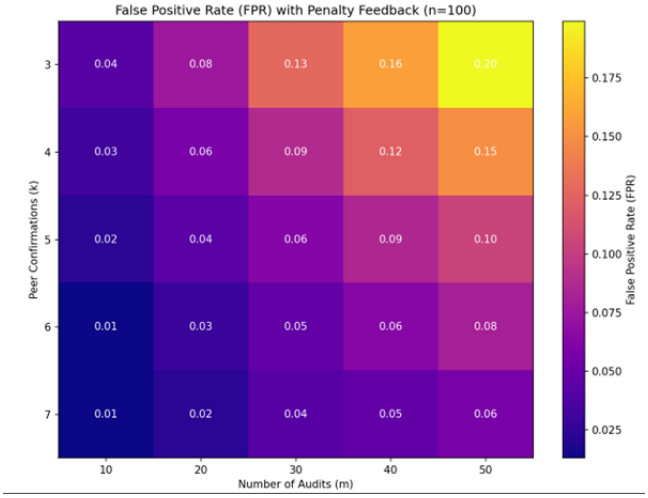

Figure 20: False positive rate ($n = 100$) [Penalty Feedback mechanism]

Figure 21 and Figure 22 show the TDR and FPR for $n = 200$. With a penalty feedback mechanism in place, the TDR remains very low compared to the dynamic behavior modeling. We notice further improvements in FPR for higher values of k and m. For $n = 200$, the

True Detection Rate (TDR) remains low with the penalty feedback mechanism because the larger population size creates more diffuse and less interconnected collusion groups, making it harder for penalties to propagate effectively and influence behavior. Additionally, the mechanism does not inherently address the adaptability of collusion strategies in a large-scale network, limiting its capacity to uncover dispersed colluders. However, the False Positive Rate (FPR) improves further for higher k and m because the combination of stringent peer confirmation requirements (k) and extensive auditing (m) minimizes the chances of incorrectly flagging honest participants, leading to more precise detection.

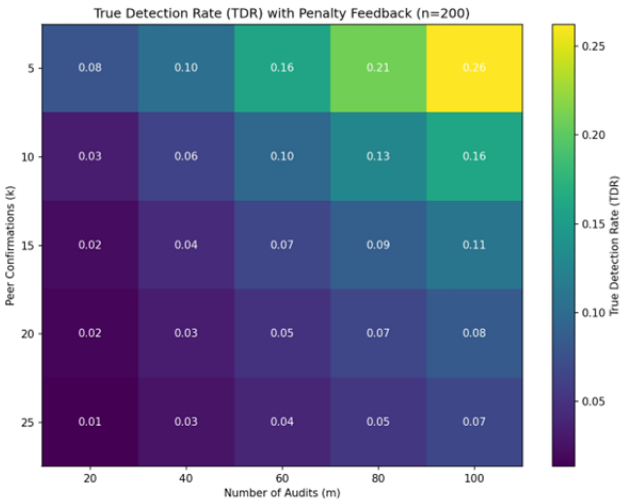

Figure 21: Truth detection rate ($n = 200$) [Penalty Feedback mechanism]

Across all simulations, one key observation is the robustness and scalability of the system in detecting collusion across different class sizes ($n = 50, 100, 200$). The TDR remains relatively consistent within a narrow range for most mechanisms, indicating the system's ability to scale effectively without significant loss of detection capability. However, certain mechanisms, such as penalty feedback and dynamic behavior modeling, demonstrate noticeable variations in performance based on class size and parameter values. For instance, dynamic behavior modeling exhibits the highest TDR values, particularly for smaller class sizes ($n = 50$), due to its ability to adapt to group changes. In contrast, penalty feedback mechanisms show improved TDR for lower k and higher m, especially in smaller populations, but their impact diminishes as n increases, reflecting limitations in addressing diffuse collusion networks in larger groups.

The False Positive Rate (FPR) remains consistently low across all mechanisms and class sizes, underscoring the system's fairness and precision in avoiding incorrect accusations. Notably, the FPR decreases with increasing n, as larger datasets provide greater differentiation between colluding and non-colluding behaviors. This trend is particularly evident with dynamic behavior modeling and penalty feedback mechanisms, where the system becomes more reliable in minimizing false positives as the population grows.

