In a network security context, SSH logs can be used to see who was or was not able to log into a system. Given this, there are fraudulent entities who illegally try to get access to system(s). Now, SSH logs can be recorded and stored in files such that system administrators can look through them to find anomalous behavior, usually manifested through failed SSH requests. Generally, accepted SSH requests are made by people who have legal access to the system, with the converse being true also. However, failed SSH requests account for more traffic than accepted SSH requests. Now, given the enormity of failed SSH requests, it can be infeasible for system administrators to look through recorded SSH logs. Therefore, a need arises for a data visualization tool to aid system administrators to easily spot patterns, general and specific trends, and outliers in data. A visualization tool can prove to be a powerful and effective way to display complex data in a simple, easy-to-understand format.

Accordingly, the visualization tool shown in this paper allows the users to visualize the SSH activities of the malevolent entities, on a continent, country and user level, following the Schneiderman mantra(1: overview first, 2: zoom and filter, 3: details on demand). Consequently, network administrators or very loosely, anyone with the power of actionable intelligence, can use this interactive tool to make data-driven, visualization-aided decisions to ban IPs, ASNs, Corporations etc. in order to reduce network traffic and help identify malevolent entities in the public sphere.