Proc. of the 7th International Conference on Engineering and Emerging Technologies (ICEET)
27-28 October 2021, Istanbul, Turkey

Security Analysis of AWS-based Video Surveillance Systems

Davies Aklamati
Department of Computer Science and Information Technology
University of the District of Columbia
Washington, DC, USA
davies.aklamati@udc.edu

Basheerah Abdus-Shakur
Department of Computer Science and Information Technology
University of the District of Columbia
Washington, DC, USA
basheerah.abdusshaku@udc.edu

Thabet Kacem
Department of Computer Science and Information Technology
University of the District of Columbia
Washington, DC, USA
thabet.kacem@udc.edu

***Abstract*—In the last few years, Cloud computing technology has benefited many organizations that have embraced it as a basis for revamping the IT infrastructure. Cloud computing utilizes Internet capabilities in order to use other computing resources. Amazon Web Services (AWS) is one of the most widely used cloud providers that leverages the endless computing capabilities that the cloud technology has to offer. AWS is continuously evolving to offer a variety of services, including but not limited to, infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service. Among the other important services offered by AWS is Video Surveillance as a Service (VSaaS) that is a hosted cloud-based video surveillance service. Even though this technology is complex and widely used, some security experts have pointed out that some of its vulnerabilities can be exploited in launching attacks aimed at cloud technologies. In this paper, we present a holistic security analysis of cloud-based video surveillance systems by examining the vulnerabilities, threats, and attacks that these technologies are susceptible to. We illustrate our findings by implementing several of these attacks on a test bed representing an AWS-based video surveillance system. The main contributions of our paper are: (1) we provided a holistic view of the security model of cloud based video surveillance summarizing the underlying threats, vulnerabilities and mitigation techniques (2) we proposed a novel taxonomy of attacks targeting such systems (3) we implemented several related attacks targeting cloud-based video surveillance system based on an AWS test environment and provide some guidelines for attack mitigation. The outcome of the conducted experiments showed that the vulnerabilities of the Internet Protocol (IP) and other protocols granted access to unauthorized VSaaS files. We aim that our proposed work on the security of cloud-based video surveillance systems will serve as a reference for cybersecurity researchers and practitioners who aim to conduct research in this field.**

***Index Terms*—Cloud computing, Cloud Video Surveillance, Video Surveillance Systems, Amazon Web Services (AWS), Video Surveillance Cyber Security**

I. Introduction

Cloud-based video surveillance, also know as Video Surveillance as a Service (VSaaS), typically includes remote viewing, storage, management alerts, video recording and storage [**1**]. Before emergence of VSaaS was Internet connected traditional digital video recorder (DVR), network video recorder (NVR) or video management system (VMS). The traditional system that handles video processing, recording, and administration transpires on a computer installed at the local site. With VSaaS, video processing, recording, and administration is executed in the cloud. VSaaS is a solution that is packaged and then delivered over the internet as a service. Depending on the features of the plan, the price varies in consideration of the amount of storage, number of cameras, and software features [**2**]. Once the video is captured, it is streamed to a service provider's data center via Internet. The service provider's cloud runs the video management software on the back-end infrastructure. To view the footage, all that is required is an internet connected device and a web browser.

One of the most important benefits of cloud technology is bandwidth availability since cloud-based solutions allow for an accessible collection of ample amounts of data. Cloud implementations are also easier to deploy and maintain and are more cost effective with the elastic computing power in the cloud for a variety of video surveillance solution use cases. The global cloud computing market size is expected to grow from $371.4 billion in 2020 to $832.1 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 17.5 percent during the forecast period [**3**]. According to the same survey, AWS had the greatest enterprise public cloud adoption in 2020 where it experience a steady 30 percent growth every quarter.

Even though these benefits make VSaaS an attractive option for video surveillance, there has been several experts, such as in [**4**, **5**], who pointed out that this technology suffers from several vulnerabilities that may be exploited by attackers. However, to the best of our knowledge, there has not been neither an in-depth security review that proposes a taxonomy of attacks targeting VSaaS, nor an actual implementation of some of these attacks.

