Controller	Prob-Domain	Rationale for domain value
Physical or wireless network access	0	Cloud services do not have a realisitic possiblity of an adversary gaining physical access to the specific server hosting the application
Gain public network access to MQTT service	0.1	Using VDBR upper bound of 10% of breaches started with administrator error
Send malcious actuator messages to MQTT service	0.01	Despite decrytion weaknesses in TLS encryption being discovered every few years (CVE search https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=openssl+decrypt) The attacker will still typically need to aquire a great deal of the data stream https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_aviram.pdf which must be acquired through passive monitoring which is not possible from an internet attacker's network access. Given this scenario, the attacker must guess the values to be included in the message since there is no method to observe them. Likelihood will be much lower than 1 perccent, treating as an upper bound.
Malware Execution	0.01	In 2021 even off brand AV products block more than 99% of known malware https://www.virusbulletin.com/virusbulletin/2021/02/vb100-certification-report/. Studied from five years earlier https://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1000&context=ebcs_tools put this number below 2% .
Credential Reuse	0.03	The most likely path to success is an adminsitrator account credential was identified in some other data breach. Most recent reports show this has a less than 3% chance of leading to a breach https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report
Weak credentials	0.01	Microsoft studies show this is a 1% success rate, https://techcommunity.microsoft.com/t5/azure-active-directory-identity/advancing-password-spray-attack-detection/ba-p/1276936 . The actual liklihood is even lower because password spraying does not guarantee the valid password guessed will be for an application administrator
Phishing	0.12	Based on ProofPoint test results year over year, 12 % is the highest average failure rate observed. https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-state-phish-report-reveals-ransomware-and-phishing-attack-trends
Access to secondary factor	0.01	Malware is the most likely scenario to result in key loss, a key will need to be on the device on which malware is executing and the malware must be programed to find it. 1% is a very high upper bound.
Exploit vulnerable service	0.1	Using VDBR upper bound of 10% of breaches started with administrator error
Gain public network access to OS administration service	0.1	Using VDBR upper bound of 10% of breaches started with administrator error
Direct file system access to crack passwords or read configuration	0.1	Using VDBR upper bound of 10% of breaches started with administrator error, extending this to programing mistakes related to credential storage

Exploit application	0.1	Using VDBR upper bound of 10% of breaches started with administrator error, extending this to programing mistakes related application programming errors that lead to privileged access. The application does not require a great deal of database access to function so remote code exection is the most likely path beyond compromising an admin account which was 7% in this study https://cdn2.hubspot.net/hubfs/4118561/BCC030%20Vulnerability%20Stats%20Report%20(2020)_WEB.pdf
User device compromise	0.01	Ranking the same as malware execution since malware execution is the common path to device compromise, desktop or mobile
Mitigation measures		
Obfuscated unique queue names & node IDs or encrypt messages for non-repudiation	0.95	Barring an application exploit that grants the attacker knowledge of node identifiers and queue names the adversary is reduced to guessing. With multiple variables this likelihood is almost 0, therefore an upper bound of 5 % for an opening due to multiple adminstative errors is the worst case. Enabling encryption for identify managment reduces even this probability to almost 0 but it may be a good deal of additional effort for limited overall improvement.
Common cyber hygiene practices	0.5	using 50% as this considered the binary possiblity that a particular practice has been followed or not at the time of the attack. It appears attack node probability calculation is combining all probabilities but the attacker is unlikely to try them all on the same target in close succession