Vishaank Ghai

Transforming Local-Infused Gaming:
New Product Development - Cloudflare Workers for Gaming

With the advent of technology in the digital space, the gaming industry has transformed drastically from the legacy disk to electronic delivery. This seismic shift in the gaming industry behavior, however, has opened up a whole new world of exploitations and other means tools with a goal to manipulate/cheat the intended gameplay(s). The gaming industry – its players, developers, and operations – across the wide array of game segments have suffered directly through the rise of such illicit activities. Cloudflare, and other companies, have taken on the task to address such issues in the web security, infrastructure, and content delivery space for the gaming industry (and the greater World Wide Web).

Through Cloudflare Workers for Gaming, Cloudflare has developed various tools that have been able to provide a greater, safer, and reliable gameplay for the gamers (while providing game developers a security net for their productions). These tools encompass some of the strongest capabilities in the digital security space today – DDoS protection, bot management, CDN enhancements, increased delivery through smart routing, and introduction of serverless computing.

The gaming industry can very much be thought of one that contains various frictions within itself; frictions involving players, developers, and operations/delivery components. The frictions can be split in a 4-quadrant arrangement, with harmful to beneficial being on the x-axis and unavoidable to avoidable being on the y-axis. Market research, segmentation, and SWOT analysis of the gaming industry must be performed in order to understand gamers, developers, and operations across the different segments of gaming. Triple-A games, the most popular and revenue generated games like Fortnite, GTA, etc., and Indie games like Minecraft, will be the 2 main segments of concern for this proposed plan.

Bringing back the topic of frictions in the gaming industry – the avoidable-harmful is the main quadrant of concern for this proposed plan as most of the trouble lies there. Akamai, a Cloudflare competitor, reported in 2019 that two-thirds of the attacks in the gaming industry today are done through SQL Injections (SQLi). Local File Inclusion (LFI) and over-the network attacks represent the remaining part of the puzzle. The SQLi attacks are typically performed in order to gain access into a player's account and take control of all their game assets (in-game currency, items, trades, etc.). In the younger generation player audience, the use of bots and LFIs has seen a rise due to the almost non-existent consequences. Keeping these ongoing behaviors in mind, the power of serverless gaming can be capitalized tremendously to drastically reduce the affections caused to and from the end-user (player) side.

To understand if the solutions involving serverless gaming would be viable for the developers and players, we start out by first analyzing some of the metrics that would provide the current on-ground situation of the industry. As starters, looking at current startup times, bit rate, session length, throughput on CDN, affections/session, traffic management, and types of attacks across Triple-A and Indie games would help us build together a framework of current end-user experience. It can be hypothesized that during popular releases, holiday season, and weekends/evenings, the performance for the end-user overall is compromised to some extent. From there on, selecting 3 game developing firms in both the Triple-A and Indie segments (and each of theirs's top 5 respected players), we work with them to understand the current pain points from both a player and a developer standpoint. It can be very well hypothesized that the whole genre of over-the-network server, LFI bots, player DDoS, and account access attacks are some of the common concerns. Once the common issues have been identified, work with the game developers to understand from a technical side the scripts and checks they have in place within their core games and servers to flag any such illicit activity. It will be very clear to understand from that, while the game developers are utilizing robust security measures, the extent of them does not pass much farther than bot traffic and account access exploits. Bringing together the 30 respected players (from the selection group above) and helping them understand the power/implications of introducing serverless gaming (as opposed to locally infused) would be the initial stepping stone.

From a technical implementation standpoint, the proposed plan for advancing Cloudflare for Gaming would be divided into a 3-part plan. Part 1 (9-month release) would be through Cloudflare CDN and Argo Smart Routing to enhance the current mechanism for accelerated delivery minimal latency. This enhancement would encompass the introduction of partial caching, through a Time to Live (TTL) implementation. Through this, even if a user is able to exploit a local file for current gameplay, the server side saved data would be able to recycle the pool of the user once the TTL cache has been expired. This would lead to the player, for a certain time, be able to utilize the perks that they gain from the exploit. However, such illicit actions would then be reverted to their original form after the cache expiry. The TTL cache would aid in content delivery through faster download and load times, specially during heavy traffic peak times. Once this implementation is complete, Part 2 would work on a serverless solution in

