An In-depth Review of Machine Learning & Deep Learning Models for Enhancing Security and Scalability in Edge Computing

Mr. Pankaj S. Wankhede^{1*}, Ganesh Khekare^{2*}, Dr. Amitabh Wahi³

¹Research Scholar, Assistant Professor, Bhagwant University, Ajmer, India. ²Associate Professor, Vellore Institute of Technology, Vellore, India. **Email:** khekare.123@gmail.com ³Associate Professor, Bhagwant University, Ajmer, India. **Email:** wahiamitabh@gmail.com ⁽¹⁾0009-0004-2346-2096

Email of Corresponding Author: Pankajwankhede5@gmail.com

Received on: 11 May,2025

Revised on: 16 June, 2025

Published on: 18 June, 2025

Abstract: The current reality is very fast-paced edge computing that shortly will be demanding robust security and scaling solutions for its necessarily distributed and resource-constrained nature. Addressing this need, this paper critically assesses machine learning and deep learning models tailored to enhance both security and scalability in edge computing and points at improvement areas so further work in these regards may be fruitful. On the other hand, most of the surveys about this topic usually suffer from the narrow scope, since most of them miss either a wide spectrum of ML and DL techniques or their concrete applications in the context of edge computing. This work gives a comprehensive review of a good number of ML and DL models, ranging from supervised learning algorithms like Support Vector Machines and Random Forests to unsupervised learning methods like K-means clustering, and advanced deep learning architectures such as Convolutional Neural Networks, Recurrent Neural Networks, and Generative Adversarial Networks. Thus, these models are primarily rated based on their capability to enhance security measures like intrusion detection, data encryption, and anomaly detection, and scalability in handling edge device dynamics and heterogeneity. As noted in the review, among all the models, very few can take such complex patterns of data and realize high accuracy for security applications like the DL models, especially CNNs and GANs. In particular, SVM and RF are known to be robust and efficient for processing small- to

medium-sized datasets typical in edge environments. However, some limitations include high computational costs and large training datasets required by the DL models are also discussed. Hybrid approaches combining multiple models have been reviewed to leverage their strengths and make up for the weaknesses of individual models. The comprehensive review has developed several insights that can support future research in strengthening more efficient, scalable, and more secure edge computing frameworks. In particular, gaps and potential improvements related to ML and DL applications stand as greatly important in the progress of edge computing technologies toward better reliability and enhanced performance in real-world scenarios. This thus has a very significant impact on the domain because it provides an in-depth understanding of the current state of capabilities and future directions for ML and DL models at the edge.

Keywords- Edge Computing, Machine Learning, Deep Learning, Security, Scalability.

I. INTRODUCTION

 E_{dge} computing is an evolutionary paradigm that brings cloud computing closer to the edge of the

brings cloud computing closer to the edge of the network, toward sources of data and end-users, aiming at reducing latency, real-time processing, and bandwidth constraints by processing data locally at edge devices.

The huge distributed and heterogeneous nature of edge computing presents major challenges to security and scalability. Preliminary security models, traditional scalability strategies, and the rich edge environments are inadequate in these highly dynamic and resourceconstrained settings. This is where machine learning and deep learning can help—in their sophisticated algorithms to perform learning from data, adapt to new threats, and scale in a manner that's appropriate with edge devices at scale. These involve efficient and effective supervised learning algorithms, like Support Vector Machines and Random Forests, applyable in various edge computing applications, and deep learning models like Convolutional Neural Networks and Generative Adversarial Networks, which show great potential for managing sophisticated data patterns and boosting all security-related measures concerning the detection of intrusion and anomaly. Although these models based on ML and DL have been viable, most of the literature to date only serves partial insight into such, typically focusing narrowly on certain models or applications without assessing the overall strengths, weaknesses, and limitations. This review is purposed to be a fill in the space by going into in-depth analysis on the present state of the art ML and DL models within the context of edge computing. After critically examining these models, this review tries to identify the existing gaps, proposes hybrid approaches to mitigate the weaknesses of every individual technique, and lays out future research directions to achieve better security and scalability in an edge computing environment. Deep, systemic analysis of a body of ML and DL models will also offer important insights for researchers and practitioners operating in the realms of practical applications, performance metrics, and deployment challenges. This deep understanding is called for in the development of robust, scalable, and secure frameworks of edge computing that would meet or intend to meet contemporary and future technological demands.