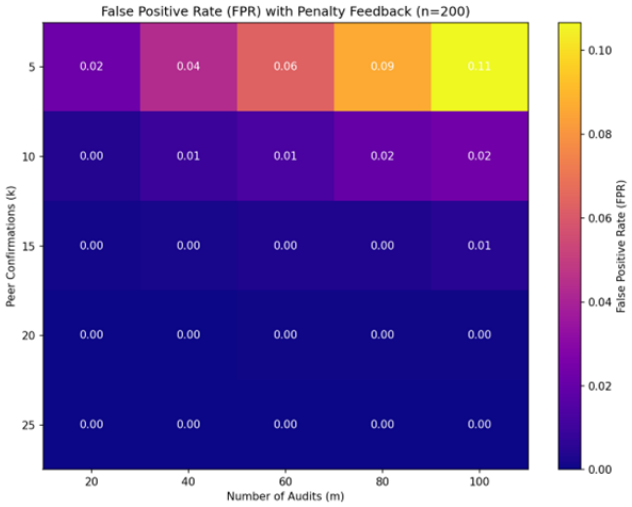

Figure 22: False positive rate ($n = 100$) [Penalty Feedback mechanism]

When comparing mechanisms, dynamic behavior modeling consistently outperforms others in terms of TDR, particularly for smaller and medium-sized classes ($n = 50$ and $n = 100$). It effectively captures evolving collusion patterns by modeling group dynamics, which is reflected in higher TDR values across all k and m. Penalty feedback mechanisms, while showing some improvement over random or community detection methods, are less effective than dynamic behavior modeling, especially for larger classes ($n = 200$). This limitation arises from the inability of penalties to address the evolving nature of collusion in larger, more diffuse networks.

In terms of parameter influence, higher audit frequencies (m) generally lead to improved TDR across all mechanisms and class sizes, as more frequent audits increase the likelihood of detecting collusion. However, this improvement diminishes beyond a certain threshold, suggesting a saturation point where additional audits yield minimal benefits. The impact of peer confirmation requirements (k) on TDR is less pronounced, with only minor variations observed. This indicates that k has a limited effect on collusion detection, as colluders may adapt their strategies to meet the confirmation thresholds.

Overall, the findings highlight the system's scalability and fairness across varying class sizes and mechanisms. While dynamic behavior modeling emerges as the most effective approach for improving TDR, especially in smaller classes, penalty feedback mechanisms offer a complementary strategy to enhance detection rates in specific scenarios. However, the relatively modest TDR values across all mechanisms emphasize the need for further refinements, such as adaptive auditing strategies or dynamic thresholds, to address the evolving nature of collusion and improve detection rates without compromising fairness.

5 RELATED WORK

The problem of ensuring accurate, fair, and privacy-preserving attendance tracking has been studied in various contexts, ranging from biometric systems to decentralized verification models. This section reviews key works that have informed the development of the proposed peer-confirmation-based attendance system.

Biometric systems, such as fingerprint scanning, facial recognition, and iris scans, have been widely adopted for attendance tracking due to their accuracy and convenience. However, these systems have faced significant ethical and privacy concerns. Sweeney's work on k-anonymity [7] highlighted the vulnerabilities of centralized biometric databases to misuse, surveillance, and identity theft. Additionally, Chaum [1] underscored the risks associated with untraceable digital systems that collect sensitive data. These studies emphasized the need for alternatives that minimize data collection and mitigate the potential for function creep, where data is used for unintended purposes.

Several frameworks for privacy-preserving data analysis, such as differential privacy [2], have informed the design of secure and ethical systems. Dwork et al. proposed mechanisms for calibrating noise in data analysis to protect individual privacy while enabling aggregate insights. These principles have inspired approaches in attendance systems to anonymize peer confirmations and reduce the risk of personal data exploitation. By adopting decentralized and pseudonymized structures, the proposed system aligns with these frameworks while addressing the unique challenges of attendance verification.

The ethical principles outlined by Friedman and Kahn [3] in their framework for embedding ethics in technology design have provided a foundation for this work. They argue for systems that prioritize human agency, transparency, and inclusivity, avoiding over-reliance on automation. Applying these principles, the proposed attendance system ensures user engagement and accountability through peer confirmation and manual audits, maintaining a clear distinction between human judgment and technological facilitation.

The concept of social identity verification has roots in distributed trust systems, such as those discussed by Chaum [1] and later expanded in blockchain and decentralized technologies. These systems leverage peer accountability to achieve consensus without centralized control. Similarly, peer-confirmation-based attendance systems use social networks to verify identity, reducing dependence on invasive biometric data. This approach is consistent with distributed trust models, where individuals collectively vouch for the authenticity of interactions.

Collusion detection has been extensively studied in the context of fraud detection in social networks. Girvan and Newman [4] introduced methods for identifying community structures in networks, which have been widely used for detecting anomalous behavior. The Louvain method, an efficient algorithm for modularity-based community detection, has further advanced the ability to identify tightly-knit groups exhibiting suspicious activity. These techniques have been instrumental in enhancing the proposed attendance system, enabling the detection of collusion groups that disproportionately vouch for each other.

Dynamic behavior modeling, as discussed in systems like the Maze framework [8], explores adaptive group behaviors and their impact on detection mechanisms. By simulating fluctuating peer relationships and evolving group memberships, such systems mimic real-world dynamics, providing valuable insights into group behavior. This concept directly informs the dynamic behavior modeling incorporated in the proposed system, allowing it to adapt to changes in attendance patterns and detect evolving collusion strategies.

