# Smart Intrusion Detection on the Niger-Delta Oil Pipeline System

Hope Daniel Bango Computer and Information Science Universiti Teknologi Petronas (UTP) Seri Iskandar, Malaysia

Abstract— As critical components of global energy infrastructure, oil pipeline systems are prime targets for cyberattacks that can lead to operational disruptions, environmental hazards, and financial losses. Intrusion Detection Systems (IDS) play a pivotal role in safeguarding these systems by identifying and mitigating cyber threats. However, the complex and evolving nature of the threat landscape, coupled with the unique challenges posed by oil pipeline operations, necessitates a tailored approach to intrusion detection. This paper explores the intricacies of intrusion detection in the context of the Niger-Delta oil pipeline systems. It highlights challenges such as the dynamic operational environment, remote and dispersed locations, legacy systems, and the need for harmonizing intrusion detection with operational technology (OT) that leverages multiple security measures to protect oil pipelines control room's assets; It is intended to overcome most of the problems associated with the current oil pipeline monitoring system of the Niger-Delta by identifying the most efficient Machine Learning Algorithms and technological features to help curb the menace of vandalism, oil spillage and theft.

Keywords—Intrusion Detection; Oil pipelines; Machine Learning; Niger-Delta; Nigeria.

# I. INTRODUCTION

Nigeria has become West Africa's biggest producer of petroleum with close to over 2 million barrels (320,000 m3) per day are extracted in the Niger Delta, with an estimated 38 billion barrels of reserves. [1]

On the 23rd of June 2023, Aljazeera; an international 24-hour English-language news channel owned by the Al Jazeera Media Network reported new oil spill at a Shell facility in Nigeria which resulted in the contamination of farmland and a river, upending livelihoods in fishing and farming communities in the Niger Delta. It lasted for over a week and busted into the Okulu River - which adjoins other rivers and ultimately empties into the Atlantic Ocean. Such oil spillages have been a long endured environmental pollution caused by the oil industry and are frequent in the region due to the inefficiency of the current intrusion detection system, vandalism, and a lack of maintenance to the pipelines. Africa's largest economy overwhelmingly depends on the Niger Delta's oil resources for its earnings, but pollution from that production has denied residents access to clean water, hurt farming and fishing and heightened the risk of violence. This paper proposes an automated way to monitor the pipelines against any form of intruders from anywhere within the Niger-Delta as such instant prompting and reporting will curb oil theft and unnecessary vandalization of resources. [2]

## II. PROBLEM STATEMENT

The petroleum pipeline oil spillage in Nigeria presents a significant and persistent challenge that demands urgent attention. Despite numerous efforts of deploying Intrusion detection systems to detect anomalies, breaches, unauthorized activities on the system or report external physical disturbances on the pipeline's communication network and alert controllers and or security personnel about unauthorized access attempts along the pipeline to mitigate and prevent oil spills, diversion, or theft, Nigeria continues to experience frequent and devastating incidents of oil spillage that has led to extensive environmental degradation, contaminating water bodies, loss of productive agricultural lands, health hazards which ultimately affects the economy output of the nation as well as impacting the livelihoods of local farmers and communities as a result of the inefficiency of the current adopted intrusion detection system to detect at optimum when there is an anomaly/unauthorized access in the system as well as clearly differentiate a false alarm from an actual intrusion. This problem statement underscores the urgent need for a more comprehensive solution.





## A. Research Questions

Question 1: What Machine learning algorithm can be deployed for optimal detection of unauthorized access in the Niger-Delta oil pipeline system?

Question 2: What technological features can clearly differentiate an actual intrusion from a false alarm in the Niger-Delta oil pipeline system? Maintaining the Integrity of the Specifications

#### B. Research Objectives

1. To identify the most efficient Machine learning algorithm that can be employed for detecting intrusions and unauthorized activities in the Niger-Delta oil pipelines in Nigeria.

2. To identify and analyze the technological sensors that can effectively distinguish genuine intrusions from false alarms within the Niger-Delta oil pipeline system.

#### III. LITERATURE REVIEW

The increasing recognition of cyber threats targeting critical infrastructure, particularly oil pipelines, has prompted extensive research in the realm of Intrusion Detection Systems (IDS) to safeguard these indispensable networks. Scholars have extensively addressed the distinctive challenges posed by the oil pipeline sector, including the dynamic operational milieu, the intricate integration of operational technology (OT) with intrusion detection [4] encrypted traffic and the nuanced differentiation of normal and anomalous behaviors [5]. Methodologies have evolved to tackle these intricacies, with proponents highlighting the potency of behavior-based anomaly detection, machine learning algorithms, and signature-based detection in accurately pinpointing potential intrusions [6]. In this section, I put together detailed research and case studies of various intrusion detection techniques for oil pipelines.

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

		~		
Paper Title	Authors	Citation	Key Findings	Objectives
Enhancin	Johnso	Johnson,	Behavior	Enhancin
g Pipeline	n, R.	R., &	-based	g Pipeline
Security:	and	Brown, C.	anomaly	Security:
Behavior-	Brown	(2018).	detection	Behavior-
based	, C.	Enhancin	effectivel	based
Anomaly		g Pipeline	У	Anomaly
Detection		Security:	identifies	Detection
		Behavior-	deviation	
		based	s in	
		Anomaly	pipeline	
		Detection.	operation	
		Energy	and	
		Systems	improves	
		Security,	overall	
		12(3),	security.	
		213-228.		
Machine	Zhang,	Zhang,	Machine	Machine
Learning	M. and	M., &	learning	Learning
for	Wang,	Wang, L.	algorithm	for
Intrusion	L.	(2019).	s,	Intrusion
Detection		Machine	including	Detection
in Oil		Learning	supervise	in Oil
Pipelines		for	d and	Pipelines
		Intrusion	unsuperv	
		Detection	ised	
		in Oil	learning,	
		Pipelines.	show	
		Journal of	potential	
		Energy	for	
		Cyberneti	enhancin	
		cs, 8(4),	. <sup>g</sup> .	
		315-332.	intrusion	
C it i al	Marth	Mantina	detection.	Critical
Critical	Martin	Martinez,	Identifyi	Critical Features
Features	ez, G. et al.	$G_{\cdot}$ , et al.	ng	
for Intrusion	et al.	(2020). Critical	specific features	for Intrusion
Detection		Features	such as	Intrusion Detection
in Oil		for	flow	in Oil
Pipeline		Intrusion	rates,	Pipeline
Systems		Detection	pressure	Systems
Systems		in Oil	levels,	Systems
		Pipeline	and valve	
		Systems.	positions	
		Energy	is crucial	
		Infrastruct	for	
		ure	accurate	
		Journal,	intrusion	
		17(1), 45-	detection.	
		62.		
	Lee, S.	Lee, S., &	Integratin	Integratin
Integratin			g	g Incident
Integratin g Incident	and	Kim, W.	5	Sincident
-	-	Kim, W. (2021).	intrusion	Response
g Incident	and		-	-
g Incident Response	and Kim,	(2021).	intrusion	Response
g Incident Response with	and Kim,	(2021). Integratin	intrusion detection	Response with
g Incident Response	and Kim,	(2021).	intrusion	Response
g Incident Response with Intrusion	and Kim,	(2021). Integratin g Incident	intrusion detection with	Response with Intrusion

