Network-based Active Defense for Securing Cloud-based Healthcare Data Processing Pipelines

Vaibhav Akashe, Roshan Lal Neupane, Mauro Lemus Alarcon, Songjie Wang, Prasad Calyam
Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO, USA
{vva8yb, neupaner, lemusm, wangso, calyamp}@umsystem.edu

2021 International Conference on Computer Communications and Networks (ICCCN) | 978-1-6654-1278-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCCN52240.2021.9522267

***Abstract*—Active defense schemes are becoming critical to secure cloud-based applications in the fields such as healthcare, entertainment, and manufacturing. Active defense mechanisms in cloud platforms need to be robust against targeted attacks (such as Distributed Denial-of-Service (DDoS), malware, and SQL injection) that make servers unresponsive and/or cause data breaches/loss, which in turn can cause high impact especially for healthcare applications. In this paper, we present a novel network-based active defense mechanism viz., "defense by pretense" that uses real-time attack detection and creates cyber deception e.g., by redirecting attacker's traffic to quarantine machines and sending spoofed responses to attacker for cloud-based healthcare data processing applications. We implement our active defense mechanism by creating a realistic testbed on AWS cloud platform featuring the Observational Health Data Sciences and Informatics (OHDSI) framework for protected health data analytics with electronic health record data (SynPUF) and COVID-19 publications (CORD-19). Our evaluation experiments show the need and effectiveness of our active defense mechanism against targeted resource and data exfiltration attacks. We compare our active defense system against state-of-the-art active defense works, and our results show that our system is cost-effective, scalable and easy to deploy for active defense.**

***Index Terms*—Active defense, Cybersecurity Analytics, Healthcare Data Application, Threat Risk Assessment.**

I. Introduction

Active defense [1] is a proactive cybersecurity strategy that involves creation of dynamic management or even offensive measures to outsmart adversaries in order to make cyber-attacks difficult to execute. Using intelligent detection systems and defense solutions such as honeypots [2] and machine learning algorithms, active defense can be performed to slow down attacks and derail attackers at an early stage so that they cannot proceed with their plan, increasing the probability that they will expose their presence or reveal their attack vector. Thus, active defense schemes gain threat intelligence on targeted attacks and enable organizations to understand the nature of attacks, create robust defenses and also prevent recurrence of attacks.

Active defense implementations in cloud platforms feature out-of-the-box Intrusion Detection Systems (IDS) or leverage high-performance computing engines with defense tools that can actively monitor benign/attack traffic at a high-scale. However, active defense mechanisms in cloud platforms need to be robust against targeted attacks (such as DDoS, malware and SQL injection) whose impact can be amplified due to the elastic resource nature of cloud platforms. Particularly, there are critical challenges in securing healthcare applications with active defense schemes to avoid issues with availability or data breaches/loss, while also providing solutions that are cost effective, efficient, and timely [3]. Healthcare applications with data processing pipelines handle critical data such as Electronic Health Records (EHR), and sensitive personal health related data generated through medical devices. There have been prior works on securing EHR data in cloud-based platforms using Blockchain-based solutions [4] or through access control mechanisms based on the lattice model [5]. There have been proposals for attribute-based encryption access control, homomorphic encryption, and storage path encryption to improve privacy and security in healthcare applications [6]. However, to the best of our knowledge, none of the prior works have focused on active defense involving making use of dynamic management or offensive strategies, particularly relating to healthcare data processing pipelines orchestrated in cloud platforms.

In this paper, we present a novel network-based active defense mechanism viz., "defense by pretense" that uses real-time attack detection and creates cyber deception for cloud-based healthcare data processing applications. Our work builds upon prior work on the Dolus 'defense by pretense' system [7] which sits on a cloud network to perform tasks to intelligently detect and mitigate targeted attacks such as DDoS and Advanced Persistent Threats (APTs) in cloud platforms. Dolus uses a 'defense by pretense' active defense strategy that creates cyber deception by leading attackers into experiencing a false sense of success while a robust co-operative defense solution is being designed to mitigate attack impact or even dis-incentivize the attacker to continue a targeted attack. The cyber deception utilizes elastic capacity provisioning via use of Quarantine Virtual Machines (QVMs) that handle redirected attacker's traffic and increase threat intelligence collection. Our main contribution in this work is to extend the Dolus system for securing an open-source Observational Health DataSciences and Informatics (OHDSI) framework [8], which is used by major healthcare organizations (e.g., Cerner, university/private hospitals) as part of their healthcare data processing pipelines. OHDSI was developed to facilitate data

Project sponsored by National Security Agency under Grant/Cooperative Agreement Number H98230-20-1-0297. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

pipelines that combine data from multiple healthcare data sources to perform research for the advancement of medical sciences and to foster success of healthcare organizations. In addition to presenting a threat model using the Microsoft STRIDE methodology [9], we assess the vulnerability of healthcare data pipelines for targeted attacks by performing a risk assessment using the NIST guidelines [10] that informs our *OHDSI-Dolus* system design.

We evaluate our *OHDSI-Dolus* system design by creating an experimental Amazon Web Services (AWS) testbed hosting a realistic OHDSI setup for protected health data analytics with electronic health record data (SynPUF) and publications data (CORD-19) related to COVID-19 [8]. Our testbed features load balancers, IDS for active monitoring of attack traffic [11] and QVMs in order to detect an attack in real-time, and perform active defense using Dolus's cyber deception principles. Our experiment results show how we are able to successfully detect targeted attacks such as e.g., DDoS and create redirection of attack sources to QVMs. As a response from QVM, we successfully initiate a defense by pretense by sending fake HTTP responses and honey files from the decoy application to attackers mimicking the OHDSI application, which creates a false sense of success for the attackers.

The remainder of the paper is organized as follows: Section II discusses related work on IDS and active defense. Section III details the OHDSI framework for healthcare data processing pipelines and the associated application threat model along with an assessment of risks. Section IV presents the proposed OHDSI-Dolus mechanism for detection and defense of security threats on healthcare data processing pipelines. Section V presents performance evaluation of the OHDSI-Dolus. Section VI concludes the paper.