partnership with the 6 game developing companies (selection group above). This concept would encompass building a new Cloudflare Serverless Worker that would allow for game developers to bring together the original game logic (as well as all objects, assets, etc.) to the server-side. With most games being built out in Java, utilizing the power of JavaScript will allow for this worker to be capitalized to its fullest ability. Now, more than ever before, all functionality and logic of the game would lie from a server level. This would create a transactional style operation between the player and server, driving the requested action across different Cloudflare endpoints to respond back with the intended functionality of the action a player is trying to take in-game. In addition, utilizing Cloudflare's Spectrum, DDoS protection, CDN, and Argo Smart Routing products, we would be able to tie together a user's behavior to detect anomalies in their connections/behavior during the game-play. These efforts would eliminate the different types of LFI attacks, including bot and other exploitary activity, because now more than ever before all game intended actions take home from the server-side. Game developers, through this new foundation of gaming, would transform their end-user game packages into encrypted packages rather than individual files. These packages would only contain the core game startup content, along with TTL cache. Apart from that, individual files with the power of modifying game logic would not be changeable. Part 3 of the plan is visionary and a step that would require the success of Part 1 and 2. Part 3 involves the utilization of a blockchain framework mechanism for games, making all actions performed in a game into transactional accounts. This, while the most ideal solution, is very sophisticated and one that would take an industry leading change in gaming to make possible. This solution would allow for each asset/object/action in the game to be recorded in reference of a transaction to a user. The user's authenticity will be managed utilizing Cloudflare's existing tools, however, this new implementation would eliminate a significant portion (if not all) of the SQLi attacks that take place today. Now, with data points being present across various nodes/blocks in real-time, it would be almost impossible to perform a SQLi attack for a specific user to gain access to their assets. Coupled Part 3 with Part 2, this would truly revolutionize the gaming industry – one that utilizes server-side gaming intent coupled with a transaction based mechanism to map out player behavior, a solution that would reduce exploitations significantly.

All parts of the solution would initially be alpha-tested with a set group of players, in order to understand the advancements/implications our solutions put upon their gameplay. In addition, the game developers would be taken through this entire journey as well to help them understand the impact such innovations allow for their gaming sustainability. Part 1 would encompass the 30 respected players (mentioned above) and gaming industry bounty volunteers, working with them to apply exploiting capabilities and utilize TTL cache power to address the concerns. This would allow for us to have a robust release timeline, working hand-in-hand to make enhancements and real-time be able to understand player experience. Part 2 would see a similar roll-out procedure, with expanding the alpha-test to a beta-test as well. This beta-test would include new users (A/B tested) to rollout the packaged versions of the game and allow for a server-side gameplay experience. After a strong foundation and rollout of Parts 1 and 2 to larger audiences, Part 3 would start in development – a much larger fundamental change to gaming. All the parts will be worked in existing Cloudflare's Agile Pod environment, allowing for UX to core development and post-release analytics teams to understand the advancements/implications of their ongoing conceptual/reiterative work.

The foundational belief is that local-user infused gaming, especially with the growth in multiplayer online and asset-based experience, is not the go-to solution for gaming industry due to the potential risk of exploits (increasing, as explained above). The KPIs to measure success would definitely include the foundational startup times, bit rate, session length, throughput on CDN, affections/session, traffic management, and types of attacks across Triple-A and Indie games. There should be an increase in startup times and a reduction in affections due to the sophisticated approaches expressed through the plan. With TTL cache based mechanism, full-content game loading would not exist and SQLi/LFI attacks will be decreased. Risks involving adoption of change, initial release reliability, higher setup costs, and tightened developer access are definitely areas of concern as Cloudflare starts to pitch this plan to game developers and players. However, walking them through the journey and the long-term impact towards both developers and players can definitely aid in offsetting the initial adoption constraints. Through a collaborative effort with players and developers – understanding their concerns and mapping out current market situation(s) – the 3-part plan can be utilized to the fullest extent to better the gaming industry across all components. Players, now more than ever before would be allowed to pursue their passion, having the trust that game-player authenticity is kept to its highest standards. This would only increase the gameplay for players, allowing for greater length of sessions and asset power within games. From the developer side, this plan only opens doors to greater gaming power – pushing the limit of the gameplay and producing high-value assets through the games (with a satisfaction that exploits will be at an ever-so low). The application of this 3-part plan would help win the Triple-A and Indie game industries (and possible expansion into the rise of mobile and console gaming), with a higher throughout from their players – one that is reliable, accelerated, and authentic based. This plan allows for the gaming industry to address the avoidable-harmful quadrant in the friction matrix, drastically lowering the humanly developed affections that are a detriment to the gaming industry, its players, and its developers.