Pipeline		Intrusion	plans	Pipeline
Security		Detection	enables	Security
		for	swift and	
		Pipeline	appropria	
		Security.	te actions	
		Journal of	during	
		Energy	cyber	
		Technolo	incidents.	
		gy, 9(2),		
		189-204.		
Validatio	Smith,	Smith, J.,	Rigorous	Validatio
n of	J. and	& Jones,	testing,	n of
Intrusion	Jones,	М.	including	Intrusion
Detection	М.	(2022).	penetrati	Detection
Systems		Validatio	on testing	Systems
for Oil		n of	and data-	for Oil
Pipelines		Intrusion	driven	Pipelines
		Detection	simulatio	
		Systems	ns,	
		for Oil	validates	
		Pipelines.	the	
		Journal of	performa	
		Infrastruct	nce of	
		ure	intrusion	
		Security,	detection	
		6(1), 23-	technique	
~ .	~	38.	<u>S.</u>	~ .
Cybersec	Chen,	Chen, Q.,	Successf	Cybersec
urity and	Q. et	et al.	ul	urity and
Operation	al.	(2023).	intrusion	Operation
al Internetie		Cybersec	detection	al Tata anati a
Integratio n in Oil		urity and	systems	Integratio
Pipeline		Operation	ensure minimal	n in Oil Dinalina
Protection		al		Pipeline Protection
riotection		Integratio n in Oil	disruptio n to	FIOLECTION
		Pipeline	pipeline	
		Protection	operation	
		. Energy	s while	
		Technolo	maintaini	
		gy	ng	
		Integratio	security	
		n, 14(3),	measures	
		135-152.		
Regulator	White,	White, L.,	Intrusion	Regulator
y	L. et	et al.	detection	y
Complian	al.	(2024).	systems	Complian
ce for		Regulator	must	ce for
Intrusion		y	align	Intrusion
Detection		Complian	with	Detection
in Oil		ce for	industry	in Oil
~		Intrusion	standards	Pipelines
Pipelines		Detection	such as	-
Pipelines		Dettection		
Pipelines		in Oil	those	
Pipelines			those outlined	
Pipelines		in Oil		
Pipelines		in Oil Pipelines.	outlined	
Pipelines		in Oil Pipelines. Energy	outlined by NERC	
Pipelines		in Oil Pipelines. Energy Regulatio	outlined by NERC and API	

#### Vol. 12 Issue 10, October-2023

		complian		
		ce.		
Table 1: (Literature Review on IDS for oil pipelines from				

previous research works)

Most of the researchers above employed similar technique of intrusion detection systems involving the utilization of sensors, however in terms of selection and adoption of machine learning algorithms, it can be concluded that no "one algorithm fits for all" kind of application. Hence, for the project, trial and error of several supervised classification algorithms are required.

#### IV. METHODOLOGY

This methodology section describes the systematic approach and techniques utilized to collect and analyze data pertaining to the research topic. It ensures the accuracy and validity of the findings by providing a clear explanation of the methods, tools, and materials employed, along with the rationale behind their selection. To address the problem statement and achieve the project objectives, a mixed-method approach encompassing qualitative and quantitative research methods will be adopted. The research will involve examining already deployed intrusion detection systems and how they work, analyzing secondary data from relevant reports, articles, and news outlets over the web as well as a case study approach which will be employed to gain in-depth insights and understanding of the current intrusion detection system deployed in the Niger delta oil pipeline in Nigeria. The study's outcomes will be utilized to formulate recommendations and potential solutions to combat the above outlined problem statement.

#### Intrusion Detection System

An intrusion detection system (IDS) is a system that monitors network traffic to detect abnormal behavior and content. In case of a successful detection, an alarm is raised or a procedure to prevent the attack is taken. A system that takes appropriate actions upon a detection is also known as Intrusion Prevention System (IPS). The outcome with respect to the correctness of the decision made by the intrusion detection system, can be classified into four categories described in table 2 below.

Output	Description
True Positive (TP)	Identifies an activity as an intrusion and
	the
	activity is actually an intrusion
True Negative (TN)	Identifies system behavior as normal and
	the
	activity is actually normal
False Positive (FP)	Identifies an activity as an intrusion but the
	activity is normal
False Negative (FN)	Identifies an activity as normal when the
	activity is an intrusion

Table 2: (Intrusion detection system output categories)

#### Vol. 12 Issue 10, October-2023

#### Intrusion Detection System Types and Classification

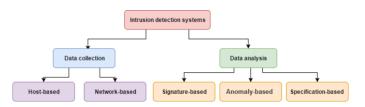


Fig 3: (IDS types and classifications)

The first step of designing an IDS, is to think about the placement of the IDS and which data needed to be collected. The IDS can be host-based, which would collect information about the file system and the behavioral patterns of the user of the system. The second approach features a network-based approach, in which the main goal is to monitor the traffic that is entering and leaving the network.

A signature-based approach is simply looking for signatures of known attack vectors and tries to find them in the collected traffic. The anomaly-based approach relies on a "baseline" condition of the system and reports everything that is striving away from this baseline. The specification-based approach is a relatively new attempt to somehow connect the aforementioned approaches. The main idea is to define a "legal behavior" of the communication which is following a certain protocol.

#### Data Collection Techniques

Intrusion detection systems can be classified according to the type of data they collect. There are two main categories for these types of IDSs: Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS). The network-based IDS, monitors the network traffic and it is usually placed on the traffic routing component, such as a network gateway, which is connecting multiple networks together. This enables the NIDS to intercept and analyze the traffic before it is entering a sub-network, e.g. the local area network (LAN). A host-based IDS, contrary to network-based, is placed on the host computer itself where it monitors the host's system behavior, e.g. which processes are accessing which resources. In addition to these main classifications of IDS, other sub-categories exist, such as:

• Stack-based: monitors the exchange of data between different layers of the protocol's stack.

• Protocol based: Monitors the protocols that are used by the host system

• Graph-based: monitors connections between several nodes or hosts

#### Data Analysis Techniques

As mentioned in the introduction to this chapter, there are three main types of intrusion detection approaches: Anomalybased detection, signature-based detection, and specificationbased detection. In this section, these different paradigms are explained in greater detail.

IDS	Features		Limitatio	n
Approach				
Anomaly-	•	Behavior	•	False
based		Profiling:		Positives:
detection,		Anomaly-		Anomaly-
also known		based		based
as behavior-		detection		systems can
based		builds		generate
detection,		profiles of		false
focuses on		normal		positives
identifying		behavior by		when
deviations		analyzing		legitimate
from		network		activities
established		traffic, user		deviate from
norms within		activities,		established
a system's		system		baselines.
behavior.		performance	•	Baseline
This method		, and other		Establishme
creates a		relevant		nt: Creating
baseline of		data.		accurate
what is	•	Statistical		baselines and
considered		Analysis:		adapting to
"normal" for		Statistical		dynamic
a network or		models are		environment
system by		often		s can be
analyzing		employed to		challenging,
historical		detect		leading to a
data, traffic		outliers and		lengthy
patterns, and		anomalies in		tuning
user		data patterns.		process.
behavior.		Techniques	•	Resource
When		like		Intensive:
activities or		clustering,		These
behaviors		time-series		systems
deviate		analysis, and		require
significantly		machine		continuous
from this		learning		monitoring
baseline, the		algorithms		and analysis,
system raises		are used to		which can be
an alarm to		identify		resource-
indicate a		unusual		intensive.
potential		activities.		
intrusion.	•	Flexibility:		
		Anomaly-		
		based		
		detection can		
		adapt to new		
		and evolving		
		threats,		
		making it		
		suitable for		
		detecting		
		previously		
		unknown		
		attacks.		
Signature-	•	Pattern	•	Limited to
based		Matching:		Known
detection,		Signature-		Threats:
also known		based		Signature-
as misuse		detection		based
detection,		performs		systems are
relies on		pattern		ineffective
predefined		matching		against new
patterns,		between		or zero-day
known as		incoming		attacks that
signatures, to		data and a		have not yet
identify				