II. Related Work

A. Intrusion Detection Systems

Many prior works have addressed detecting security threats in cloud environments by using a variety of IDS techniques that utilize pattern recognition and machine learning concepts. The study presented in [12] provides an extensive review on cloud computing focusing on security gaps, and proposes a proactive machine learning based threat detection model. Similarly, authors in [13] propose a learning-based IDS to detect network-based intrusion in cloud platforms. Particularly, DDoS attacks pose serious threats to cloud-hosted services. Studies presented in [14]–[16] detail detection of DDoS attacks, and studies in [17]–[20] present techniques for detection of APTs, including attacks such as malware, botnets, data breach and data scraping.

Coupled with these emerging techniques, IDSes tend to be effective against detecting targeted attack threats. The work in [11] presents a comprehensive review about IDS and a study in [21] outlines current need for an advanced novel IDS approach additionally studies in [22] detail many host-based and network-based IDS techniques that are widely used by enterprises in both their data centers, as well as in their cloud-hosted application environments.

Nevertheless, there are only a few prior works such as [23] and [24] that present active defense techniques for healthcare applications in cloud environments. Our work presents a novel attack detection and active defense mechanism to mitigate cyber threats especially against cloud-based healthcare data processing pipelines. Our work takes advantage of services provided by AWS and network-based IDS, which can be used to monitor traffic and alert/block traffic flagged as suspicious. Our OHDSI-Dolus mechanism presents active defense against threats by initiating a pretense to deceive the attacker, which is scalable, cost-effective and easy-to-deploy in public cloud environments.

B. Active Defense

There are many prior works involving different kinds of cyber deception to trick the attacker and defend against threats. For example, the work presented in [22] proposes the use of system agents to launch on-demand honeypot VMs with enhanced VM introspection techniques. Another study in [25] uses the concept of a 'honey patch' to make a patched server reply to an adversary in a similar fashion to the way a non-patched server would. It then produces a container that appears to be a vulnerable system – but with redacted information hidden from the adversary, which helps to avoid leaking of sensitive information.

Studies such as those in [23] propose prevention strategies against DDoS attacks targeting eHealth clouds. Their approach involves detection of malicious activity to alert system administrator and subsequently blacklist the attacker's source address to block communications from the adversary. Similarly, the study in [24] proposed an active defense mechanism against data ex-filtration attacks in SaaS clouds by using a technique that matches the default identifier i.e., MAC address with the embedded identifier within the file. If the MAC address does not match, a corresponding decoy document (i.e., a honey file) is returned. Additionally, the framework in [26] involves an active defense strategy that uses decoys of real system components to obfuscate the network and in turn make it harder for a potential adversary to identify the real components. In our recent work on Dolus [7], we developed a defense by pretense system that blacklists the attacker upon detection, and then redirects the attacker to an alike QVM server that pretends to run as the real application server, resulting in the attacker's false sense of success. Dolus takes advantage of pretense theory and is established upon works in [27] and [28] that incorporate principles of of child pretense play in the field of psychology.

In this work, we adapt Dolus for OHDSI in AWS as a novelty, and create an active defense scheme that can be used by major healthcare companies such as Cerner EHR in HealtheDataLab products, and in OHDSI-like deployments at many university/private hospitals. Specifically, we show how active defense strategies can address security gaps in healthcare data processing pipelines that are hosted on cloud platforms for access to research/clinical use cases.

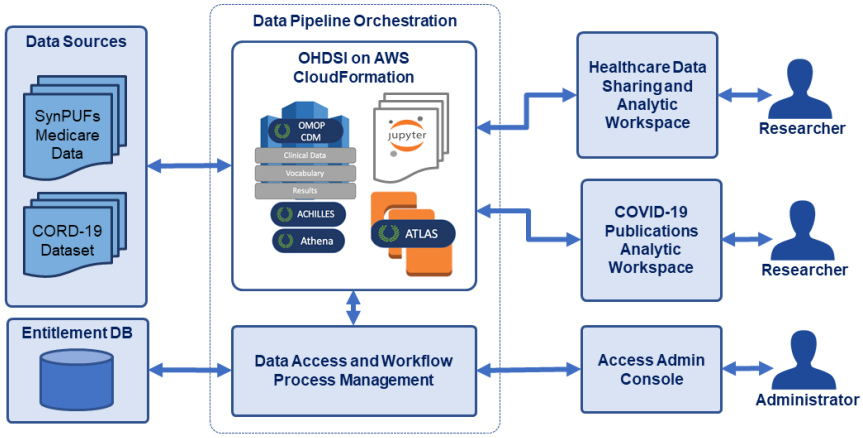

Fig. 1: Overview of the data pipeline orchestration built on top of the OHDSI on AWS infrastructure.

III. Cloud-based Healthcare Data Processing

In this section, we first describe OHDSI, which an open-source framework used to build cloud-based data processing pipeline systems. Following this, we present an application threat model using the Microsoft STRIDE model [9] for OHDSI-based healthcare applications. Lastly, we present the risks associated with the threats presented by the STRIDE model using the NIST risk assessment guidelines [10].

A. OHDSI Overview

Healthcare data consumers (e.g., clinicians and researchers) require access to massive datasets which are usually residing in multiple and disparate data sources. This creates many challenges for the data consumers to access and compile the data required to conduct research and make timely decisions. Data processing pipelines are increasingly being used to combine data from multiple sources, allow access to multiple users, and include multiple data analytic tools to orchestrate data aggregation, processing and visualization processes. To facilitate the orchestration of such data pipelines, exemplar technologies, such as OHDSI [29] have been adopted for use in cloud environments by healthcare organizations.