II. LITERATURE REVIEW

The exponential growth in the number of IoT devices and increasing demands of real-time data processing made the evolution of Edge Computing a much-needed technology to complement Cloud Computing. Since edge computing is decentralized, this opens the way for very complex security challenges: data integrity, privacy concerns, and vulnerability to cyber-attacks. At the same time, scalability has to be achieved in edge networks so that data can be managed and processed as seamlessly as possible over an array of heterogeneous devices that is constantly increasing. Traditional security measures and scalability techniques rely extensively on centralized architectures; hence, in all these decentralized environments, they turn out to be inadequate—therefore, requiring innovative methods that would avail the adaptive and predictive capabilities of machine learning and deep learning models. This review assumes a timely need to explore, analyze, and synthesize existing ML and DL models for their efficacy in improving the security of edge computing frameworks while also enhancing their scalability.

This review regards considering detailed coverage of a wide section of ML and DL models including, but not limited to, Support Vector Machines, Random Forests, Convolutional Neural Networks, and Generative Adversarial Networks. The selected models are driven by their earlier proved capabilities: pattern recognition, anomaly detection, and predictive analytics in different fields, all instrumental in the construction of robust security mechanisms in edge computing. The review will further critically go through the strengths of such models: high accuracy delivered by CNNs while detecting sophisticated patterns of attacks and efficiency of RF in handling small-scale data typical of edge devices & deployments. We outline a few dimensions of contributions resulting from this survey. The first part offers a comprehensive overview of the current landscape in ML and DL models, including the unique applications and performance metrics used to underpin improvements in security and scalability. It fleshes out some important gaps in the existing literature with respect to this host of studies and empirical evidence by pointing out critical deficiencies that relate to integrating different models in a way that empirically utilizes their complementary strengths. These hybrid models are designed to be more scalable to efficiently handle the dynamic and resource-constrained nature of edge environments. Concretely, this survey offers the practical ideas for deployment and optimization of these models in edge computing systems. Among other things, it talks about computational resource management, reduction of latency, and striking a balance between security and scalability during deployment. This review, therefore, adds value to the field of edge computing through the systematic evaluation and synthesization of existing ML and DL models for security and scalability enhancement. It points out critical gaps in literature today, proposes innovative hybrid approaches, and

International Journal of Innovations in Engineering and Science, www.ijies.net

provides practical deployment insights. The work could, therefore, lead to the establishment of stronger, more efficient, and more scalable edge computing frameworks to increase both security and performance in edge computing systems in the future.

III. METHODOLOGY

Research in the past few years has been oriented toward integration: machine learning and deep learning models for enhanced security and scalability in edge computing. The edge computing environment is inherently characterized by scarce computational resources, enhanced security threats, and low latency, and innovative solutions are needed. It synthesizes recent developments in this area and explores the deployment of ML and DL models to tackle these challenges. Edge computing has obviously emerged as one of the most interesting paradigms able to sustain the growing requirements of Internet of Things applications by providing decentralized data processing closer to the source of data. This shift, however, brings along a lot of new security challenges related to the integration of Blockchain technologies. According to [1], the smart eHealth framework SSEHCET introduced the capabilities of some of the modern technologies such as IoT, 5G, and mobile edge computing in solving the challenge of secure transmission of data. The work underlines the very important function of BCT in protecting patient data, especially at the time when quick consensus is expected and the environment requires very stringent privacy standards. The six-layer architecture of SSEHCET proposed highlights multilayer security approaches in edge computing. For MEC, [2] proposed scheduling for optimizing system response time and energy consumption using deep reinforcement learning, guaranteeing that data is secure. This research showed how an ML model could be utilized for managing the dynamism and resource constraint-based edge environment. The authors brought forth a deep learningbased optimization technique for secure data transfer using collaboration and hybrid federated server-based stochastic vector networks. It has been shown that, by integrating DL models into the enhancement of network security, improvements in throughput, latency, and energy consumption are very real under unstable networks and a larger attack surface.