In this paper, we conducted a holistic security analysis of VSaaS by examining the vulnerabilities, threats, and attacks that target it. We proposed a novel taxonomy of attacks targeting cloud-based video surveillance systems that takes three criteria of classification, including the technique being used in the attack, its difficulty of implementation and its location. We also illustrate our findings by building a video surveillance test bed based on AWS cloud, due to its popularity [**6**], where we

This work was funded by NSF award 2011689

successfully injected four types of attacks: Denial of Service (DoS), Distributed Denial of Service (DDoS), passive man-in-the-middle (MITM) and active MITM. We also provide some guidelines to be followed in order to mitigate these attacks.

The rest of the paper is organized as follows. Section II provides some required background of Cloud Computing. Section III discusses the related work. Section IV discusses the vulnerabilities and attack taxonomy. Section VI describes the AWS-based test bed and the implementation of attacks.

II. Cloud Computing Background

Cloud computing is an on-demand service, which is delivered via Internet to computing resources, applications, physical and virtual servers, networking intelligence and development tools hosted at a remote data center and administered by a cloud service provider (CSP). The term cloud computing could also refer to the technology that forms the infrastructure to operate; i.e virtualization. The services included in cloud computing are, as shown in Fig. 1, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) models. VSaaS rides on the back and shoulders of SaaS model.

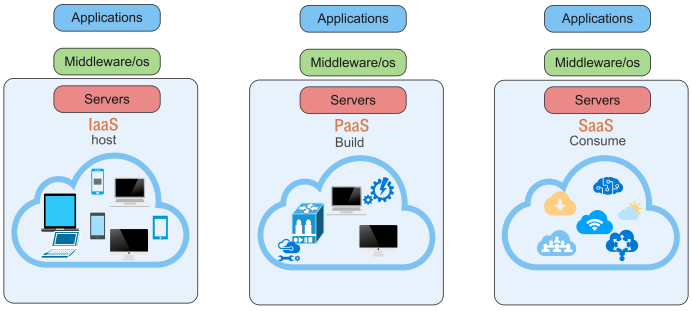

Fig. 1. Cloud Models

SaaS, also known as cloud applications, is an application software that is hosted in the cloud and can be accessed and used via a web browser or mobile client [**7**]. To a large extent, SaaS users may end up paying a monthly or annual subscription fee; others may offer an on-demand model depending on the consumption. IaaS includes computational resources which are made available to users as on-demand services. Sample resources include servers, network devices, memory, and storage. IaaS offer virtual machines that enable customers to develop complex network infrastructures with the use of virtualization technology.

PaaS is designed to provide the development platform for customers to construct tailor-made applications. Services included in this model incorporate tools and libraries for application development which enable users to have command over the application deployment and configuration settings.

III. Related Work

Du et al. [**8**] looked into privacy preserving in cloud surveillance systems. They investigated the privacy agreement of users in a group. To retain possession of user-sensitive videos confidential to the cloud, they implemented the protection mechanisms locally, before videos are transmitted to the cloud. In their work, they require to accumulate a series of frames first, which implies there is an incurred delay that may be costly. Also, they did not provide a clear taxonomy of attacks that are specific to the technologies in use.

Zhou et al. [**9**] discussed cloud-based visual surveillance systems related to VSaaS and its corresponding wireless security system that enables users to remotely store, manage, record, play and monitor surveillance videos. This research focused on video streaming input, intelligent visual surveillance, video trans-coding and storage in real time, and message push notification and streaming media output. The research further discussed security measures of VSaaS, quite interesting but failed to discuss the vulnerabilities associated with web technology and other communication protocols in place.

Mabrouk et al. [**10**] discussed the unorthodox behavior recognition by proposing an intelligent video surveillance system as a service and further discussed the geographical extension of this service. The authors integrated preceding knowledge in the field of surveillance systems with up to the minute trends of computation distribution within the cloud. They further stated that the availability of a cloud architecture brings into existence advanced solutions available which can stretch out surveillance competencies to general bodies. The complexity of video surveillance systems makes them prone to other threats and attacks, hence the focus of this research.

Assante et al. [**11**] proposed a virtual software as a service architecture for the cloud computing environment. In their discussion, the authors explicitly discussed the virtual execution layer and concluded that the prevailing legacy software can be embraced in the absence of redevelopment or redesign work; and that the distribution handling the back-end resource pool is dynamically managed in an on-demand process without pre-installation. Furthermore, they stated that security was taken into consideration using a verification mechanism based on hash-based message authentication code (HMAC). Our work focuses instead on the security analysis of Amazon Web Services-based video surveillance systems and gives recommendations for attack mitigation.