To develop our network-based active defense solution, we deployed the open-source OHDSI on the AWS platform as illustrated in Figure 1. The OHDSI on AWS deployment provides an enterprise class, multi-user, and scalable healthcare data sharing and analytics functionality [8]. Its main components include a Common Data Model (CDM) based on the OMOP-CDM schema, which is deployed on an AWS Redshift data warehouse. The CDM schema allows the integration of disparate data-sources into a common format (model) and common representation (terminology, vocabulary, coding), allowing the definition and execution of standard analytic processes. Other OHDSI components include out-of-the-box open-source analytic tools such as: (i) ATLAS, a web-based application for researchers to conduct analyses on data loaded to the OMOP-CDM through creation of cohorts based on drug exposure or diagnosis of a particular condition. The cohort results are visualized in the tool's user interface, or stored in a relational repository to be used by other analytic tools; (ii) ACHILLES, an application used to analyze the database hosting the CDM and evaluate data quality; (iii) ATHENA, a tool that is used to generate and load standardized data vocabularies into the CDM repository. Once data is available in the CDM, evidence knowledge can be generated using the included analytic tools and models available in the workspace available via Jupyter Notebooks or R-Studio.

Our cloud-based service extends OHDSI through integration of the following new components we have developed: (i) a basic role-based user access and workflow management component to keep control on the authentication and authorization of the data, and ensure data privacy and security compliance; this functionality allows users to submit data requests, which are fulfilled by the system based on the role-based user access privileges; and, (ii) the functionality that allows users to perform publications analytics (considering hundreds or thousands of articles knowledge pattern mining in CORD-19 dataset) and big data analytics (considering millions of patient related records in SynPUF dataset) relevant to COVID-19. The original OHDSI features are complemented by the above two components and the result is a flexible platform for researchers to analyze data with open-source tools, and find correlations as well as gain insights, all within the same platform.

Although our cloud-based healthcare data processing pipeline service is functional, the critically and sensitivity of the data it contains and the always increasing sophistication of targeted attacks such as DDoS attacks and APTs, drive the need for formalising a robust and reliable active defense mechanism. Our goal of the OHDSI-Dolus effort is to develop a general framework for detection and active defense against serious threats that broadly impact cloud-hosted healthcare data analytics applications [30]–[32].

B. Application Threat Model

To better understand the threats and their imposed risks to the OHDSI application use cases, we use the Microsoft STRIDE methodology [9] to create an application-level threat risk model. We organised the attacks against the OHDSI application into Loss of users' trust, Loss of confidentiality, Loss of availability and Loss of integrity.

- **S**poofing: IP spoofing Example - An attacker can alter the IP packet to gain access to the OHDSI application server as an authorized user. Successful IP spoofing attack can cause loss of trust for users and loss of confidentiality in the OHDSI system.
- **T**ampering: Data Alteration Example - Malicious user can spoof queries to retrieve and modify data and can cause loss of integrity in the OHDSI system.
- **R**epudiation: Example - Attacker can impersonate a user to retrieve and modify data that can lead to loss of confidentiality and integrity for OHDSI system users.
- **I**nformation Disclosure: SQL injection/Malware infection Example - Attacker can perform a SQL injection attack to affect the database or gain access to unauthorized data. Also presence of malware on system can lead to leakage of users' data. Such attacks can cause loss of confidentiality and integrity for OHDSI application users.
- **D**enial of Service: Example - Attacker can perform multiple SQL queries to overwhelm the database system, which can lead to loss of availability for OHDSI users.
- **E**levation of Privilege: Data Tampering Example - An attacker can tamper data or even delete data on the network, which can then lead to loss of integrity for data, and loss of availability for the OHDSI users.

Exploitation of potential vulnerabilities such as DDoS, Malware/SQL injection identified by our threat model pose major threats to healthcare data processing pipelines. These vulnerabilities may result in possible risks to patient safety and theft or loss of health related information, which have serious consequences in the healthcare organization operations.

C. Risk Assessment

Following the threat modeling study performed using the STRIDE methodology, we use the methodology in the NIST risk assessment guideline [10] to calculate the potential risk levels for various threats impacting the OHDSI in AWS application. The NIST methodology populates the impact values and likelihood values for specific threats being considered. The impact values are derived from assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability for any information type due to security threats. The likelihood values are a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability of the threats. Following this, the overall risk values are calculated by factoring the likelihood and impact scores, which are finally normalized into a quantitative scale of 0-10. These ranges for scales are: 9-10 indicating very high risk, 7-8 indicating high risk, 4-6 indicating moderate risk, 1-3 indicating low risk, and 0 indicating very low level of risk. We evaluate the risk levels for different threat events in the STRIDE model based on the NIST methodology and present the details of the results in Section V (Performance Evaluation) of this paper. Our risk assessment guides the design principles for our Dolus-OHDSI active defense system design.

IV. OHDSI-Dolus System Design

In this section, we present an overview of our attack detection and defense steps in our OHDSI-Dolus architecture. Following this, we describe how the pretense theory is used for the active defense mechanism in our OHDSI-Dolus system.

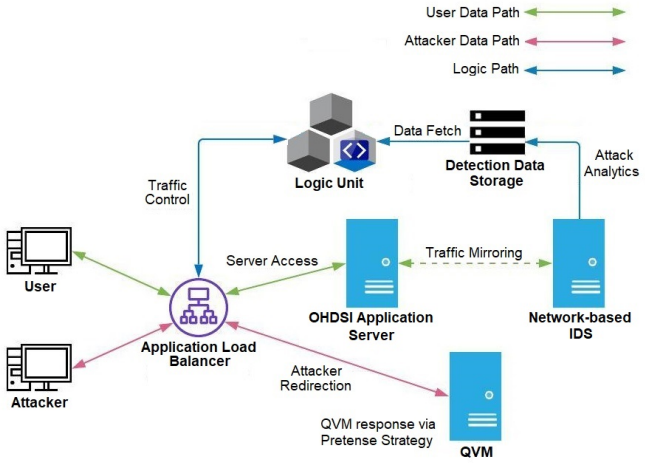

Fig. 2: Illustration of proposed OHDSI-Dolus system where an attacker is tricked by redirection of malicious traffic to a quarantine VM for pretense, while the legitimate users can access the OHDSI hosted data sets.