According to [4], increasing attention to blockchain technology in edge computing has driven some opportunities and challenges. In this paper, a method for detecting blockchain nodes has been proposed as T2A2vec for malicious node identification and mitigation in the network against security threats. In the current study, a BP neural network and a random walk strategy for feature extraction have been applied to reveal the potential of DL models in enriching reliability and security for blockchain-based edge computing systems. This necessitates real-time intrusion detection in the Industrial Internet of Things. The authors of [5] sought to improve the accuracy of intrusion detection techniques by using machine learning models such as PSO and PCA. They showed that the deployment of these models at edge devices, more so in resourceconstrained scenarios, would not only reduce latency but also be accurate enough. The present paper focuses on the role of ML in preventing cyber-attacks within IIoT environments. The authors of [6] commented that nextgeneration silicon chips at the edge represent a very challenging field of hardware security, and security needs to be ubiquitous. The authors have proposed some innovative design principles that include immersed-inlogic and in-memory security approaches, which can integrate ML at the hardware level. This work underlines the necessity of ML models designed for adaptation to new, emerging security threats, especially in large-scale distributed systems with large attack surfaces.

Edge computing, combined with secure message transmission protocols, is important from both safety and privacy points of view in vehicular networks. In, an edge computing-based security protocol has been proposed with attribute-based encryption and a reconfigured cryptographic scheme. This paper shows how machine learning models find their applications not only in the optimization of resource allocation but also in guaranteeing secure communications over very resourceconstrained vehicular networks. This effort underlines the tight interaction among machine learning, security, resource management in edge computing and environments. In [9], further research into cloud-edge computing addresses privacy and deployment challenges, and introduces a cryptographic primitive called Controllable Outsourced Attribute-Based Proxy Re-Encryption. The approach of this paper is to realize bilateral and distributed access control via ML models. Accordingly, data privacy and verifiability are expressed by their edge computing system. This work exemplifies the efficacy of ML in managing the intricacies of secure data outsourcing and cross-platform deployment. In [10], a comprehensive survey on edge computing security has been done where the authors have taken an in-depth review of various attack surfaces and defense mechanisms. The authors argue that robust ML models are needed to take care of the dynamically changing

security threats in edge computing that result from increased connectivity and distributed nature in edge environments.

In vehicular networks, the implementation of edge nodes for secure video-reporting services has been studied using ML models for optimized message verification and classification, as in [11]. This will be beneficial in terms of cost from computation on the cloud and a reduction in the storage footprint, pointing towards the way ML could bring security and effectiveness into 5G-powered vehicular networks. In other words, intelligent transport systems are one of the most important things located in the automotive sector, so security guarantees for safe operation are built in teleinformatic systems. The work in [12] was based on new evaluation methodologies concerning network security and gave rise to the importance of ML models in ensuring the safety of automotive edge computing systems. This study draws attention to security evaluations on multi-levels and the application of ML toward all-embracing security guarantees. In the edge computing framework, [13] proposed the AADEC (Anonymous and Auditable Distributed Access Control) framework for solving issues, including privacy leakage and fake data broadcasting. The framework proposed herein integrates machine learning models for conditional anonymous authentication and auditable attribute-based encryption, indicating the balance among anonymity, confidentiality, and auditability in edge computing systems. For instance, ML models were addressed in terms of optimal secure information capacity and local computation delay in Vehicular Edge Computing (VEC) systems. The authors adopted a general Benders-style decomposition to simultaneously optimize multiple factors, and the experimental results indicate the effectiveness of ML application to enhance security and fairness among VEC.

Another consideration is about the adaptability of the model of security evaluation to resource-constrained edge information systems. The authors of [15] proposed a new improvement in the PCA-S method for index screening and introduced a fuzzy comprehensive evaluation model for balancing energy consumption with performance. This work shows the usefulness of ML in refining security evaluation processes and reducing resource consumption in edge computing systems. In [16], a new, invasive, task offloading framework that can handle security and load balancing challenges connected with ECC is presented. In particular, this work demonstrates how ML in ECC systems has the potential to allow energy savings and latency reduction by using

advanced encryption standards and utilizing ML-based load-balancing algorithms. It was discussed in [17] that using ML models in edge-cloud environments to schedule tasks, particularly in scenarios with very stringent security requirements, where the authors proposed a scheduling framework closely balancing the response time with security. It has been shown that ML is a solution for the optimization of task scheduling in edge-cloud environments that have very high security requirements. Data deduplication in edge-assisted cloud storage systems is very important for ML. The work in [18] introduced a security-aware deduplication scheme that leverages ML models for balancing deduplication efficiency and protection against frequency analysis attacks. This underscores the importance of ML in enhancing data security while keeping system efficiency. Finally, it brings out the significance of ML to enhance data security level while keeping the efficiency of the whole system. This is established in works [19, 20], where it is shown that ML could provide optimizations to the authentication security levels, hence making any kind of secure computations over the social IoT systems possible. Both studies demonstrate the potential that the ML models have in addressing challenges and ensuring secure and efficient operations unique to the nature of the edge computing environment within resourceconstrained settings.