# Published by : http://www.ijert.org

known attacks.database of signatures.been identified and added to the signature database.These signatures encapsulate the characteristi cs of specific identifying attacks or such as byte sequences or patterns. The gainst against an extensive data or of extising tincoming data or the lagainst against an extensive data or of extising signatures to data or signatures to datase of signatures to datase of signatures, the signatures, relatively low when detection, relase of signatures, the signatures, the signatures, the signatures, the signatures, the signatures, relatively low when detection, relase of signatures, the signatures, relatively low when detection, relase of signatures, relatively low when detection, relase of solves, relase specification s that describe authorized or acceptable behavior, authorized or and added to solves, or rules that sepecification system. Any deviation from these prodefined rules, deviation from these prodefined intrusion.behavior, subsequentity the alexity sightly the alexity, behavior, sightly deviation solves the alexity, behavior, sightly sightly deviation from these prodefined intrusion, from the p			
These signatures encapsulate the encapsulate the encapsulate the encapsulate the encapsulate the encapsulate the encapsulate the signatures the sof specific tidentifying attacks or well-known making it equences or making it behavioral gattacks such as byte sequences or making it behavioral gattacks or variations such as byte sequences or making it against more attacks such as byte sequences or making it behavioral gattacks or variations encountered incoming data or extensive data or of extising threats.and added to the system or variations or variations signatures, the signatures, the signa	known	database of	been
signatures encapsulate This database. the signature database. This database. The system cannot detect and database are are are are are are are are are ar	attacks.	signatures.	identified
signatures encapsulate This database. This database. This database. The database. The system database. The system cannot detect attacks or well-known novel attacks malware, attacks or or variations such as byte quickly, sequences or making it attacks that behavioral effective do not patterns. The against previously compares encountered existing incoming threats. data or • • Low False • • Maintenance traffic Positives: against an Since the updates to vettensive detection is the signatures. database of based on signatures to datess of signatures, database of based on signatures to database are signatures to database of based on signatures to detect signatures, trigger alerts. Specification • Rule-Based of rules or subsequently trigger alerts. Specification define s that defines a set predefined acceptable encompass behavior authorized or subtaria a perdefined acceptable behavior, authorized or s that predefined configuratio behavior, an alert predefined configuratio behaviors, from these predefined configuratio behaviors, from these predefined configuratio behaviors, from these predefined configuratio behaviors, from these predefined configuratio behaviors, from these predefined configuratio behaviors, from these predefined configuratio behaviors, from these predefined configuratio behaviors, from the predefined configuratio behaviors, from these predefined configuratio behaviors from the predefined configuratio behaviors from the prodefined configuratio behaviors from the prodefi	These	Rapid	and added to
encapsulateThis approachdatabase.theapproachInflexibility: The systemcs of specificidentifyingattacksmovel attackssuch as bytequickly, sequences ormalking it attacksbehavioraleffectivebehavioraleffectivecomparesencountered encounteredincomingthreats.dataorlocalPositives:againstpreviously matchcomparesencountered detection isdataorvextensivedetection is database of signatures, matchsdataSince the detection is database of signatures, matchs and falsesubsequently urger alerts.positives are threats.low when detection, as rule-basedenclessedofficies:Rule-Basedspecification detection, as rule-basedenclessedofficies:Developmen detection detectiondefines a set acceptablepredefined encompassaccuptableencompass accessbehavior as uthorized or accessencompass accessdescribe acceptableencompass encompassbehavior andthyuser predefinedof rules or system. Any uuthorized or accessencompass accessbehavior andthyencompass predefinedconsultation system. Any uuthorized or andsystem indicating a predefinedenforces encompass predefinedfrom the	signatures	-	the signature
theapproachInflexibility: The systemcharacteristiexcels atcannot detectattackswell-knownnovel attacksmalware,attacksor variationssuch as bytequickly,of existingsequences ormaking itattacks thatbehavioraleffectivedo notpatterns. Theagainstpreciselysystempreviouslymatchcomparesencounteredexistingincomingthreats.signatures.dataorLow FalseMaintenancetrafficPositives:signatures.against anSince thethe signatures.datase ofbased onnecessary todetectsignatures,keep up withmatches andfalsepreviouslyattacksnecessary todetectnecognizedthreats.asubsequentlypositives arethreats.low whendetactioncomprehensidetection,Specificationtimealso known-basedDevelopingas rule-baseddetectioncomprehensidetection,relies onve anddefine s asetpredefinedcomprehensispecificationdefineconsuming.authorized orThese rulesFalsepoletinalencompassStringentwithin apermissions, system. Anyusergenerificatinenforcement predefinedpositives if <td>encapsulate</td> <td>This</td> <td></td>	encapsulate	This	
characteristi excels at cs of specific identifying cannot detect well-known novel attacks or variations such as byte quickly, of existing sequences or making it behavioral effective do not patterns. The against previously match compares encountered existing incoming threats. data or econometered existing signatures. data or or econometered existing against an encountered based on database of based on detect signatures, database of based on detect signatures, relatively positives are trigger alerts. relatively positives are trigger alerts. relatively positives are trigger alerts. The system detection as rule-based detection as rule-based detection define or rules that behavior accurate rule of rules or rules that behavior accurate rule of rules or rules that behavior accurate rule shaved matches at predefined of rules or rules that behavior accurate rule of rules or rules that behavior accurate rule shaved detection define complex and system Any user detex on the signatures is can be behavior access Stringent within a permissions, rules can behavior access Stringent predefined inform these and system normal perfective for rules, This compliance and system predefined inform these and system normal perfective for rules, This compliance and system predefined inform these and system normal perfective for rules, This compliance and sightly an alert • Polici rules, This compliance and system predefined inform these and system normal perfective for rules, This compliance and system predefined inform these and system normal perfective for rules, This compliance and system predefined policies: This compliance and system predefined policies and accurate true policies and a		approach	• Inflexibility:
cs of specific attacksidentifying well-known malware, attackscannot detect novel attacksmalware, malware, sequences or behavioral orpatterns. The againstattacks effective gaginstof existing signatures.data or againstpreviously encountered incoming against an extensive database of signaturesMaintenance ising it based on based on detection is detection is database of signatures, database of signatures, detect.Maintenance ising it updates to the signature database of signatures, having relatively positives are trigger alertsMaintenance ising ising it updates to the signature database of signatures, having relatively positives are trigger alertsMaintenance ising ising ising it detect ising it positives are threats.Specification -based detice, of rules or signative of detection, as tub-based detection define as et specification s that degitimate solation solation.Rule positives are threats.Specification defines a set predefined s that indicating a predefined if rom these acceptable deviation from these indicating a predification if rom these and system if rom these and system indicating a predefined indicating a predificed indicating a predifined indicating a<	characteristi		-
attackswell-knownnovel attacksmalware,quickly,or variationssuch as bytequickly,of existingsequences ormaking itattacks thatbehavioraleffectivedo notpatterns. Theagainstprecioslycomparesencounteredexistingincomingthreats.signatures.data or•Low False•trafficPositives:updates todatabase ofbased ondatabase aresignatures toknowndatabase aredatabase ofbased onnecessary todetectsignatures,database arematches andfalseemergingsubsequentlypositives arethreats.trigger alerts.relativelyDevelopmendetection,relativelyDevelopingas ub-baseddetectioncomprehensidetection,relies onve anddefines a setpredefinedaccurate ruleof rules orrules thatsets can bespecificationdefinecomplex ands thatlegitimatetime-deviationbehavior.consuming.autorized andsystempredefinedauceptableencompassStringentrules triggersn.s.slightlys andgentorizesstringents and alertPolicydeviatesfrom theseand systemprodefinedrules triggers <t< td=""><td></td><td></td><td>•</td></t<>			•
malware, such as byte sequences or patterns. The gainst systemattacks quickly, making it effective against encountered existing signatures.or variations of existing attacks that do not precisely match existing signatures.data against against an extensive database of subsequently trigger alerts.• Low False Positives: based on detection is database of subsequently positives are trigger alerts.• Maintenance the signatures, matches and false positives are threats.Specification also known also known also known also known also known of rules or s that behavior.• Rule-Based precisely trigger attack patterns.• Rule positives are threats.Specification of rules or s that behavior authorized or a subsequently as rule-based detection, also known a sub-based detection, a lefine a set predefined accurate rule of rules or s that behavior.• Rule positives comprehensi detection comprehensi comprehensi detection define s that behavior. access acceptable behavior accurate rules setharion behavior, a alert ifrom these predifined accurate rules setharion from these prodefined and system predefined intrusion. the system and alert when efforces from these producing a predefined intrusion, from these producing a producing a predefined intrusion, indicating a predefined intrusion, intrusion, intrusion triggering violations of alerts when intrusion intrusion intrusion intrusion intrusion intrusion intrusion intrusion intrusion 			
such as byte sequences or behavioral patterns. The system incoming data or encountered incoming data or encountered intreats. incoming data or encountered intreats. incoming data base of based on signatures, data or encountered intreats. incoming data base of based on signatures, data or encountered intreats. incoming data base of based on false intreats. i			
sequences or making it effective against match effective against system previously match existing signatures. data or Low False traffic Positives: Regular against an Since the extensive detection is the signature database of based or bas			
behavioral effective against an grecisely match control of threats. against an Since the updates to the signatures to detection is database of based on signatures to known detect signatures, updates to the signature database of based on signatures to known detect signatures, updates to the signature to grecisely positives are threats. Trelatively low when dealing with recognized attack putters. Specification • Rule-Based Otto Rule-Based Developmen Developmen detection, Specification also known -based as the predefined of rules or rules that legitimate describe attack putters that legitimate describe abavior access within a periodes and system of the signature detring in the system Any user lead to false positives; and system Any user lead to false predefined intrusion. The system and s match ecompass and system of the system of th			