A. OHDSI-Dolus Architecture

Figure 2 shows the OHDSI-Dolus system with physical architecture components for initiation and maintenance of pretense in the event of a targeted attack. The OHDSI-Dolus takes advantage of elastic compute services provided by cloud service providers, particularly the application load balancer and on-demand provisioning of virtual instances. We place the application load balancer in between user and the cloud resources that are deployed in a virtual private cloud (VPC).

When the IDS suspects a network intrusion or cyber-attack event, then a *Quality of Detection* (QoD) protocol gets triggered in the OHDSI-Dolus system. If QoD value is above a certain threshold which validates that an intrusion or cyber-attack event has indeed been detected accurately, then the Dolus pretense is initiated and maintained.

B. Active Defense Methodology

In the following, we first describe the attack detection algorithm and subsequently provide details of the OHDSI-Dolus QoD calculation scheme. Lastly, based on the success measure of the QoD value, we present how the active defense i.e., defense by pretense is invoked that involves a sequence of steps to minimize the threat risk and record the blacklisted IP addresses for further analysis/traceback.

1) Ensemble Learning: We use the ensemble learning methodology to determine the accuracy of our attack detection. Network traffic is collected through the network-based IDS in OHDSI-Dolus when legitimate users and attackers try to access the cloud-hosted OHDSI services. Users interact with the OHDSI application server by requesting different

healthcare related data resources. We monitor the attack traffic targeted to the data processing pipeline server and capture e.g., bytes transmitted, number of packets, source, and destination IP address. Subsequently, the QoD is calculated by taking attack-related factors into consideration as well as the based on the complexity/effectiveness of the detection mechanisms evidenced by e.g., data sanity, and detection time/accuracy. The formula to calculate the QoD value is as follows:

$$QoD = \frac{1}{n}\sum_{i=1}^{n}\frac{a_i}{t_d} \tag{1}$$

In the QoD formula, the ($a_i \in [0,1]$) refers to the accuracy of the ensemble learning model (dependent also on data sanity) used to identify the cyber-attacks. t_d is the time taken (in seconds) for the machine learning model to detect the attacks and n represents number of test iterations in the evaluation. These QoD values ranges from 0 to 100, hence we normalize these values into [0,10] range by dividing the values by 10. If QoD values are above non-zero, the pretense initiation and maintenance is invoked, however the administrator may set a higher threshold as suited in accordance with the active defense policies of the healthcare organization.

We use Frenetic (an open-source software-defined network controller platform [7]) to execute Python scripts that identify suspicious packets, gather attack patterns in order to redirect packets to pertinent QVMs. IP addresses of the attackers are then blacklisted by updating a corresponding network policy. We characterize the attack data for DDoS by measuring e.g., the total bytes transferred, rate of transfer, connections made, and attack duration. This allows us to get dynamic "suspiciousness scores" of attackers and their domain nodes for targeted attacks. To emulate a DDoS attack, we exhaust the targeted application using a SlowHTTPTest [33] and thereby cause random changes in e.g., number of packets, and attack times. We also perform event-based simulations to get different suspiciousness scores for attacks as follows:
Destination suspiciousness for trace t:

$$dst_i = w_{dst} \times \frac{numDst_i - numDstMin_i}{numDstMax_i - numDstMin_i} \tag{2}$$

Flow suspiciousness for trace t:

$$flows_i = w_{flows} \times \frac{numFlows_i - numFlowsMin_i}{numFlowsMax_i - numFlowsMin_i} \tag{3}$$

Bytes suspiciousness for trace t:

$$bytes_i = w_{bytes} \times \frac{numBytes_i - numBytesMin_i}{numBytesMax_i - numBytesMin_i}; \quad w_{dst} \in [0.0, 1.0]; w_{flows} \in [0.0, 1.0]; w_{bytes} \in [0.0, 1.0] \tag{4}$$

Device suspiciousness for trace t:

$$ss_i = \sqrt{\frac{dst_i^2 + flows_i^2 + bytes_i^2}{3}} \tag{5}$$

We calculate the ss values based on the captured network traces using three main features: destinations, flows, and bytes. For each attacker node i on the network, and for trace t, we assume the weight parameters i.e., w_{dst}, w_{flows}, w_{bytes} to be equal to 1 in a general case of suspiciousness score calculations. Also, the *Min* and *Max* values are assumptions made per attack nodes based on the expected behavior of the network flows corresponding to user hosts' traffic.

2) OHDSI-Dolus Pretense Initiation and Maintenance: The entire procedure of our OHDSI-Dolus interactions involving sequential steps are shown in Figure 3 for classification of user traffic and attacker traffic as well as creation of the attacker quarantine with active defense through initiation and maintenance of pretense. Firstly, a user from a remote network location accessing the cloud-based healthcare data applications makes requests to the listener based on rules configured in OHDSI. The listener then redirects the user's traffic to the target application server. An IDS placed inside the VPC is used detect network intrusions or any malicious activities by sniffing network traffic flows in real-time from the user to the OHDSI application server. If network intrusion or malicious activity is detected, the IDS will alert the system administrator, and then the adversary's IP address will be blocked at the application server. After blocking attackers IP address, the listener on the load balancer will automatically redirect the traffic coming from the attacker to a Quarantine Virtual Machine (QVM) by using configured rules. Finally, by initiating pretense, the attacker will be deceived by being presented with decoy honey files of protected data to give a false sense of success.

V. Performance Evaluation

In this section, we first describe the experimental testbed setup based on OHDSI [8] deployed on AWS. We use this testbed for the evaluation of our novel OHDSI-Dolus against state-of-the art active detection and defense systems. Next, we discuss the results of a risk assessment based on threats analyzed from STRIDE model to build active defense mechanism against a high risk threat i.e., DDoS attack. Following this, we present the QoD results for detection of threats against the OHDSI application using machine learning models for the DDoS attack. In this context, we compare the performance of the our OHDSI-Dolus with state-of-the-art active defense mechanisms that have the potential to be used for protection of OHDSI-like systems. Lastly, we present a qualitative evaluation for the active defense approach to lure the attacker to a QVM mimicking the OHDSI application.