IV. Vulnerabilities of Cloud-based Video Surveillance Systems

VSaaS, as shown in Fig. 2, is purposefully designed to allocate extensive and on-demand network access to a distributed pool of recorded multimedia resources, quickly obtainable and delivered with the least possible management involvement or service assistance which makes it relatively effortless for the end user. The on-site camera records the audio/video stream, forwards it to the cloud, then the Video Management Software (VMS) transports the footage on-demand to the end user. However, from a comprehensive perspective, the process involves other various valuable steps in tandem with VSaaS cloud distribution architecture as public, private or hybrid or a composition of the two (hybrid). Public architecture uses

a CSP with a previously setup environment for video surveillance management and currently, it is the largely used scenario for VSaaS [**12**]. Private architecture leverages locally hosted cloud service by an agency or enterprise with interest to utilize the platform for video surveillance purposes. This architecture is usually exhausting to maintain. Hybrid architecture rely on pre-configured systems in order to implement the end user preferences based on the clients' selection and business-driven data procurement, which includes motion observation, sound and alarm system activation.

Comparably, the vulnerabilities and threats are inescapable in the cloud. Cloud systems are multi-subscriber domains that allocate infrastructure and resources across manifold far-reaching clients. Cloud providers do diligent work to service the nobility of its allocated infrastructure [**12**]. All together, the cloud is a self-service structure, in addition to, each and every client is compelled to diligently describe the exact standards for each of its workloads and resources. With all these processes going on, vulnerabilities do exist. A vulnerability could be an error, weakness or flaw in the cloud service provider security posture. There are innumerable vulnerabilities associated with VSaaS including but not limited to mis-configured firewalls, unencrypted data or unpatched operating system.

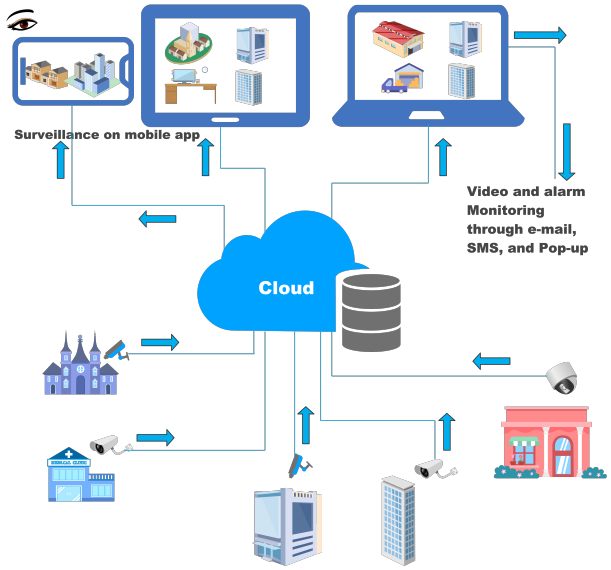

Fig. 2. VSaaS Architecture

A. Implementation of Camera System

IP cameras, also known as network cameras, distribute digital video surveillance content by means of transmitting and receiving footage across the internet or local area network (LAN). As the name indicates, IP cameras bridge to a network by means of wireless fidelity (WiFi) or a Power over Ethernet (PoE) cable [**13**].

B. Exploitable Vulnerabilities

The authentication protocol of the IP camera generally uses the advanced encryption standard (AES) protocol which is vulnerable to Man in the middle attack (MITM) and brute force attack [**13**]. These vulnerabilities are further discussed in the attacks and experiment section of the paper. Other exploitable vulnerabilities include cross site scripting and cross site request forgery.

V. Cloud-based Video Surveillance Systems Attack Taxonomy

This section presents our proposed taxonomy of attacks that target cloud-based video surveillance systems. Our attack taxonomy is based on the following criteria; difficulty of attack, attack technique, and attack location.

The taxonomy of attack identifies the complexities in preparing and executing the attack, the technique being used by the attack, and location of the attack. The discussion in this section is limited to cloud-based Video Surveillance Systems with reference to VSaaS. The VSaaS requires the IP camera to operate and these devices are susceptible to hardware and network vulnerabilities. The attacks discussed are relative to VSaaS with malevolent effects to disrupt data in transit, inject malware to data at rest, and intercept video data logs stored in the cloud.