patterns. The system commands in coming previously encountered existing signatures. data or Low False Positives: signatures. data or Low False Positives: Regular updates to extensive detection is database of based on signatures to detect signatures, matches and false matches and false positives are trigger alerts. relatively positives are trigger alerts. relatively low when dealing with recognized attack patterns. Specification • Rule-Based Policies: Developmen detection, aspecification trigger alerts of rules that sets can be positives are trigger alerts of rules that legitimate tests are predefined of rules or rules that legitimate tests triggers ns. and alert of policy from these and system normal of these and system normal triggering approach is with particularly predefined time tests triggers ns. and alert of policy the system violations of alerts when violations of alerts when violations of access Customizability: organizations can policies but with particularly predefined policies. This access Customizability: organizations can policies but with particularly predefined test or rules, consuming test predefined policies. This access Customizability: organizations can policies but with particularly predefined policies. This access customizability: organizations can policies but with policies but predefined policies. This access customizability: organizations can policies but with policies but with policies but policies but with policies but predefined policies. This access customizability: organizations can policies but polic		-	_
system previously encountered existing signatures. data or Low False i Regular updates to extensive detection is the signature database of based on signatures, matches and false updates to known necessary to detect signatures, matches and false updates are signatures. Nown detaing with recognized attack patterns. Specification Rule-Based Policies: Developmen detection, Specification trues patterns. Specification Rule-Based Developing as rule-based detection comprehensi detection, relies on detection detection, relies on the specification define s ast predefined so that legitimate describe behavior. access Stringent within a permissions, system Any user lead to false positives; behavior access ns. slightly an alert Policy in these and system predefined intrusion. The system intrusion. The system predefined policies: This acceptale encompase positives; from these and system predefined configuratio behavior shown behaviors, positives if from these and system predefined configuratio behavior shown behaviors, positives if from these and system predefined configuratio behavior shown behaviors, positives if from these and system predefined configuratio behavior shown behaviors, prostives if form these and system predefined configuratio behavior shightly an alert • Policy deviates from the predefined rules, trues, trues, trues, trues can system form these and system predefined policies: This acceptale encomplance and system predefined trues, trues, trues can sightly predefined policies; trues,			
comparesencounteredexistingincomingthreats.signatures.dataor• Low False• MaintenancetrafficPositives:: Regularagainst anSince theupdates toextensivedetection isthe signaturedatabase ofbased ondatabase aresignatures toknownneccessary todetectsignatures,keep up withmatches andfalseemergingsubsequentlypositives arethreats.trigger alerts.relativelythreats.Specification• Rule-Based• Rule-baseddetection,Specificationtalso known-baseddetectioncomprehensidetection,releises onve anddetection,relies onve anddefines a setpredefinedaccurate rules thatlegitimatetime-describebehavior.consuming.authorized orThese rules• FalseacceptableencompassPositives:behavioraccessStringentwithin apermissions,rules canpredefinedconfiguratiobehavioralse triggersns.slightlyan alert• Policydeviatesindicating aEnforcementfrom thepredefinedcomplicesrules.indicating aEnforcementfrom thepredefinedconfiguratiobehavior<	•	-	
incoming data or traffic against an signatures to database of signatures to database of signatures to database of signatures to database of signatures to database of signatures to database of signatures to database of signatures, matches and subsequently trigger alerts. Specification -based detection, also known defines a set of rules or specification s that detection, defines a set of rules or specification s that define for rules or subsequently detection, defines a set of rules or specification s that define for rules or specification s that define s that define from these prodefined tribes deviation from these predefined tribes predefined tribes predefined tribes predefined tribes predefined tribes predefined tribes predefined tribes violations define s tribes s tringering violations of alerts when s effective for violations of alerts when s of alerts whe	•		
dataorLow FalseMaintenancetrafficPositives::Regularagainst anSince theupdates todatabase ofbased onthe signaturesdatabase ofbased onknowndetectsignatures,keep up withmatches andpositives arethreats.subsequentlypositives arethreats.trigger alerts.low whendealing withdetection,SpecificationthreatsbasedPolicies:Developmendetection,Specificationtas rule-baseddetectioncomprehensidetection,relies onveas rule-baseddefinecomprehensigacceptableencompassconsuming.authorized orThese rulesFalsepolicitionaccessStringentsthatlegitimatetime-describeand systemnormalgateringnormalslightlyan alertPolicyfrom thepotential: The systemnormalpredefinedconfiguratioslightlynultoring aEnforcementfrom thepredefinedconfiguratioslightlysindicating aEnforcementproach iswithcomplancean alertPolicydeviatesindicating aEnforcementproach iswitheffective forsystemyoilations ofalerts when <t< td=""><td>-</td><td></td><td>-</td></t<>	-		-
traffic Positives: Regular against an Since the updates to the signatures to database of based on signatures database of based on cessary to detect signatures, matches and false trees ubsequently positives are relatively low when dealing with recognized attack patterns. Specification • Rule-Based Policies: detection, Specification trees also known -based detection comprehensi detection, Specification trees as rule-based detection ve and defines a set predefined acturate the specification define complex and specification define trees specification define complex and s that legitimate time- detscribe behavior, authorized or s that legitimate time- detoring a premissions, rules can be specified or these and system normal s that specification trues if an alert Policy from these and system normal predefined configuratio trues triggers ns. specificating a Enforcement from the predefined configuratio trues triggers ns. specification trues that sets can be consuming. authorized or These rules from these and system normal predefined configuratio trues triggers ns. specification from these and system normal predefined configuratio trues triggers ns. specificating a Enforcement from the predefined rules. This compliance trues. This detecting triggering approach is within a perdefined predefined predefined rules. This detecting triggering approach is within a compliance to system violations of alerts when violations of access Customizability: violations of access Customizability: violations of alerts when violations of access Customizability: known policies but			ũ
against extensive database of signatures to detectSince the detection is signatures, falseupdates to the signature database are necessary to detectmatches and subsequently trigger alerts.false relatively low when dealing with recognized attack patterns.emerging emerging threats.Specification -based• Rule-Based policies: detection, also known est that s that s that s that behavior s that s			
extensive database of signatures to knownthe signature database are necessary to keep up with emerging up ositives are trigger alerts.the signature database are necessary to keep up with emerging threats.matches and subsequently trigger alerts.false necessary to detectemerging threats.aubsequently trigger alerts.positives are relatively low when dealing with recognized attack patterns.threats.Specification -based• Rule-Based Policies:• Rule Developmen to we and accurate rule sets can be comprehensi detection, as rule-based• Rule-Based detection relies on ue and defines a set sets can be comprehensi to rules that sets can be specification defined• Rule Based accurate rule sets can be complex and sets can be complex and sets can be complex and system. Any user• False positives: Stringent within a a permissions, system. Any user• False positives if normal sightly deviation from these and system an alert predefined intrusion.• Policy rules, can sightly predefined intrusion.na alert potential effective for violations of system• Policy rules, can sightly predefined intrusion, enforces intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, compliance intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, intrusion, in			0
databaseof basedbased signatures, signatures, signatures, falsedie signature atabase are necessary to keep up with emerging threats.matches and matches and subsequently trigger alerts.false positives are relatively low when dealing with recognized attack patterns.Rule Developmen to eveloping comprehensi to eveloping comprehensi to eveloping comprehensi test comprehensi test comp			
signatures to detect signatures, matches and subsequently trigger alerts. relatively low when dealing with recognized attack patterns. Specification -based Policies: detection, also known as rule-based detection detection, also known s that defines a set predefined of rules or subact or subsequently positives are patterns. Specification as rule-based detection detection, also known as rule-based detection, s that describe authorized or s that describe authorized or s that describe authorized or system. Any predefined accurate rule behavior, system. Any predefined rules triggers an alert potential infurusion. These specification s that detection s that behaviors, from these predefined configuratio s that behaviors, from these predefined configuratio s that behaviors, from these predefined configuratio s that behaviors, from these predefined configuratio s that behaviors, from these positives an alert predefined configuratio s this compliance theotions the compliance theotions the compliance theotions the compliance theotions the compliance theotions the compliance theotions the compliance theotions the compliance theotions theotions theotions theotions theotions of theotions theotions theotions theotions theotions theotions theotions theotions theotions theotions theotions theotions theot			0
detectsignatures, falsekeep up with emerging threats.matches and subsequentlypositives are relatively low when dealing with recognized attackthreats.Specification• Rule-Based patterns.• Rule Developmen to to attackSpecification• Rule-Based Policies:• Rule Developmen to accurate rule sets can be sets can be sets can be specificationdetection, also known defines a set of rules or suth-based• Rule Developing comprehensi detection, relies on to rules that sets can be specification define sets can be specification• Rule Developing comprehensi detection, relies on to rules that sets can be specification s that legitimate describe authorized or authorized or authorized or authorized or authorized or an alert predefined configuratio predefined configuratio system. Any user behavior, an alert indicating a predefined compliance solution• False positives: positives: slightly deviates to rules, to make subhavior an alert indicating a efforcement intrusion.• Dolicy rules, compliance swith effored rules, compliance with particularly predefined intrusions of approach is with predefined intrusions of alerts when violations count of access customizability: controls, or Organizations can• Dolicies but this count of access customizability: count of organizations can			