A. Experimental Testbed Setup

Our OHDSI on AWS testbed set up is shown in Figure 4. There are three servers, including the application (OHDSI Server), the network-based IDS, and the QVM. All of these servers are set up using EC2 virtual instances, and are configured within the same virtual private cloud as private nodes, i.e., only accessible from other nodes within the testbed. While the data from the application and the QVM can be accessed by the users (benign or malicious) depending on their request type, the network-based IDS server is used solely for network traffic mirroring and for analysis involving attack detection. Our

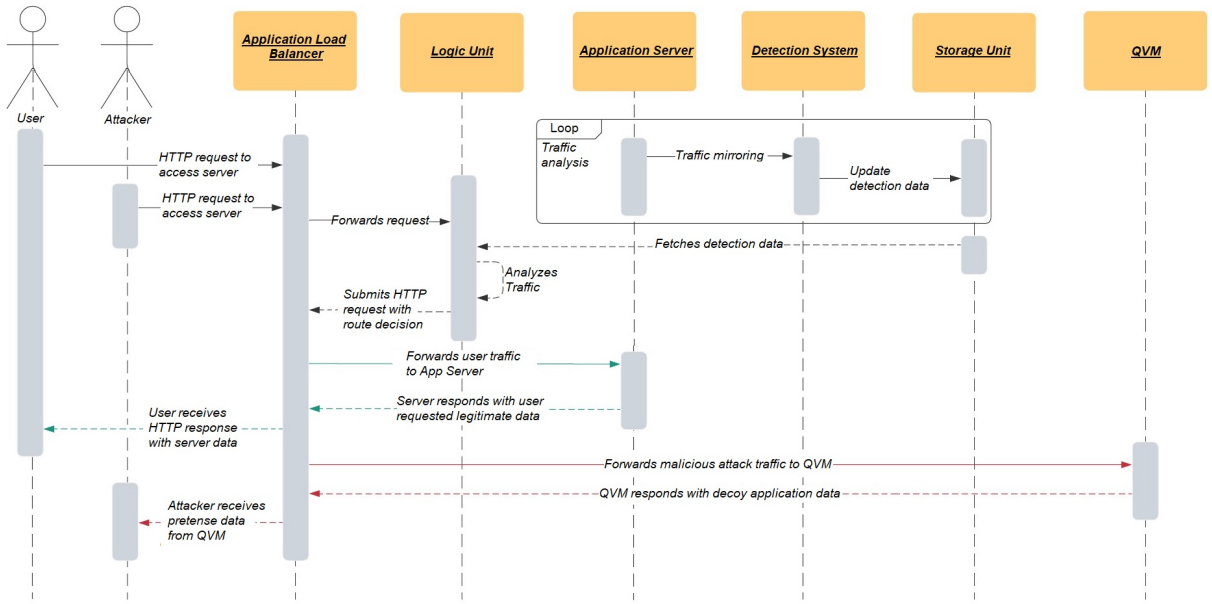

Fig. 3: Sequence diagram of OHDSI-Dolus defense system interactions for network traffic analysis and attack detection, along with attacker quarantine and active defense through initiation and maintenance of pretense.

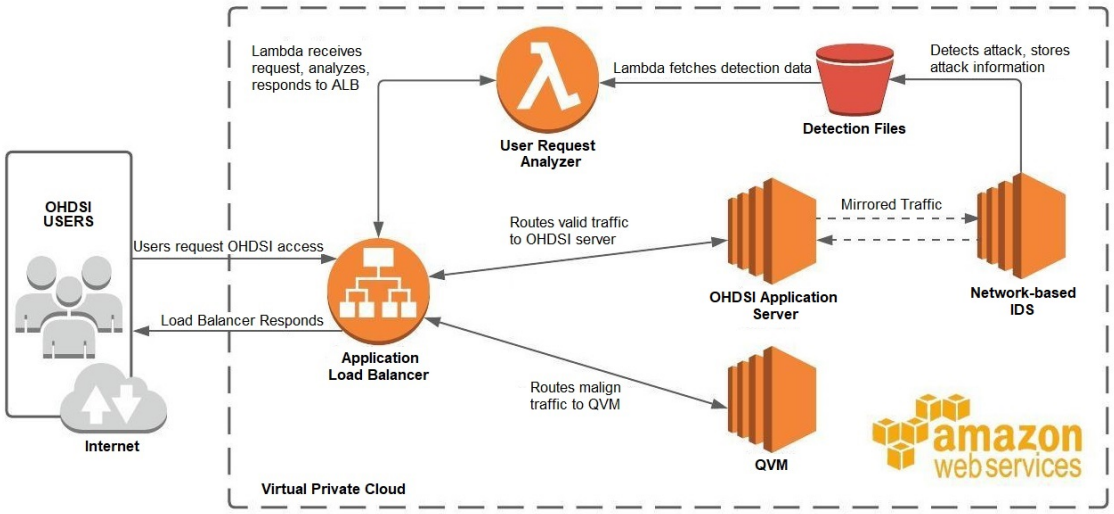

Fig. 4: AWS testbed used to evaluate OHDSI-Dolus for targeted attacks.

testbed also includes an Application Load Balancer (ALB), the only public-facing component in the testbed. The ALB works as a wrapper component which performs both the logic check and acts as a distributor depending on the load it receives, through which users can access the private servers by using their public IP addresses.

The ALB has three listener rules, each pointing to a target server or AWS service and has a different priority. The first listener rule points to a Lambda function as a target which has the highest priority of all the rules. This Lambda function receives all the HTTP requests when users try to access the OHDSI application server, and will obtain the source IP of the user trying to access the server. Lambda function also fetches the blacklisted IP list from the AWS S3 bucket to match with the previously blacklisted attacker's IP addresses. The Lambda function then maps the source IP of the user with this list to conclude whether or not the traffic that the ALB is receiving is coming from an attacker IP. Once such a conclusion is made, the Lambda function responds to the ALB with an HTTP response that provides the re-route information which consists of the port numbers that the ALB uses to forward the traffic to either the OHDSI application server or to the QVM.