|--|

Sr.	Method	Findings	Strengths	Limitation
No	Used	_	_	s
1)	Smart	Enhanced	Comprehe	Limited by
	and	security	nsive	the
	Secure	and	multi-	inability of
	eHealth	privacy in	layered	Blockchain
	Framewo	eHealth	architectu	to store
	rk	data	re; strong	large IoT-
	(SSEHC	transmissi	privacy	generated
	ET)	on and	protection	data,
	leveragin	processin	using	requiring
	g IoT,	g;	Blockchai	external
	5G,	demonstr	n	storage
	mobile	ated		solutions
	edge	exception		
	computin	al		
	g, and	performa		
	Blockcha	nce in a		
	in	case		
	technolog	study		
	ies			
2)	Deep	Simultane	Effective	Potential
	reinforce	ous	load	complexity
	ment	optimizati	balancing	in
	learning-	on of	and	implementi
	based	system	security	ng DRL-

International Journal of Innovations in Engineering and Science, www.ijies.net

	110001	iunonui o	in nun of 1	into i difforms		8			ii ii iyresiire	
	secure	response	optimizati	based			in next-	focusing	low-cost	require
	offloadin	time and	on; real-	solutions			generatio	on	sensorizat	significant
	g	energy	time	in dynamic			n silicon	adaptive	ion for	redesign
	(DRLSO)	consumpt	adaptation	environme			chips	and	attack	efforts
	algorithm	ion while	of	nts				sustainabl	detection	
	in MEC	ensuring	objective					e security		
	environm	data	weights					measures		
	ent	security				7)	Edge	Ensured	Strong	Potential
3)	Deep	Improved	Effective	Increased			computin	secure	security	overhead
	learning-	network	combinati	energy			g-based	message	for	in
	based	security	on of deep	usage			security	transmissi	resource-	implementi
	optimizat	and data	learning	compared			protocol	on in	limited	ng
	ion and	privacy	and	to some			with fine-	vehicular	environm	reconfigure
	multiple	with	encryptio	other			grained	networks,	ents;	d
	encryptio	reduced	n	methods;			attribute-	addressin	efficient	cryptograp
	n	energy	technique	potential			based	g	use of	hic
	technique	consumpt	s; robust	overhead			encryptio	resource	edge	schemes
	s for	ion and	security	from			n	constraint	computin	
	secure	latency	analysis	multiple				s through	g for	
	data			encryption				offloadin	cryptogra	
	transfer			layers				g	phic	
	in edge-								operations	
	assisted					8)	Mobility-	Improved	Effective	Complexit
	IoT				-		aware	task	combinati	y in real-
4)	Blockcha	Enhanced	Strong	Complexit			task	offloadin	on of	time
	in node	security	security	y of neural			offloadin	g	security	adaptation
	detection	and	through	network			g scheme	efficiency	with	to channel
	method	reliability	advanced	implement			in MEC	by	energy	variations
	(T2A2ve	in	node	ation;			for	optimizin	and	and vehicle
	c) using	blockchai	detection	requires			autonom	g	latency	mobility
	BP neural	n-based	technique	extensive			ous	security,	optimizati	
	network	edge	s; use of	training			vehicles	latency,	on;	
	and	computin	neural	data				and	adaptabilit	
	random	g by	networks					energy	y to	
	walk	identifyin	for feature					consumpt	vehicle	
	strategy	g	extraction					ion	movement	
		malicious				9)	Controlla	Enhanced	Strong	Complexit
		nodes					ble	data	bilateral	y in
5)	Intrusion	Achieved	High	Potential			Outsourc	privacy	and	implement
	detection	100%	accuracy	resource			ed	and	distribute	ation; may
	using	accuracy	and	constraints			Attribute-	deployme	d access	require
	Particle	in	reduced	in			Based	nt	control;	high
	Swarm	intrusion	latency	implementi			Proxy	efficiency	comprehe	computatio
	Optimiza	detection	through	ng			Re-	in cloud-	nsive	nal
	tion	with	quantizati	complex			Encryptio	edge	verifiabilit	resources
	(PSO),	reduced	on;	ML			n	computin	У	on edge
	PCA, and	model	effective	models on			(COAB-	g		devices
	MARS in	latency	feature	edge			PRE) for	environm		
	IIoT		selection	devices			cloud-	ents		
			and				edge			
			reduction		1		computin			
6)	Design	Proposed	Comprehe	High			g			
	principles	methods	nsive	complexity		10)	Review	Provided	Thorough	Limited by
	for	for	security	in			and	a .	analysis	the scope
	ubiquitou	enhancin	approach	ımplementi			analysis	comprehe	of attack	of
	s and	g	covering	ng across			of	nsive	surfaces;	reviewed
	sustainab	hardware	physical	different			security	overview	identificat	literature;
	le	security	to	design			threats	of	10n of	may not
	hardware	at the	algorithmi	abstraction			and	security	future	cover
1	security	edge.	c levels:	s: may	1		defense	challenge	research	emerging