matches and subsequently trigger alerts. Specification -based detection, also known detection, also known detection, as rule-based detection, as rule-based detection, detection, sa rule-based detection, defines a set specification s that describe behavior authorized or asystem. Any within a predefined s that describe behavior authorized or access behavior mules that deter system. Any define s specification s that define s system predefined s that describe behavior system. Any define s specification s that describe behavior system intrusion. This compliante system trus system system system complation s trus system trus system system system complation s trus system system system system system system system system complation s trus system syste	-		5
subsequently trigger alerts. Specification -based -based -based detection, also known defines a set predefined s that describe bavior authorized or subsequable -based detection, detection, defines a set predefined s that describe behavior authorized or system from these predefined subser behavior authorized or system predefined subser behavior authorized or system predefined subser behavior subser system predefined subser system predefined subser system predefined subser subser system predefined subser subse		0	
trigger alerts. relatively low when dealing with recognized attack patterns. Specification -based -based -based -based -based -based detection, also known -based detection, also known -based detection detiction, relies of rules specification s that defines s that describe acceptable behavior. authorized or s system Any defines s that degitimate describe acceptable behavior, acceptable behavior, acceptable behavior, acceptable behavior, system an alert predefined configuratio behaviors, an alert predefined configuratio behavior triles s tringent tringent s tringent s tringent			00
Iowwhen dealing with recognized attack patterns.Rule DevelopmenSpecification -based• Rule-Based Policies: Developmen• Rule Developmendetection, also known defines a set specification as that describe acceptable• Rule Developing comprehensi define behavior.• Rule Developing comprehensi define comprehensi define comprehensi define sets can be specification define s that describe acceptable behavior.• Rule Developmen define comprehensi comsuming.authorized or acceptable behavior system. Any uuser indicating a potential intrusion.• False positives; specification access and system predefined configuratio slightly an alert potential intrusion.• False positives; positives; sightly deviates from the enforces rules.This approach is violations detecting violations formor his policies, compliance alerts when yoilations of access• Limited to Known effective for rules, triggering alerts when effective for system occur.Nown policies, policies, controls, or• Organizations can cocur.• Dicies but		-	threats.
dealing with recognized attack patterns.dealing with recognized attack patterns.Specification -based• Rule-Based Policies: Specification also known also known also known also known detection, also known as rule-based detection, detection, idetection, relies on rules that sets can be specification define s that describe acceptable deviation behavior.• Rule Developmen comprehensi comprehensi detection comprehensi detection comprehensi detection, relies on rules that sets can be specification define s that describe acceptable deviation from these and aget system. Any user indicating a predefined configuratio rules triggers an alert potential intrusion.• Rule Rule consuming. consuming. consuming. rules can slightly deviates indicating a enforces tribis compliance enforces this compliance this compliance compliance triggering triggering triggering approach is with policies, occur. consuming cocur. consuming cocur. compliance triggering toilations of alerts when effective for system violations of succes cocur. cocu	trigger alerts.	relatively	
recognized attack patterns.recognized attack patterns.Specification -based• Rule-Based Policies: specification• Rule Developmen t: also known as rule-based detection, detection, relies on of rules or s that sectification• Rule Developing comprehensi detection detectiondefines a set of rules or s that describe acceptablepredefined behavior. These rules encompass encompass behavior• False Positives: behavior stringent within a permissions, system. Any rules rules endefined indicating a predefined• False positives: behavior stringent stringent time- consuming. encompass positives: behavior stringent within a permissions, system. Any user lead to false positives if from these and system enforces normal enforces trules triggers non nalert indicating a potential intrusion. enforces this compliance trules, tringent stringent stringent stringent trom the enforces trules. This compliance tringering			
Attack patterns.Rule patterns.Specification -based• Rule-Based Policies: also known also known -based• Rule Developmen to based detection detection, relies on predefined of rules or s that escribe acceptable• Rule Developing comprehensi detection define sets can be sets can be complex and sets can be sets can be se		dealing with	
patterns.Specification -based• Rule-Based Policies: Specification• Rule Developmendetection, also known as rule-based-based detection reliesDeveloping comprehensi detectiondetection, detection, detection, detectionrelies on veDeveloping comprehensi detectiondetection, detection, detines a setpredefined of rules or rules that behavioraccurate rule sets can be consuming.authorized or acceptableThese rules behavior• False positives: behavior, accesswithin a predefined configuratiopermissions, behaviors, from these and system predefined• False positives: positives: behavior indicating a pertecting indicating a protential intrusion.• Policy enforcement enforces compliance intrusion.This compliance of potential intrusion, particularly predefined intrusion, prodefined intrusion, enforces compliance effective for rules, this detecting tiolations of alerts when violations of alerts when violations court.• Limited to Known effective for rules, this alerts when effective for rules, triggering alerts when effective for rules, court.• Kale violations of alerts when effective for rules, triggering alerts when effective for rules, triggering alerts when effective for rules, triggering alerts when effective for rules, triggering alerts when effective for rules, triggering alerts when effective for rules, triggering alerts when effe		recognized	
Specification -based• Rule-Based Policies: Specification• Rule Developmen t: Developing comprehensi detection, detection, detection, detection, detection, detection, detection, detines a set specification s that describe acceptable behavior authorized or acceptable behavior within a system. Any deviation from these predefined rules triggers an alert potential intrusion.• Rule Policies; behavior, access ns. an alert timicating a potential intrusion.• Rule Developmen t: Developing comprehensi ve and accurate rule sets can be consuming.Specification define s that describe acceptable behavior access tringent rules triggers ns. an alert potential intrusion.• Rule Developing comprehensi ve and accurate rule sets can be consuming.Specification s deviation rules triggers an alert potential intrusion.• Policy enforcement time triggering alerts when violations occur.• Rule Developing comprehensi time- complex and time- consuming.This approach is violations of alerts when violations of alerts when violations controls, or Organizations controls, or• Rule Developing comprehensi time- consuming.• Rule behavior. and system violations configuratio• False positives: stringent rules the predefined rules.• Dicy time time total violations of alerts when violations occur.• Limited to Known effective for violations of alerts when violations of alerts whe		attack	
-based detection, also known as rule-based detection,Policies: Specification -based detection relies on predefined of rules or s that sets can be specification define s that describe acceptable behavior within a system. Any predefined construction deviationDevelopmen to comprehensi accurate rule sets can be complex and time- consuming. acceptable behavior access within a permissions, rules triggers an alert intrusion.Developmen to comprehensi detection time- to access stringent stringent stringent stringent stringent stringent trules can behavior trules can behaviors, from these and system normal predefined trules, this compliance trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting tetting trules, tetting tetting trules, tetting tetting trules, tetting tetting trules, tetting tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting trules, tetting tetting trules, tetting trules, tetting tetting trules, tetting tetting trules, tetting tetting trules, tetting tetting trules, tetting tetting tetting trules, tetting tetting tetting tetting tetting tetting tetting tetting tetting tetting tetting tetting tetting tetting tett		patterns.	
detection, also known as rule-based detection,Specification -based detection relies on predefined behavior.t: Developing comprehensi detection accurate rule sets can be complex and time- consuming.defines a set of rules or s that describe acceptable behavior within a system. Any predefined rules that system. Any user from these predefined configuratio rules triggers an alert predefined intrusion.t: behavior, rules acceptable behavior, access acceptable behavior, access and system predefined rules triggers nn an alert potential intrusion.t: rules complex and time- consuming.this an alert potential intrusion.: The system enforces rules, time- to approach is with particularly predefined rules, teffective for rules, teffective for rules, detecting violations of alerts when violations occur.t: to approach is alerts when violations occur.detection, access rules, teffective, for rules, octurios, or organizations controls, ort: to approach is can triggering alerts when violations cocur.this teles policies, policies, controls, orCustomizability: to approach is can triggering alerts when violations cocur.this teles policies teles telest: teles teles teles telesthis teles teles telest: teles teles telesthis teles teles teles telest: teles teles teles telesthis teles teles teles <td>Specification</td> <td><ul> <li>Rule-Based</li> </ul></td> <td>Rule</td>	Specification	<ul> <li>Rule-Based</li> </ul>	Rule
also known as rule-based-based detectionDeveloping comprehensias rule-baseddetectioncomprehensidetection,relies onve and accurate ruleof rules orrules thatsets can bespecificationdefinecomplex and time-describebehavior.consuming.authorized orThese rules• FalseacceptableencompassPositives:behavioraccessStringentwithin apermissions,rules cansystem. Anyuserlead to falsedeviationbehaviors,positives ifnormalbehaviors,positives ifnormalenforcementfrom thepredefinedconfiguratioslightlyan alertPolicydeviatesindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance• Limited toapproach iswithPolicies:effective forrules,Thisviolations ofalerts wheneffective forviolations ofalerts wheneffective forviolations ofalerts wheneffective forpolicies,occur.violations ofalerts whenviolations ofalerts whenpolicies but	-based	Policies:	Developmen
as rule-based detection,detection reliescomprehensi vedefines a set of rules or specificationpredefined defineaccurate rule sets can be complex and time- consuming.as athatlegitimate behavior.complex and time- consuming.authorized or acceptableThese rules encompassFalse Positives:behavior accessaccess encompassStringent rules can behaviors, positives if normalgeven these predefined rules triggersand system enforcementnormal predefined indicating a enforces trules, thisThis approach is violations of accessStringent rules, compliance triggering approach is effective for violations of accesscomplex and time- consuming.acceptable behaviorBenforcement enforces rules, trules, triggering approach is effective for systemFalse positives if normal behaviors, trules trules trules trules trules trulesThis approach is violations of accessCustomizability: cocur. violations of alerts when violations of accessthe complex and trules triggering approach is effective for violations of alerts when violations of accesscontrols, or ortrols, orOrganizations cocur.policies but	detection,	Specification	t:
as rule-based detection,detection reliescomprehensi vedefines a set of rules or specificationpredefined defineaccurate rule sets can be complex and time- consuming.as athatlegitimate behavior.complex and time- consuming.authorized or acceptableThese rules encompassFalse Positives:behavior accessaccess encompassStringent rules can behaviors, positives if normalgeven these predefined rules triggersand system enforcementnormal predefined indicating a enforces trules, thisThis approach is violations of accessStringent rules, compliance triggering approach is effective for violations of accesscomplex and time- consuming.acceptable behaviorBenforcement enforces rules, trules, triggering approach is effective for systemFalse positives if normal behaviors, trules trules trules trules trules trulesThis approach is violations of accessCustomizability: cocur. violations of alerts when violations of accessthe complex and trules triggering approach is effective for violations of alerts when violations of accesscontrols, or ortrols, orOrganizations cocur.policies but	also known	-based	Developing
defines a setpredefinedaccurate ruleof rules orrules thatsets can bespecificationdefinecomplex andas thatlegitimateconsuming.describebehavior.consuming.authorized orThese rulesFalseacceptableencompassPositives:behavioraccessStringentwithin apermissions,rules cansystem. Anyuserlead to falsedeviationbehaviors,positives iffrom theseand systemnormalpredefinedconfiguratiobehaviorrules triggersns.slightlyan alertPolicydeviatesindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.ThiscomplianceLimited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingviolations ofalerts wheneffective forsystemviolationsdetectingviolations ofalerts wheneffective forsystemviolationsdetectingviolations ofalerts wheneffective forsystemviolations ofpolicies but	as rule-based	detection	
of rules or specificationrules that definesets can be complex and time- consuming.a that describelegitimate behavior.consuming.authorized or acceptableThese rules encompass accessFalse Positives:behavior within a system. Any deviationpermissions, behaviors, and system or ules triggers an alertrules can behaviors, from these predefinedauthorized or accessDesitives: sourcesauthorized or accessnormal behaviors, positives if normalpredefined predefinedconfiguratio normalpredefined indicating a potential intrusion.Enforcement enforcesThis potential intrusion.: The system with predefined rules, the system predefinedfrom the potential intrusion.enforces rules, rules, thisfrom the potential intrusion.enforces rules, rules, thisfrom the potential intrusion.predefined rules, rules, thisffective for system policies, policies, occur.Limited to known effective for violations detecting violations of alerts when violations occur.outoriols, or policies, or policies, or controls, orCustomizability: controls core	detection,	relies on	ve and
of rules or specificationrules that definesets can be complex and time- consuming.a that describelegitimate behavior.consuming.authorized or acceptableThese rules encompass accessFalse Positives:behavior within a system. Any deviationpermissions, behaviors, and system or ules triggers an alertrules can behaviors, from these predefinedauthorized or accessDesitives: sourcesauthorized or accessnormal behaviors, positives if normalpredefined predefinedconfiguratio normalpredefined indicating a potential intrusion.Enforcement enforcesThis potential intrusion.: The system with predefined rules, the system predefinedfrom the potential intrusion.enforces rules, rules, thisfrom the potential intrusion.enforces rules, rules, thisfrom the potential intrusion.predefined rules, rules, thisffective for system policies, policies, occur.Limited to known effective for violations detecting violations of alerts when violations occur.outoriols, or policies, or policies, or controls, orCustomizability: controls core	defines a set	predefined	accurate rule
s that legitimate legitimate describe behavior. authorized or These rules acceptable encompass behavior access Stringent vithin a permissions, system. Any user lead to false deviation behaviors, from these and system ormal predefined configuratio mules triggers ns. Silghtly an alert • Policy deviates indicating a Enforcement intrusion. Enforcement intrusion. Enforces This compliance approach is with particularly predefined rules, This detecting triggering approach is with particularly predefined rules, to system violations of access Customizability: controls, or Organizations can organizations can substant controls, or Organizations can organizations c	of rules or		sets can be
describebehavior.consuming.authorized orThese rulesFalseacceptableencompassPositives:behavioraccessStringentwithin apermissions,rules cansystem. Anyuserlead to falsedeviationbehaviors,positives iffrom theseand systemnormalpredefinedconfiguratiobehaviorrules triggersns.slightlyanalertPolicyindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.ThiscomplianceLimited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knownpolicies, orOrganizations canpolicies but	specification	define	complex and
describebehavior.consuming.authorized orThese rulesFalseacceptableencompassPositives:behavioraccessStringentwithin apermissions,rules cansystem. Anyuserlead to falsedeviationbehaviors,positives iffrom theseand systemnormalpredefinedconfiguratiobehaviorrules triggersns.slightlyanalertPolicyindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.ThiscomplianceLimited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knownpolicies, orOrganizations canpolicies but	s that	legitimate	time-
authorized or acceptableThese rules encompass accessFalse 	describe	behavior.	
acceptableencompassPositives:behavioraccessStringentwithin apermissions,rulessystem. Anyuserlead to falsedeviationbehaviors,positives iffrom theseand systemnormalpredefinedconfiguratiobehaviorrules triggersns.slightlyanalertPolicyindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.ThiscomplianceLimited toapproach iswithPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knownpolicies, orOrganizationscanpolicies butpolicies but	authorized or		
behavioraccessStringentwithin apermissions,rules cansystem. Anyuserlead to falsedeviationbehaviors,positives iffrom theseand systemnormalpredefinedconfiguratiobehaviorrules triggersns.slightlyanalert• Policyindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance• Limited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knownpolicies, orOrganizations canpolicies but			
within a system. Anypermissions, userrulescandeviationbehaviors, behaviors, and systemlead to false positives iffrom these predefinedand system configurationormal behaviorpredefinedconfiguratio ns.behavior slightlyan alert ottationPolicy enforcementdeviates from the predefined rules.indicating a potentialEnforcement enforcesfrom the predefined rules.This approach is effective for systemcompliance rules, triggering alerts when violations of alerts when violations of accessThis corrules, triggering approach is effective for violations of alerts when violations of accessCustomizability: known policies but		-	
system. Any deviationuserlead to falsefrom these predefinedbehaviors, and systempositives if normalpredefined rules triggersns.slightly deviatesan alert potentialPolicy Enforcementdeviatesindicating a potentialEnforcement enforcesfrom the predefinedThis approach is effective for systemcompliance rules, triggering alerts when violations of systemLimited to Known effective for violations of accesscurrent currentrules, rules, triggering occur.This effective for violations of alerts when violations of alerts when policies, current current policies, current policies, current current current current policies, current c			0
deviationbehaviors, and systempositives if normalfrom theseand systemnormalpredefinedconfiguratiobehaviorrules triggersns.slightlyanalertPolicydeviatesindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance• Limited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscanpolicies butorganizations		_	
from theseand systempointees inpredefinedconfigurationormalrules triggersns.slightlyan alertPolicydeviatesindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance• Limited toapproach iswithPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knownpolicies, orOrganizationscanpolicies, orpoliciesbelaviorpolicies, orpoliciesbelavior <td>• •</td> <td></td> <td></td>	• •		
predefinedconfiguratiobehaviorrules triggersns.slightlyanalertPolicyindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance• Limited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knownpolicies, orOrganizationspolicies but			
rules triggersns.slightlyanalertPolicydeviatesindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance• Limited toapproach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscanpolicies butorganizations		•	
analert•Policydeviatesindicating aEnforcementfrom thepotential: The systempredefinedintrusion.enforcesrules.Thiscompliance•approach iswithKnownparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscan	1	-	
indicating a potentialEnforcement Enforcementfrom the predefined rules.intrusion.enforces enforcesrules.Thiscompliance with• Limited to Known Policies:approach is particularlypredefined triggering alerts when violations of system• Dicies: effective for detectingviolations of systemalerts when violations occur.effective for detecting violations of accesscontrols, or ortrols, orOrganizations ocacan policies but			
potential intrusion.: The system enforcespredefined rules.Thiscompliance approach is• Limited to Knownapproach iswith predefined• Dolicies:effective for stetctingrules, rules, triggering alerts when violations of access• This compliance predefined triggering approach is effective for detecting violations of access• Limited to Known Policies: effective for detecting violations of cocur. violations of accesspolicies, controls, orOrganizations Organizations canpredefined could policies known policies but		•	
intrusion.enforcesrules.ThiscomplianceLimited toapproach iswithPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscan	•		
ThiscomplianceLimitedapproach iswithLimitedtoparticularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalertswhensystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscanpoliciespoliciesbut	-	-	_
approach is particularlywith predefinedKnown Policies:effective for detectingrules, triggeringThis approach is effective for detectingviolations of systemalerts when violationseffective for detectingpolicies, accessoccur. Organizationsviolations of canoffective, policies, controls,organizations ocanorganizations			
particularlypredefinedPolicies:effective forrules,Thisdetectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscan		-	
effective for detectingrules, triggeringThisdetectingtriggering alerts whenapproach isviolations of systemalerts when violationseffective forgolicies, accessoccur. Customizability: controls, orviolations or Organizationshow controls	••		
detectingtriggeringapproach isviolations ofalerts wheneffective forsystemviolationsdetectingpolicies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscan		• .	
violations of systemalerts when violationseffective for detectingpolicies, ccessoccur.violations of accesscontrols, or controls, orOrganizations canpolicies but		,	This
violations of systemalerts when violationseffective for detectingpolicies, accessoccur.violations of knowncontrols, orOrganizations canpolicies but		triggering	
policies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscan		alerts when	effective for
policies,occur.violations ofaccessCustomizability:knowncontrols, orOrganizationscanpoliciesbut	•	violations	detecting
access Customizability: known controls, or Organizations can policies but	policies,	occur.	violations of
controls, or Organizations can policies but	access	Customizability:	
	controls, or	Organizations can	policies but
		tailor the detection	