After receiving response from the Lambda function, the ALB will re-route traffic to the respective OHDSI application server or to the QVM. The other two listener rules point to the application server and the QVM. There is no need

to prioritize these rules because both of them use different conditions, which will make them both exclusive of each other. For evaluation purposes, we use different ports to determine which server to re-route when a certain rule is matched.

The network-based IDS server constantly monitors the traffic for the OHDSI application server that has been mirrored to the network-based IDS using VPC traffic mirroring. It checks to categorize if an attack has occurred based on the network connection patterns and our attack detection logic. Upon detection of an attack, the network-based IDS server creates a list of IPs to be blacklisted and appends them to a database to keep track of the IPs that need to be re-directed to the QVM whenever a request is made from related IPs.

B. Risk Assessment Results

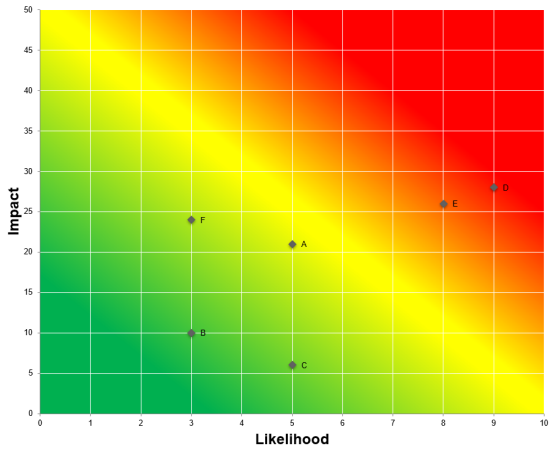

Fig. 5: Heat map visualization of risk levels for different STRIDE categories A - F

We evaluate the risks of various threat events in the STRIDE categories based on the NIST guidelines [10]. As shown in Table I, the risk levels for different threats against the OHDSI healthcare application varies in the STRIDE model due to their distinct potential impact and likelihood values. The risk value of Data Alteration event under the Tampering category is the lowest among all the threats in the STRIDE categories. Due to the fact that the likelihood of tampering is relatively low (score of 3), which leads to a minimal chance of occurrence. Recently many techniques have been developed to enforce encryption of Data-at-Rest and Data-in-Transit. In addition, file integrity monitoring systems can be placed to deal with tampering threats, which also contributes to the low likelihood value in this category.

On the other hand, the SQL injection/Malware infection under the Information Disclosure category and the DDoS attack under the Denial of Service are the two highest risk categories, with risk levels of 9 and 8, respectively. This is due to the fact that the impact and likelihood are both high in these two categories relating to modern healthcare data processing applications, as opposed to Data Tampering, which also has a high impact but a very low likelihood of occurrence. The rest of the STRIDE categories have risk values that lie in between the Tampering and Information Disclosure categories, indicating that they represent moderate threats in the healthcare data processing pipeline applications. The risk levels are also visualized in the heat map in Figure 5, where the red color represents high risk, green color represents low risk, and yellow color represents medium risk in the relative STRIDE categories A - F.

C. Detection Results

We present the performance of our OHDSI-Dolus considering an exemplar attack with a high risk level, i.e., the DDoS attack, which is one of the most prevalent attacks in the STRIDE categories with regarding to OHDSI health data processing applications. Recall that the QoD parameter determines the overall the accuracy and speed of cyber-attack detection impacting the OHDSI healthcare application. We evaluate the QoD metric based on the ensemble learning accuracy and time taken for the models to run in OHDSI-Dolus, and compare the performance with state-of-the-art detection schemes in [23] and [34].

To identify potential network intrusion or a cyber-attack event, we setup our network-based IDS in our VPC on an EC2 instance. We use the ensemble learning based detection scheme used as part of the OHDSI-Dolus related IDS implementation. We take advantage of the AWS VPC traffic mirroring service to mirror the network traffic flowing into our VPC that is routed to the IDS. We also used the AWS Cloud Watch service to monitor the OHDSI application server's network flow i.e., mirrored network traffic, as shown in Figure 6. We can see from the graph, the different levels of network packets mirrored from the OHDSI server during the EC2 instance initiation, OHDSI application server launch and during user data query.

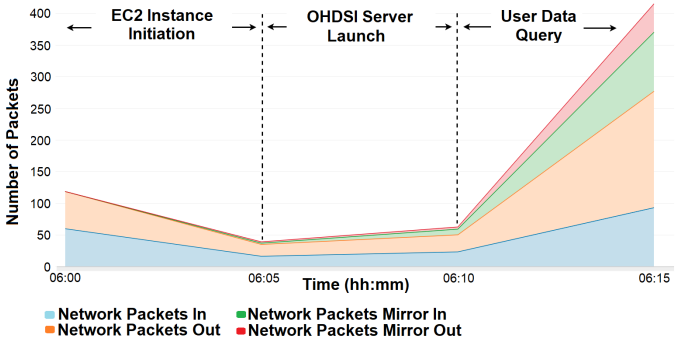

Fig. 6: Dolus mirroring OHDSI server traffic at different stages for analysis and detection as viewed with AWS Cloud Watch.

To evaluate the performance of our OHDSI-Dolus mechanism, we compare its performance with other DDoS detection mechanisms presented in [23] and [34]. We primarily choose these works for comparison since the studies presented take advantage of ML based attack detection against cloud-based systems. The work in [23] presents CS_DDoS, a framework for detection and prevention of DDoS attack in cloud environments. In CS_DDoS, the incoming packets are classified using several machine learning models to decide whether the sources are associated with a genuine client or an attacker

TABLE I: Threat events related to OHDSI application with NIST-based guideline [10] used for risk calculation.