VSaaS systems encompass third party infrastructure (Internet, client systems, network infrastructure), external cloud infrastructure (schedulers, firewalls), and internal cloud infrastructure (host hardware, hypervisors, internal networks, and administrator domain) that an attacker can exploit to launch attacks [**14**].

The complexity of an attack is analogous to the competence level to perpetuate the attack. The complexity level of the attack can be classified as high, medium or low. High-level of an attack references difficulty of the attack and implies that the attack requires ample knowledge about VSaaS systems. Medium-level of an attack implies that the difficulty level of the attack requires competency refinement in order to accomplish the appropriate results, thus, such attacks assume relatively moderate understanding level of VSaaS systems. Low-level difficulty of an attack implies that the attack can be carried out by means of promptly obtainable hardware and software with very little familiarity with VSaaS systems.

A. Description of Attacks

This subsection discusses some attack instances that utilize vulnerabilities associated with VSaaS systems. Each attack instance comprises an outline accompanied by features of the attack taxonomy. It is important to note that, an instance of an attack may comprise different and several attacks that are integrated to produce complex ones.

Man in the Middle (MITM)- Every single operating system (OS) has a built-in function known as the *traceroute* or some alternative thereof. This network diagnostic tool facilitates tracking in real time the pathway taken by a packet on an IP network from its original source to destination while broadcasting all the IP addresses it intermediately pinged. The traceroute utility is used to send packets from the attack system to the target client, listing the entire route it took

to destination [**15**]. This discloses the total of devices the attacker network data is passing through which includes the IP addresses of each device. A traceroute to aws.amazon.com for instance took 30 hops maximum to reach and not all the gateways are secure. Sentient Hyper-Optimised Data Access Network (SHODAN) is a search engine that reveals relatively any device that is connected to the Internet. SHODAN strips down bits of information known as banners from these devices. The SHODAN port inspects and takes back information such as IP addresses and firmware versions on devices that are particularly not secured. Immediately, the banners are obtained with weak login credentials, a packet sniffer can then installed to listen to any information that passes through the gateway.

- **Difficulty:** High.
- **Technique:** Obtain banners and sniff packet.
- **Location:** IP network.

Denial of Service (DoS) - DOS attack is intended to shut down a network or machine, thus, making it inaccessible to cloud clients. After successfully deploying MITM, a botnet is created out of the unsecured devices and floods client target with traffic. The humongous traffic sent to the client machine, in consequence, causes it to be laggy and eventually to stop. Leveraging the Internet Control Message Protocol (ICMP) flooding service and misconfigured network devices, spoofed packets are forwarded to ping every computer on the targeted network instead of a specific machine. Synchronize (SYN) flood is another DOS attack technique that is exploited to forward requests to connect to the cloud server without completing a handshake [**16**]. The activity is continued till all open ports are overloaded with requests until none is available for cloud users to connect to.

- **Difficulty:** Medium.
- **Technique:** Ping every machine on network.
- **Location:** Client machine.

Distributed Denial of Service (DDoS) - A DDoS attack occurs when collective systems direct a synchronized DoS attack to a single target. The key difference is that, instead of being attacked from one location, the client target is attacked from numerous locations at the same time [**16**]. The distribution of hosts that defines a DDoS provide the adversary with different advantages in leveraging the greater volume of machines to implement a critically unorthodox attack.

- **Difficulty:** Medium.
- **Technique:** Redirect synchronized DoS attack.
- **Location:** Client machine and IP network.

IP Spoofing IP spoofing is a kind of attack where a threat agent wiretaps the network with the intent to compromise the target computer or the network by imitating the characteristic features of a genuine source address and replaces with a replica. The threat agent exploits this vulnerability by signing up with cloud service provider to obtain Virtual Private Cloud (VPC). The VPC is then used to run attack scripts that initiate the intended spoofed traffic to overwhelm a VSaaS user's network with unnecessary traffic, modifies the source address in the packet header to make the VSaaS think that the packet is from a reliable source on the network [**17**]. The spoofed packets are redirected out of the cloud provider's network that hosts the threat agent's VPC with the aim to conduct a direct attack on the target. The video data generated from VSaaS user is then captured during transmission on the target's Wide Area Network.

- **Difficulty:** Medium.
- **Technique:** Eavesdrop on network.
- **Location:** Client machine or IP network.