usage policies.	rules to match their specific security policies and regulatory requirements.	may struggle with detecting new and novel
		attacks

#### Table 3: (IDS Approaches)

To model the behavior of the host system or the network traffic observed, there is a need to construct a view which has a certain level of abstraction, that leads to extraction of features. These features are then used together with machine learning techniques that can construct a hypothesis that models the behavior of the system e.g., Neural networks, support vector machines, time series, standard deviation and more. Upon the IDS run-time, features similar to the one used to train the model have to be extracted again before passing them to the hypothesis that will perform the classification.

#### Intrusion Detection System Architecture

The following section focuses on the basic system architecture of a network-based intrusion detection system. This will aid in gaining a deeper understanding of how to plan and build the prototype IDS for an oil pipeline system. When implementing an Intrusion detection system, it is not possible to completely resort to a common standard due to varying requirements when utilizing the gathering of the data and its analysis. Nevertheless, almost all of them have some basic components/modules that they all share. These components are:

I. A Network-Based IDS (NIDS) monitors network traffic to identify suspicious or malicious activities. It operates at the network perimeter, analyzing data as it flows through routers, switches, and other network devices. The architecture typically includes the following components:

II. Sensors/Probes: These are strategically placed on network segments to capture and analyze incoming and outgoing network traffic. They can be physical appliances or software-based sensors running on dedicated hardware.

III. Network Taps or Span Ports: These provide the necessary access to network traffic for the sensors to analyze. Taps ensure passive monitoring without affecting network performance.

IV. Preprocessors: Incoming network traffic may be preprocessed to remove redundant or irrelevant information, making the analysis process more efficient.

V. Detection Engine: The core of the NIDS, this engine applies various detection techniques such as signature-based, anomaly-based, and heuristic-based methods to identify potential intrusions.

VI. Alert Generation: When the detection engine identifies suspicious activity, it generates alerts or alarms. These alerts provide details about the detected event, severity, and potential impact.

VII. Central Management Console: This component aggregates alerts from various sensors, provides a

centralized view of network activity, and allows security analysts to manage and respond to detected incidents.

VIII. Databases: Logs and metadata about network traffic and detected events are stored in databases for future analysis, reporting, and forensic investigations.

IX. Response Mechanism: Some NIDS architectures include automated response mechanisms that can take actions such as blocking traffic from specific sources or isolating compromised devices. [7]

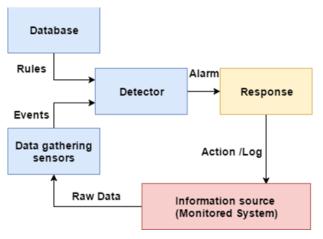


Fig 4: (Typical IDS Architecture) [8]

# Comparison of Machine Learning Algorithms for Intrusion Detection.

Machine learning algorithms have gained popularity in this field due to their ability to detect anomalies and patterns indicative of intrusions. Here are some commonly used machine learning algorithms for intrusion detection.

