By combining payment behavior-based features with action-based features, it becomes possible to identify shared accounts to a certain extent without disrupting user experience. Effective modeling of multiple users enables risk identification. In Alipay, we have devised the following framework to assess account risks, as shown in Figure 1.

4 EVALUATION

4.1 Evaluation Protocol

Data Collection. We collected the daily usage characteristics of 10,000 accounts from the Alipay-dev application, among which 2,000 accounts were shared. The ground truth regarding these accounts was determined by other departments within Alipay through user surveys and analysis of user usage patterns, ensuring the reliability of the results. Each data entry contains the following information:

Device information includes IMEI and geographical location.

User information includes the user's identity information.

Payment behavior information covers historical payment data, such as timestamps, amounts, merchant types, and locations.

Action information encompasses touchscreen data (click timestamps, locations, duration, and pressure) and motion sensor data (timestamps, accelerometer, magnetometer, and gyroscope).

It is essential to note that all users of the Alipay-dev have consented to provide this sensitive information, and the data is strictly protected within Alipay's internal servers.

Evaluation Metric. We mainly report the Area Under ROC Curve (AUC) metric. Specifically, the AUC metric is based on four major metrics: the True Positive, False Negative, True Negative, and False Positive results in detecting the shared account usage problem under different thresholds.

The AUC depends on the various thresholds that decide whether the account is shared. The Receiver Operating Characteristic (ROC) curve plots the True Positive Rate ($TPR = \frac{TP}{TP+FN}$) against False Acceptance Rate ($FAR = \frac{FP}{TN+FP}$) in different thresholds.

The resulting area between such curve and the X-axis at an interval of [0, 1] is termed AUC and evaluate the performance in detecting shared account.

Implementation Details. We implement the detection framework with Python 3.7 and PyTorch 1.8. The framework runs on a server with Ubuntu 20.04.6, 128 GB memory, 48 cores provided by Intel Xeon CPUs, and 4 NVIDIA GeForce GTX 2080Ti GPUs. All experiments are repeated by 3 times and reported the average performance.

4.2 Result

To demonstrate the effectiveness of detecting shared account problems, we present in Table 3 the performance of detecting shared accounts using payment behavior features, action features, and their combination. When combining both features, the AUC reaches 0.88, which represents the best performance. Moreover, using payment behavior features (0.79) or action features (0.78) separately shows little difference, but when compared to their combination, there is a significant drop in performance.

Table 3: AUC of detecting shared accounts.

Features	Payment	Action	Payment+Action
AUC	0.79	0.78	0.88

5 RELATED WORK

Super apps have emerged as an innovative and convenient platform that offers a wide range of services within a single application [6]. While these apps bring numerous benefits to users, they also introduce unique security and privacy challenges. Researchers have explored various methods and mechanisms to enhance trust and accountability, such as user authentication techniques [2], Cross-miniapp allowlisting [7], and API restrictions [5]. However, the security concerns surrounding super apps become even more critical. one of which is the shared account problem. Detecting timely and ensuring safety in shared accounts is crucial for maintaining user satisfaction and preventing misuse.

6 CONCLUSION

In conclusion, shared account problem presents security challenges. Current security protocols may misinterpret normal variations in multi-user behavior, causing inconveniences for legitimate users. In this paper, we underscore the need for an adaptive, user-inclusive approach to account security. By studying device account-sharing practices and implications on security protocols, we emphasize the importance of striking a delicate balance between robust security and seamless user experience. Developers must enhance security measures to accommodate shared usage while maintaining user trust. Moreover, we propose a shared account detection mechanism, which uses the payment behavior features and action features to detect the possibility of accounts whether shared with multiple users. Evaluation demonstrates the proposed solution achieves respectable performance.

ACKNOWLEDGMENTS

Ding Li and Yao Guo are corresponding authors. This work was sponsored by CCF-AFSG Research Fund (RF20220006).

REFERENCES

[1] Supraja Baskaran, Lianying Zhao, Mohammad Mannan, and Amr Youssef. 2023. Measuring the Leakage and Exploitability of Authentication Secrets in Super-apps: The WeChat Case. *arXiv:2307.09317* (2023).

[2] Hossein Fereidooni, Jan König, Phillip Rieger, Marco Chilese, Bora Gökbakan, Moritz Finke, Alexandra Dmitrienko, and Ahmad-Reza Sadeghi. 2023. AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms. *arXiv:2302.02740* (2023).

[3] Marc Hasselwander. 2023. Digital platforms' growth strategies and the rise of super apps.

[4] Lerong Lu. 2018. Decoding Alipay: mobile payments, a cashless society and regulatory challenges. *Butterworths Journal of International Banking and Financial Law* (2018), 40–43.

[5] Chao Wang, Yue Zhang, and Zhiqiang Lin. 2023. Uncovering and Exploiting Hidden APIs in Mobile Super Apps. *arXiv:2306.08134* (2023).

[6] Yuqing Yang, Chao Wang, Yue Zhang, and Zhiqiang Lin. 2023. SoK: Decoding the Super App Enigma: The Security Mechanisms, Threats, and Trade-offs in OS-alike Apps. *arXiv:2306.07495* (2023).

[7] Yuqing Yang, Yue Zhang, and Zhiqiang Lin. 2022. Cross miniapp request forgery: Root causes, attacks, and vulnerability detection. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 3079–3092.

[8] Yue Zhang, Yuqing Yang, and Zhiqiang Lin. 2023. Don't Leak Your Keys: Understanding, Measuring, and Exploiting the AppSecret Leaks in Mini-Programs. *arXiv:2306.08151* (2023).