Cloud Malware Injection Attack With this attack instance, the adversary attempts to gain access over the victim's data stored in the cloud by injecting an implementation of a malicious service or virtual machine [**18**]. Once successful, the adversary can eavesdrop on every activity in the cloud, redirect VSaaS user's requests, eventually gaining full access and possibly modifying data. For instance, SQL servers for VSaaS can be targeted using SQL injection attack.

- **Difficulty:** Medium-high.
- **Technique:** Add malicious script to victim's web page.
- **Location:** VSaaS network.

Cloud Zombie Attack This attack instance is purported to be one of the state-of-the-art attacks in cloud computing domain which deteriorates the capabilities and throughput of the network. Leveraging the capabilities and vulnerabilities of the Internet, the adversary makes an attempt to escalate the casualty by sending requests from innocent hosts or zombies in the network. Zombies are used by adversaries to launch DoS or DDoS attacks [**18**]. This type of attack interferes with the conventional performance of the cloud affecting the availability of cloud services.

- **Difficulty:** Medium-high.
- **Technique:** Deteriorate network.
- **Location:** IP network.

TABLE I
CLOUD-BASED VIDEO SURVEILLANCE SYSTEMS ATTACK TAXONOMY

Attacks	Difficulty	Technique	Location
MITM	High	Sniff packets from obtained banners	IP network
DoS	Medium	Intercept machine or network	Client machine, VSaaS network.
DDoS	Medium-high	Redirect synchronized DoS attack	Client machine and network
IP Spoofing	Medium	Wiretap network	Client machine and or network
Cloud Malware Injection	Medium-high	Inject malicious script	IP network
Cloud zombie	Medium-high	Deteriorate network	IP network

To summarize this section, Table I provides an overview by listing most common attacks with regards to their difficulty of implementation, technique being used and location in the cloud-based video surveillance system.

VI. Evaluation

This section discusses the assessment of VSaaS model with reference to attacks that elastic cloud compute is susceptible to. With enhanced network bandwidth, low cost, storage and easy deployment and maintenance, end users have a high opinion and see the shift in accepting cloud-based solutions, not knowing the assailable risks facing the cloud technology. Experimental analyses of the attacks are detailed with corresponding outcome. In particular, four categories of attacks were implemented in the experiments.

A. Test Bed

The test bed, as described in Figure 3, is composed of the following components. First, we used two wireless IP camera IP2M-091B . Then, we created an AWS Elastic Compute Cloud (EC2) instance, used to store the surveillance data, from which we launched a kali Linux instance connected via the terminal command-line-interface (CLI).

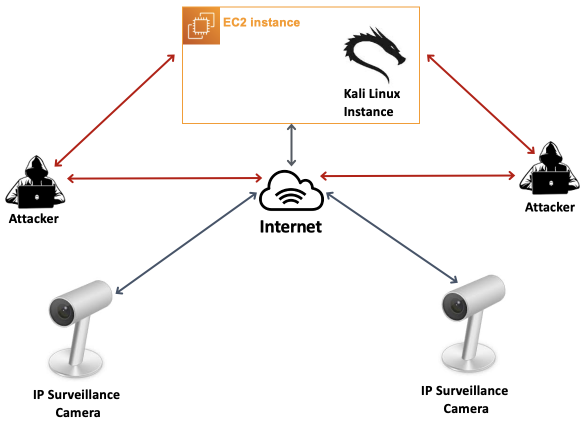

Fig. 3. Cloud based video surveillance architecture

B. Experiments

1) Experiment 1 - DoS Attack:: Implementation of this attack instance is deployed on kali linux via EC2 compute. Using metasploit auxiliary SYN flood, a penetration testing platform, exploits are triggered.

- **Step 1:** Metasploit is launched with the "msfconsole" command from terminal. Once metasploit is launched, the auxiliary is selected with the command "use auxiliary/dos/tcp/synflood".
- **Step 2:** The "traceroute" function is evoked to reveal the IP and port number for the target. This is required to setup RHOST (IP address of the target) and RPORT (port number of the target).
- **Step 3:** To launch the attack, the "exploit" command is run to initiate SYN flooding. Wireshark is then placed in the target machine to display the packets that hit the target. In order not to be highly vulnerable to discovery, half-open state is created on the target machine to prevent the attacker machine from responding to the server's SYN-ACK packets.

2) Experiment 2 - DDoS Attack:: The goal of this attack is to exploit vulnerabilities in the cloud network with the aim of making a vulnerable system the DDoS master. The aim is to overload the HTTP servers in order to exhaust the resources in the cloud.