Game-theoretic approaches to incentivize honest behavior and discourage collusion have been explored in various domains, including online marketplaces and voting systems. Mechanisms that dynamically adjust penalties, such as those proposed in Dwork et al.'s work on calibration [2], have inspired the penalty feedback mechanism integrated into this system. By reducing the influence of penalized individuals in subsequent iterations, the system dynamically adapts to discourage repeated collusion.

6 CONCLUSION

This project introduces a novel peer-confirmation-based attendance system designed to address privacy concerns and ethical issues associated with traditional biometric systems. By leveraging social identity verification, the proposed model fosters a decentralized and privacy-preserving approach to attendance tracking. The system not only avoids invasive data collection but also encourages collective responsibility and accountability through a combination of peer confirmations and random roll-call audits. Through simulations, the study evaluates the performance of the system under varying conditions, analyzing the impact of parameters such as k (peer confirmation threshold), m (audit frequency), and n (class size) on key metrics like the True Detection Rate (TDR) and False Positive Rate (FPR).

The initial results demonstrate the robustness and scalability of the system, as it performs consistently across varying class sizes. The incorporation of community detection algorithms enhances the ability to detect collusion by identifying tightly-knit subgroups with disproportionately high mutual confirmations. Dynamic behavior modeling further refines the system, adapting to evolving attendance patterns by capturing fluctuations in group memberships and peer relationships. This approach is particularly effective in smaller populations, where collusion patterns are more concentrated. Additionally, the penalty feedback mechanism adds a dynamic layer of deterrence, reducing the likelihood of repeated collusion by penalizing detected individuals and adjusting their influence in subsequent iterations.

Key findings from the simulations reveal that dynamic behavior modeling achieves the highest TDR, particularly in smaller class sizes (e.g., $n = 50$), due to its ability to adapt to changing collusion patterns. However, as class size increases (e.g., $n = 200$), the effectiveness of this mechanism diminishes, emphasizing the challenges of detecting diffuse collusion networks in larger populations. The penalty feedback mechanism, while effective in specific scenarios, demonstrates limited scalability for larger classes, as penalties alone do not fully address the adaptability of collusion strategies. Across all mechanisms, the FPR remains consistently low, underscoring the fairness and precision of the system in minimizing false accusations.

Larger datasets further enhance this trend, as the increased diversity in attendance behaviors improves the differentiation between colluding and non-colluding participants.

Despite its promising results, the system exhibits some limitations, including modest TDR values across all mechanisms, particularly for larger populations. This highlights the need for further refinements, such as incorporating adaptive auditing strategies, dynamic confirmation thresholds, or machine learning-based predictive models to enhance detection rates without compromising fairness. Additionally, while the penalty feedback mechanism introduces a deterrent against repeated collusion, it may benefit from integrating more sophisticated game-theoretic approaches to anticipate and counter evolving collusion strategies.

In conclusion, the peer-confirmation-based attendance system represents a significant step toward creating a privacy-preserving, ethical, and robust alternative to biometric systems. By combining techniques such as community detection, dynamic behavior modeling, and penalty feedback mechanisms, the system effectively balances privacy, fairness, and detection accuracy. Its scalability and adaptability make it a promising solution for decentralized attendance tracking in diverse scenarios. However, continued exploration of advanced detection methods and adaptive strategies will be essential to further enhance its robustness and applicability in real-world settings. This work lays a solid foundation for future research and development in privacy-focused attendance systems, aligning technological innovation with ethical principles.

REFERENCES

[1] David Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 2 (1981), 84–90. https://doi.org/10.1145/358549.358563

[2] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. 2006. Calibrating Noise to Sensitivity in Private Data Analysis. In *Theory of Cryptography Conference*, Shai Halevi and Tal Rabin (Eds.). Springer, Berlin, Heidelberg, 265–284. https://doi.org/10.1007/11681878_14

[3] Batya Friedman and Peter H. Kahn Jr. 2003. Human Values, Ethics, and Design. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*. CRC Press, 1177–1201.

[4] M. Girvan and M. E. J. Newman. 2002. Community structure in social and biological networks. *Proceedings of the National Academy of Sciences* 99, 12 (2002), 7821–7826. https://doi.org/10.1073/pnas.122653799

[5] K. Jain, R. Nandakumar, and A. Ross. 2007. Biometric Template Security: Challenges and Solutions. *IEEE Signal Processing Magazine* 24, 5 (2007), 88–100.

[6] Pasquale De Meo, Emilio Ferrara, Giacomo Fiumara, and Alessandro Provetti. 2011. Generalized Louvain method for community detection in large networks. *IEEE Transactions on Knowledge and Data Engineering* (2011).

[7] Latanya Sweeney. 2002. K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 5 (2002), 557–570. https://doi.org/10.1142/S0218488502001648

[8] Feng Zhu, Xinran He, Jiliang Tang, and Yuqing Sun. 2019. The Maze System: Modeling and Analysis of Online Collusion. *Journal of the Association for Information Systems* (2019).