International Journal of Innovations in Engineering and Science, www.ijies.net

	.1 1	1	1'	.1 .	1	<u>a</u>	(1 1		1 1	1:00
	methods	s and	directions	threats			method	consumpt	reduced	different
	in edge	defense		comprehen			for	ion in	energy	edge
	computin	strategies		sively			security	security	consumpti	scenarios;
	g	in edge					evaluatio	evaluatio	on	limited
		computin					n in edge	n models		generalizab
		g					informati			ility
11)	Secure	Reduced	Low	Potential			on			
,	edge	authentic	authentica	limitations			systems			
	computin	ation	tion	in		16)	Security	Reduced	High	Potential
	computin a assisted	overbaad	overband	acalability		10)	load	Reduced	aalability	aomplayity
	g-assisted	overneau	overnead,	scalability			load halanaina	system	scalability	complexity
	video	and	efficient	with			balancing	energy	and	111 1 1 1
	reporting	storage	use of	increasing			, and	consumpt	energy	balancing
	service in	requireme	edge	network			energy-	ion while	savings;	multiple
	5G-	nts for	nodes for	size			aware	maintaini	comprehe	objectives
	enabled	real-time	local data				task	ng	nsive	simultaneo
	vehicular	video	processin				offloadin	security	security	usly
	networks	reporting	g				g	and load	framewor	-
12)	New	Proposed	Systemati	Limited to			framewor	balancing	k	
,	methodol	security	C C	the			k in ECC	8		
	ogies for	assurance	annroach	automotive		17)	Time and	Balanced	Effective	May face
	ovoluatin	stratogios	to	automotive		17)	socurity	rasponso	tosk	challongos
	evaluatiii	for the	10	sector,			security-	time and	task	in domentia
	g	for the	network	may not be			efficient	time and	schedunn	
	network	automotiv	assurance	generalizab			task	security	g; strong	and highly
	security	e sector	levels;	le to other			schedulin	for	performan	variable
	in	using 5G	applicabili	domains			g	applicatio	ce	environme
	automoti	networks	ty to				framewor	n service	compared	nts
	ve 5G		automotiv				k in	placemen	to other	
	applicatio		e				edge-	t in IoT	methods	
	ns		applicatio				cloud	systems		
			ns				environm	2		
13)	Anonym	Addresse	Balanced	Potential			ent			
,	ous and	d privacy	anonymit	trade-offs		18)	Security-	Improved	High	Potential
	Auditable	leakage	v	between			aware	deduplica	efficiency	trade-offs
	Distribut	and data	y, confidanti	officionav			aware	tion	in in	hotwoon
	Distribut	and uata	ality and	enticiency			afficient	officiency	III dadunliaat	occurity
	eu	spreading	anty, and				data	efficiency	ieuupiicat	
	Access	issues in	auditabilit	security;			data	and	101;	levels and
	Control	edge	y; strong	may			deduplica	reduced	strong	deduplicati
	Framewo	computin	performan	require			tion	informati	protection	on
	rk	g	ce	fine-tuning			scheme	on	against	efficiency
	(AADEC	environm	benchmar	for			for edge-	leakage in	frequency	
)	ents	ks	different			assisted	cloud	analysis	
				environme			cloud	storage	attacks	
				nts			storage			
14)	Max-min	Enhanced	Effective	Complexit		19)	Optimiza	Balanced	Effective	May
	optimizat	security	optimizati	vin			tion of	time	trade-off	require
	ion	and	on of	solving			authentic	delay and	between	significant
	problem	fairness	multiple	mixed			ation	security	security	computatio
	for secure	in	factors	integer			security	level in	and	nal
	informati	vehicular	applicabili	nonlinear			level in	computati	resource	resources
	on	odaa	ty to real	programmi			adaa	computati	ontimizati	for high
		euge	ty to real-	programmi			euge	OII	opumizati	
	capacity	computin	time	ng			computin	orrioadin	on; strong	security
	and local	g with	venicular	problems			g using	g	convergen	levels
	computat	optimized	environm				Merkle		ce in	
	ion delay	resource	ents				tree		simulation	
	in VEC	allocation			l		signature		S	
15)	PCA-	Improved	Effective	May		20)	Secure	Enhanced	Strong	May be
	SDC	adaptabili	screening	require			edge-	security	theoretical	challengin
	combinat	ty and	and	specific			aided	in	and	g to
	ion	reduced	evaluation	adaptations			computat	computati	experimen	implement
	screening	resource	process:	for			ion	on	tal	in highly
1	B		r-00000,		L			<u> </u>		BJ