- **Step 1:** To implement this attack, we used hping3 that is a command in kali used to analyze the IP network.
- **Step 2:** "-S" option of this command specifies sending SYN packets, while "-p 80" targets port 80 and "-i u1" waits for 1 microseconds between packets up to 4,000 packets per second.
- **Step 3:** While the simulated attack was up and running, the load time, latency in transmission, and number of transmissions were monitored for irregularities.

3) Experiment 3 - Passive MITM Attack:: The purpose of this experiment was to find vulnerabilities that a hacker could exploit. This experiment was conducted on AWS kali Linux Virtual Machine (VM) following the procedure outlined in IJERT-Penetration Testing using Linux Tools: Attacks and Defense Strategies [**19**]. This technique involves using Ettercap, a comprehensive suite for MITM attacks, and Drifnet that enables attackers to watch network traffic and picks up images for display.

- **Step 1:** Using bridged sniffing, we enabled the packets to be forwarded and routed to the destination.
- **Step 2:** After scanning, the host list was displayed at which point you can define your targets.
- **Step 3:** Then we began sniffing and extracted traffic.

4) Experiment 4 - Active MITM Attack:: Active MITM attacks can be utilized to intercept real-time transport protocol (RTP) video streams to perform any of the following: freeze frame content, archive and loop a clip to disrupt live streaming and reroute and inject content into video streams in the cloud. Furthermore, fake certificates can be provided for HTTPS, traffic can be deleted or injected with malware and passwords can be sniffed.

- **Step 1:** Using a video security assessment tool on kali Linux to simulate a proof of concept video interception, the RTP port was first captured.
- **Step 2:** Next, analysis of the RTP packets, collecting the sequence numbers and timestamp values used between two video endpoints.
- **Step 3:** Then, a custom video payload was created by changing the sequence numbers and timestamp values.
- **Step 4:** Lastly, this resulted in video replay of a previous session, playing a random file and severely degraded audio and video quality.

C. Guidelines for Attack Mitigation

1) DoS and DDoS Mitigation:: The availability of a service, resource or data may be affected during a DDoS attack where the video surveillance may be interrupted where it ceases to transmit video content, eliminate historic content

or block access through the use of a remote botnet. DoS and DDoS, web application programs and DNS infrastructure attacks illustrate some of the most analytical threats to cloud environments and enterprises. The ultimate technique for protecting systems and resources against DoS and DDoS coupled with other cyber attacks is to maintain several security resolutions that implement a disparate approach in detecting harmful incidents for internal and external threats. For internal threats, it is essential to have a competently designed security infrastructure that incorporate components such as firewalls, Intrusion Prevention System (IPS) or Intrusion Detection System (IDS), email and application security solutions.

2) MITM Mitigation:: Countermeasures to protect video surveillance against MITM attacks on the cloud should include the use of IDS and IPS systems and enforcing secure communication mechanisms to ensure the integrity of the video content where possible, disable APIs, reevaluate the configurations and encryption used for devices, and restrict physical access.

VII. Conclusion

In this paper, we presented a holistic security analysis of VSaaS by analyzing its vulnerabilities and the corresponding attacks that may exploit them. We also provided a novel taxonomy that provides a basis for security experts wishing to pursue research in this area. We developed a test bed representing an AWS-based VSaaS and we implemented four types of attacks that revealed how the network can be sabotaged considering the vulnerabilities. The novelty of our research is the classification of attacks that exploit vulnerabilities in VSaaS and cloud technologies. System investigation was primarily carried out by creating a test environment with a EC2 instance from which kali instance was run. Certain attack vectors such as SYN flood, UDP flood, and DNS amplification helped us analyze the delayed access or retrieval of files. Some useful parameters for mitigation are virtual availability of detection mechanism for advanced attacks in cloud technologies. The real time reporting mechanism parameter would help determine how network ACLs allow and deny rules of engagement in the event of an attack. The outcome of the carried out attacks are summarized as follows:

- **Result 1:** SYN packets sent to server caused denial of legitimate client request.
- **Result 2:** Multiple requests sent to target generated heavy traffic to the web server.
- **Result 3:** ARP poisoning placed between target systems redirected traffic for impersonation, file deletion and manipulation.
- **Result 4:** RTP capturing resulted in video replay of previous sessions and random files.