Category	Threat Events	Application Impact	STRIDE Threat	Likelihood	Impact	Threat Risk
A	IP spoofing	An attacker can alter the IP packet to gain access to Healthcare application server as authorised user.	Spoofing	5	21	Moderate (5)
B	Data Alteration	Malicious user can spoof the query to retrieve unauthorized data.	Tampering	3	10	Low (3)
C	Man-In-Middle attack	Attacker can impersonates as a user to retrieve unauthorized data.	Repudiation	5	6	Moderate (4)
D	SQL injection/Malware infection	An attacker can perform an SQL injection attack to affect the database or to gain access to unauthorized data. Also, the presence of malware on the system can lead to leakage of users' unauthorized data.	Information Disclosure	9	28	Very High (9)
E	DDoS Attack	Attacker can perform multiple SQL queries to overwhelm the database system.	Denial of Service	8	26	High (8)
F	Data Tampering	An attacker can tamper data because there's no integrity protection for data on the network.	Elevation of Privilege	3	24	Moderate (4)

TABLE II: Comparison of OHDSI-Dolus performance with state-of-the-art active defense mechanisms that have the potential to be used for protection of cloud-based healthcare data processing pipelines.

	CS_DDoS Detection/Defense [23]	Deception based Defense [24]	OHDSI-Dolus Detection/Defense
Features	ML-based detection attacks and prevention using IP blacklisting.	Detection using detection engine and prevention by generating decoy documents.	Detection of cyber-attacks by ML-enabled network-based IDS and mitigation by initiating Pretense.
Advantages	Able to reduce bandwidth consumption by early detection.	Detection without relying on cloud providers using cyber deception.	Scalable, Cost-effective and easy to deploy.
Suitable for	Early DDoS attack detection.	Generation of decoy objects based on input.	The scalable and cost-effective mechanism for early detection and mitigation.
Limitations	Detection fails if attacker is using spoofed IP's.	Detection scheme can be spoofed by spoofing MAC addresses.	The proposed scheme is based on relevant services provided by cloud providers.

based on feature matching. Authors in [34] propose to use the extreme gradient boosting (XGBoost) as the detection method in a cloud platform with software-defined networking. The detection results validate that XGBoost performs relatively better than CS_DDoS with higher accuracy, lower false positive rate, fast-speed and has scalability in detection of DDoS attacks.

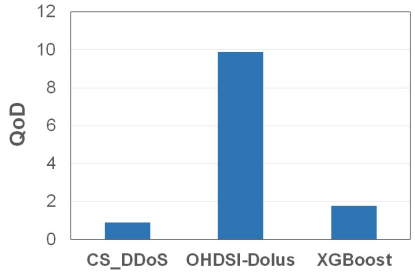

Fig. 7: Quality of Detection (QoD) results of DDoS attack detection based on accuracy and time taken by state-of-the-art detection mechanisms in comparison with our OHDSI-Dolus.

Figure 7 shows that our healthcare data processing pipeline, the OHDSI, equipped with OHDSI-Dolus outperforms the state-of-the-art mechanisms viz., CS_DDoS and XGBoost in DDoS attack detection. The comparison is done using the accuracy over time QoD calculation in Equation 1. In the results, we average the accuracy of different machine learning models used across the average of time they took for the calculation for QoD as discussed in Section IV-B2.

D. Defense by Pretense Qualitative Evaluation

Upon detection of a DDoS attack, our OHDSI-Dolus system initiates attack mitigation by re-routing the network traffic from the attacker to the QVM. In the QVM, we successfully deployed a decoy service that mimics a running OHDSI application server. This server serves dummy honey files that are intended only to be provided to attackers to maintain the pretense, and the attackers are led to believe they have gained access to the main OHDSI application server, while in reality they have been deceived.

We perform qualitative comparison between our OHDSI-Dolus system with the defense scheme presented in the works of [23] and [24]. The CS_DDoS framework in [23] uses IP blacklisting to mitigate DDoS attacks on a cloud platform. In contrast, [24] proposes a mechanism to mitigate data exfiltration attacks using deception in cloud platforms. Whenever a download or sharing request is made, if the host MAC address does not match the embedded identifier within the file, the corresponding decoy document (instead of the actual file) is returned to deceive the attacker.

Table II summarizes the main features of our OHDSI-Dolus and qualitatively compares it with two state-of-the-art mechanisms i.e., CS_DDoS [23] and Deception based defense [24] in terms of the features, advantages, use case spectrum, and their limitations. We show that our OHDSI-Dolus scheme is more scalable, cost-effective, and easier to deploy as we take advantage of low-cost and most commonly used services provided by public cloud providers. Thereby, using our OHDSI-Dolus, the attackers can be effectively engaged with a QVM that helps to gain more threat intelligence information on the attacker and the corresponding attack vectors.

VI. Conclusion

In this paper, we developed a novel cloud-based attack detection and active defense mechanism for a cloud-hosted healthcare application with a protected data processing pipeline. We analyzed unique attack surfaces in the healthcare data processing pipelines using the Microsoft STRIDE methodology and performed a related risk assessment based on the NIST guidelines to identify the prominent threats such as DDoS attack and APT. Based on the the risk assessment, we developed a design for an active defense solution i.e.,

OHDSI-Dolus that can be integrated with healthcare data processing pipelines. Our OHDSI-Dolus architecture allows us to combine healthcare data from multiple sources, and mediates protected access from multiple users, while proving robust access to multiple data analytic tools to orchestrate data collection, processing, and visualization processes. Through active defense strategies, our OHDSI-Dolus system is capable of threat detection and provides threat mitigation services to effectively defend against targeted attacks in a robust manner. We showed how our OHDSI-Dolus system actually takes advantage of "defense by pretense" theory for mitigation of threats such as DDoS and APTs for cloud-based healthcare data processing pipelines by luring the attacker to quarantine virtual machine instances. Lastly, using a dataset related to the most prominent threat event i.e., DDoS attack that we noted in our risk assessment, we show how OHDSI-Dolus outperforms state-of-the-art defense mechanisms and can minimize suspected threat risks for cloud-based healthcare data processing pipelines effectively.