Algorithm	Туре	Strength	Weaknesses
Decision	Supervise	Interpretabl	Prone to
Trees	d	e, handles	overfitting,
		categorical	may not
		data	capture
			complex
			patterns
Random	Ensemble	High	Computationall
Forest		accuracy,	y intensive, less
		reduced	interpretable
		overfitting	
Support	Supervise	Effective in	Sensitive to
Vector	d	high-	hyperparameter
Machines		dimensional	s, limited
(SVM)		spaces	scalability
K-Nearest	Supervise	Simple,	Sensitive to
Neighbors	d	effective for	distance metric,
(KNN)		anomaly	scalability
		detection	issues
Naive	Supervise	Fast,	Assumes
Bayes	d	handles	feature
			independence

r		1	1
		categorical	(naive
		data	assumption)
Neural	Deep	Captures	Requires large
Networks	Learning	complex	datasets,
	_	patterns,	computationall
		adaptable	y intensive
Unsupervise	Clusterin	Anomaly	Difficulty in
d Learning	g	detection,	setting
_	_	no need for	appropriate
		labels	thresholds
Ensemble	Ensemble	Improved	Complexity,
Methods		accuracy	parameter
		and	tuning required
		robustness	

# Table 4: (Comparison of ML Algorithms for IDS) [9]

Detecting intrusion or unauthorized access in oil pipeline systems is a critical security concern, and the choice of a machine learning algorithm should be based on the unique characteristics of pipeline data and operational requirements. Given the nature of the Niger-Delta region, data in oil pipeline systems and the need for real-time detection, using a combination of the following machine learning algorithms will aid in efficiently and effectively detecting intrusion:

1. Support Vector Machines (SVM)

SVMs can be effective for intrusion detection in oil pipeline systems, especially when dealing with highdimensional sensor data. They are robust and can handle non-linear data patterns. SVMs can be used for binary classification tasks to identify anomalies indicative of intrusion.

2. Recurrent Neural Networks (RNN)

RNNs, particularly Long Short-Term Memory (LSTM) networks, are well-suited for handling time-series data commonly found in pipeline systems. They can capture temporal dependencies and recognize abnormal patterns or sequences of events that might indicate unauthorized access or tampering.

3. Ensemble Methods

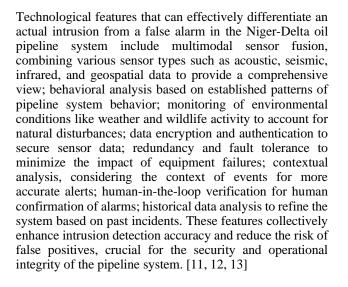
Combining multiple machine learning models, such as Random Forests, SVMs, and neural networks, into an ensemble can provide robust and accurate intrusion detection. Ensemble methods can help reduce false positives and improve overall system reliability.

4. Deep Reinforcement Learning

If the pipeline system's security involves decisionmaking or control aspects, deep reinforcement learning can be used to train agents to take actions that minimize intrusion risks based on sensor data. This approach is suitable for dynamic security responses. [10]

Technological Features that can differentiate an actual intrusion from a false alarm.

Vol. 12 Issue 10, October-2023



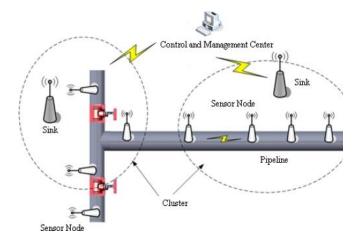
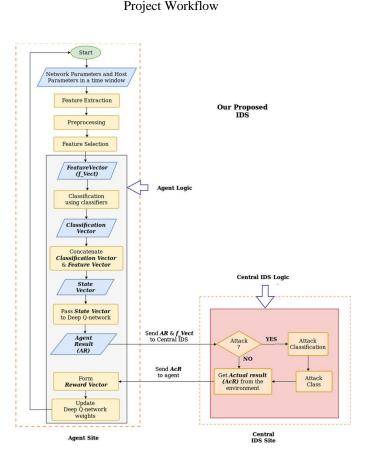


Fig 5: (Architecture of pipeline monitoring sensor networks) [<u>17</u>]



(Derived project workflow with reference (Kamalakanta Sethi, 2020))

#### REFERENCES

- [1] Niger Delta (2023) Wikipedia. Available at: https://en.wikipedia.org/wiki/Niger\_Delta (Accessed: 18 October 2023).
- [2] Al Jazeera (2023) Shell pipeline spill fouls farms, river in Nigeria's Niger Delta, Business and Economy News | Al Jazeera. Available at: https://www.aljazeera.com/news/2023/6/26/shell-pipeline-spill-foulsfarms-river-in-nigerias-niger-delta (Accessed: 11 August 2023).
- [3] Al Jazeera (2022) Nigerian oil exports at lowest level in 25 years due to oil theft, Oil and Gas News | Al Jazeera. Available at: https://www.aljazeera.com/news/2022/9/9/nigerian-oil-exports-atlowest-level-in-25-years-due-to-oil-theft (Accessed: 18 August 2023).
- [4] Alshahrani, H. et al. (2023) Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network, MDPI. Available at: https://www.mdpi.com/2071-1050/15/11/9001 (Accessed: 18 October 2023).
- [5] Liu, H. and Lang, B. (2019) Machine learning and deep learning methods for intrusion detection systems: A survey, MDPI. Available at: https://www.mdpi.com/2076-3417/9/20/4396 (Accessed: 18 September 2023).
- [6] Aljameel, S.S. et al. (2022) An anomaly detection model for oil and gas pipelines using machine learning, MDPI. Available at: https://www.mdpi.com/2079-3197/10/8/138 (Accessed: 18 October 2023).
- [7] (No date) Architecture of network-based Intrusion Detection System (NIDS). Available at: https://www.researchgate.net/figure/Architectureof-network-based-intrusion-detection-system-NIDS\_fig1\_357153369 (Accessed: 18 October 2023).
- [8] (No date a) Basic architecture of Intrusion Detection System (IDS). Available at: https://www.researchgate.net/figure/4-Basic-architecture-

of-intrusion-detection-system-IDS\_fig2\_226650646 (Accessed: 18 October 2023).

- [9] (No date c) Architecture of network-based Intrusion Detection System (NIDS). Available at: https://www.researchgate.net/figure/Architectureof-network-based-intrusion-detection-system-NIDS\_fig1\_357153369 (Accessed: 18 October 2023).
- [10] Obonna, U.O. et al. (2023) Detection of man-in-the-middle (MITM) cyberattacks in oil and gas process control networks using machine learning algorithms, MDPI. Available at: https://www.mdpi.com/1999-5903/15/8/280 (Accessed: 18 October 2023).
- [11] Liu1, Y.H. (2018) IOPscience, Journal of Physics: Conference Series. Available at: https://iopscience.iop.org/article/10.1088/1742-6596/1087/6/062032 (Accessed: 19 October 2023).
- [12] (No date a) View of identifying false alarm for network intrusion detection system using hybrid data mining and decision tree. Available at: https://ejournal.um.edu.my/index.php/MJCS/article/view/6323/4001 (Accessed: 18 October 2023).
- [13] Tejedor, J. et al. (2017) A novel fiber optic based surveillance system for prevention of Pipeline Integrity Threats, MDPI. Available at: https://www.mdpi.com/1424-8220/17/2/355 (Accessed: 10 September 2023).
- [14] Defense in depth (computing) (2023) Wikipedia. Available at: https://en.wikipedia.org/wiki/Defense\_in\_depth\_(computing) (Accessed: 18 August 2023).
- [15] https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html
- [16] Pandey, S. (n.d.). Pipeline Intrusion Detection Systems a crucial tool for O&G companies in detecting threats. The Times of India. [online] Available at: https://timesofindia.indiatimes.com/blogs/voices/pipelineintrusion-detection-systems-a-crucial-tool-for-og-companies-indetecting-threats/ [Accessed 3 Jul. 2023].