The cost of EC2 resources is not readily made known, hence, certain attack vectors that needed to be run for a certain time frame had to be stopped in order to avoid excess cost. Newbies to EC2 can find it quite challenging to understand the networking and the auto-scaling is quite complex. Technically, cloud technology is here to stay, researchers can explore some attack vectors and leverage on available tools for cloud exploits.

In future work, we plan to explore testing how AWS reacts to other types of attacks and what are the proper techniques to thwart them. Also, we plan to evaluate how other cloud providers react to these attacks.

References

[1] D'Angelo, G., & Rampone, S. (2018). A NAT traversal mechanism for cloud video surveillance applications using WebSocket. Multimedia Tools and Applications, 77(19), 25861-25888.

[2] Wang, R., Tsai, W. T., He, J., Liu, C., Li, Q., & Deng, E. (2019, February). A video surveillance system based on permissioned blockchains and edge computing. In 2019 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 1-6). IEEE.

[3] Siddiqui, S. T., Alam, S., Khan, Z. A., & Gupta, A. (2019). Cloud-based e-learning: using cloud computing platform for an effective e-learning. In Smart Innovations in Communication and Computational Sciences (pp. 335-346). Springer, Singapore.

[4] Obermaier, Johannes, and Martin Hutle. "Analyzing the security and privacy of cloud-based video surveillance systems." In Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security, pp. 22-28. 2016.

[5] Costin, Andrei. "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations." In Proceedings of the 6th international workshop on trustworthy embedded devices, pp. 45-54. 2016.

[6] Limna, T., & Tandayya, P. (2018). Workload scheduling for Nokkhum video surveillance as a service. Multimedia Tools and Applications, 77(1), 1363-1389.

[7] Markova, O., Semerikov, S., Striuk, A., Shalatska, H., Nechypurenko, P., & Tron, V. (2019). Implementation of cloud service models in training of future information technology specialists.

[8] Du, H., Chen, L., Qian, J., Hou, J., Jung, T., & Li, X. Y. (2020). PatronuS: A System for Privacy-Preserving Cloud Video Surveillance. IEEE Journal on Selected Areas in Communications, 38(6), 1252-1261.

[9] Zhou, L., Yan, W. Q., Shu, Y., & Yu, J. (2018). CVSS: A cloud-based visual surveillance system. International Journal of Digital Crime and Forensics (IJDCF), 10(1), 79-91.

[10] Mabrouk, A. B., & Zagrouba, E. (2018). Abnormal behavior recognition for intelligent video surveillance systems: A review. Expert Systems with Applications, 91, 480-491.

[11] Assante, M., Candela, L., Castelli, D., Cirillo, R., Coro, G., Frosini, L., & Sinibaldi, F. (2019). The gCube system: delivering virtual research environments as-a-service. Future Generation Computer Systems, 95, 445-453.

[12] Kim, H., Cha, Y., Kim, T., & Kim, P. (2020, January). A study on the security threats and privacy policy of intelligent video surveillance system considering 5G network architecture. In 2020 International Conference on Electronics, Information, and Communication (ICEIC) (pp. 1-4). IEEE.

[13] Abdalla, P. A., & Varol, C. (2020, June). Testing IoT Security: The Case Study of an IP Camera. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

[14] Zhigalov, K., & Avetisyan, K. (2018). Using cloud computing technologies in IP-video surveillance systems with the function of 3d-object modelling. In ITM Web of Conferences (Vol. 18, p. 02004). EDP Sciences.

[15] DeviPriya, K., & Lingamgunta, S. (2020). Multi factor two-way hash-based authentication in cloud computing. International Journal of Cloud Applications and Computing (IJCAC), 10(2), 56-76.

[16] Gupta, B. B., & Badve, O. P. (2017). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications, 28(12), 3655-3682.

[17] Vlajic, N., Chowdhury, M., & Litoiu, M. (2019). IP Spoofing in and out of the public cloud: from policy to practice. Computers, 8(4), 81.

[18] Mishra, P., Verma, I., & Gupta, S. (2020). KVMInspector: KVM Based introspection approach to detect malware in cloud environment. Journal of Information Security and Applications, 51, 102460.

[19] Kalbo, N., Mirsky, Y., Shabtai, A. and Elovici, Y., 2020. The security of ip-based video surveillance systems. Sensors, 20(17), p.4806.