REFERENCES

[1] F. De Gaspari, S. Jajodia, L. V. Mancini, and A. Panico, "Ahead: A new architecture for active defense," in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*, ser. SafeConfig '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 11–16. [Online]. Available: https://doi.org/10.1145/2994475.2994481

[2] A. Mairh, D. Barik, K. Verma, and D. Jena, "Honeypot in network security: a survey," in *Proceedings of the 2011 international conference on communication, computing & security*, 2011, pp. 600–605.

[3] M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *Journal of medical Internet research*, vol. 13, no. 3, p. e67, 2011.

[4] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, pp. 1–8, 2016.

[5] D. R. Matos, M. L. Pardal, P. Adao, A. R. Silva, and M. Correia, "Securing electronic health records in the cloud," in *Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems*, 2018, pp. 1–6.

[6] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of Big Data*, vol. 5, no. 1, pp. 1–18, 2018.

[7] R. L. Neupane, T. Neely, P. Calyam, N. Chettri, M. Vassell, and R. Durairajan, "Intelligent defense using pretense against targeted attacks in cloud platforms," *Future Generation Computer Systems*, vol. 93, pp. 609–626, 2019.

[8] A. P. Mauro Lemus Alarcon, Roland Oruche and P. Calyam, "Cloud-based data pipeline orchestration platform for covid-19 evidence-based analytics," Submitted for publication.

[9] L. Jiang, H. Chen, and F. Deng, "A security evaluation method based on stride model for web service," in *2010 2nd International Workshop on Intelligent Systems and Applications*. IEEE, 2010, pp. 1–5.

[10] R. S. Ross, "Guide for conducting risk assessments (nist sp-800-30rev1)," *The National Institute of Standards and Technology (NIST), Gaithersburg*, 2012.

[11] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[12] M. T. Khorshed, A. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation computer systems*, vol. 28, no. 6, pp. 833–851, 2012.

[13] V. Kanimozhi and T. P. Jacob, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset cse-cic-ids2018 using cloud computing," in *2019 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2019, pp. 0033–0036.

[14] A. Aborujilah and S. Musa, "Cloud-based ddos http attack detection using covariance matrix approach," *Journal of Computer Networks and Communications*, vol. 2017, 2017.

[15] Z. He, T. Zhang, and R. B. Lee, "Machine learning based ddos attack detection from source side in cloud," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE, 2017, pp. 114–120.

[16] J. Choi, C. Choi, B. Ko, and P. Kim, "A method of ddos attack detection using http packet pattern and rule engine in cloud computing environment," *Soft Computing*, vol. 18, no. 9, pp. 1697–1703, 2014.

[17] J. Kim, T. Lee, H.-g. Kim, and H. Park, "Detection of advanced persistent threat by analyzing the big data log," *Advanced Science and Technology Letters*, vol. 29, pp. 30–36, 2013.

[18] P. Bhatt, E. T. Yano, and P. Gustavsson, "Towards a framework to detect multi-stage advanced persistent threats attacks," in *2014 IEEE 8th international symposium on service oriented system engineering*. IEEE, 2014, pp. 390–395.

[19] B. Binde, R. McRee, and T. J. O'Connor, "Assessing outbound traffic to uncover advanced persistent threat," *SANS Institute. Whitepaper*, vol. 16, 2011.

[20] J. Vukalović and D. Delija, "Advanced persistent threats-detection and defense," in *2015 38Th international convention on information and communication technology, electronics and microelectronics (MIPRO)*. IEEE, 2015, pp. 1324–1330.

[21] W. Stout, V. Urias, C. Loverro, and B. Anthony, "Now you see me now you don't: Advancing network defense through network deception." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2017.

[22] M. L. Bringer, C. A. Chelmecki, and H. Fujinoki, "A survey: Recent advances and future trends in honeypot research," *International Journal of Computer Network and Information Security*, vol. 4, no. 10, p. 63, 2012.

[23] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient ddos tcp flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[24] D. Wilson and J. Avery, "Mitigating data exfiltration in storage-as-a-service clouds," *arXiv preprint arXiv:1606.08378*, 2016.

[25] F. Araujo, K. W. Hamlen, S. Biedermann, and S. Katzenbeisser, "From patches to honey-patches: Lightweight attacker misdirection, deception, and disinformation," in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 2014, pp. 942–953.

[26] R. A. H. J. R.-M. B. S. T. C. Cifranic, Nicholas and G. Coca, "Decepti-scada: A cyber deception framework for active defense of networked critical infrastructures," *Internet of Things*, vol. 12, p. 100320, 2020.

[27] C. Baer and O. Friedman, "Children's generic interpretation of pretense," *Journal of experimental child psychology*, vol. 150, pp. 99–111, 2016.

[28] J. W. Van de Vondervoort and O. Friedman, "Young children protest and correct pretense that contradicts their general knowledge," *Cognitive Development*, vol. 43, pp. 182–189, 2017.

[29] G. Hripcsak, J. D. Duke, N. H. Shah, C. G. Reich, V. Huser, M. J. Schuemie, M. A. Suchard, R. W. Park, I. C. K. Wong, P. R. Rijnbeek *et al.*, "Observational health data sciences and informatics (ohdsi): opportunities for observational researchers," *Studies in health technology and informatics*, vol. 216, p. 574, 2015.

[30] B. Gupta and O. P. Badve, "Taxonomy of dos and ddos attacks and desirable defense mechanism in a cloud computing environment," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3655–3682, 2017.

[31] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: taxonomy and risk assessment," in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*. IEEE, 2017, pp. 112–120.

[32] P. Suryateja, "Threats and vulnerabilities of cloud computing: a review," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 3, pp. 297–302, 2018.

[33] (2011) S. Shekyan, SlowHTTPTest. Application Layer DoS attack. [Online]. Available: https://github.com/shekyan/slowhttptest/wiki

[34] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, "Xgboost classifier for ddos attack detection and analysis in sdn-based cloud," in *2018 IEEE international conference on big data and smart computing (bigcomp)*. IEEE, 2018, pp. 251–256.