International Journal of Innovations in Engineering and Science, www.ijies.net

	Interne		<i>un nun oj</i> 11			8			, in tyrestiter	1
	scheme	outsourci	support;	heterogene			edge	n systems		
	for social	ng for	robust	ous loT			computi			
	IoT	resource-	against	environme			ng			
	systems	constrain	identified	nts						
		ed IoT	security			[24]	ID-based	Achieved	Lightwei	May
		devices	threats				key	high	ght	involve
		-		-	-		agreeme	efficiency	protocols	complexit
Refei	Method	Findings	Strengths	Limitatio			nt	and	with	v in
ence	Used			ns			110		with	y 111
							protocols	security	strong	deployme
[21]	Batch	Improved	Lightwei	May not			for	in key	security	nt across
	authentic	data	ght and	address			blockcha	agreemen	properties	different
	ation	security	efficient	all types			in-	t	;	edge
	scheme	and	for	of			powered	protocols	applicabl	nodes and
	based on	reduced	resource-	security			intellige	while	e in	environm
	odgo	aomputati	aonstrain	throats in			nt edge	resisting	resource-	ents
	euge	computati					U	side-	constrain	
	computi	onal	ed llo1	nignly				channel	ed	
	ng for	overhead	devices	dynamic				ottoolse	anvironm	
	IIoT	in IIoT		IIoT				attacks	environini	
		environm		networks					ents	
		ents				[25]	Es devete	Enhanzal	A	T inside d
		through				[25]	Federate	Ennanced	Addresse	Limited
		batch					d	security	s key	by the
		authentic					Learning	and	challenge	current
		ation					model	efficiency	s in VEC	offloadin
		ation					for	in	environm	g
[22]	Lightwei	Ensured	Effective	May	-		computat	autonomo	ents;	systems;
[22]	abt	privoov	balanco	roquiro			ional	us	improves	challenge
	giit	privacy	batance	fina			offloadin	vehicular	model	s in
	privacy-	preservati	between	line-			σ and	networks	training	consistent
	preservin	on in	privacy	tuning for			resource	with	and	cloud
	g	medical	and	different			managa	fadaratad		cioud
	medical	data with	computati	medical			manage		resource	access
	diagnosi	efficient	onal	data types			ment in	learning	managem	
	s	real-time	efficiency	and edge			6G-VEC		ent	
	mechani	diagnosis	; secure	environm		[0.6]	D 1		C.	
	sm	on edge	and	ents		[26]	Deploym	Optimize	Strong	NP-hard
	(LPME)	devices	timelv				ent of Al	d the	optimizati	problem
	using		diagnosis				service	deployme	on	complexit
	XGRoos		angilosis				chains	nt of	technique	y; may
	+						(AISCs)	VNFs	s;	require
	L L						on	and	effective	significan
[23]	Stochasti	Enhanced	Strong	Complexi			trusted	BVNFs,	in real-	t
[23]	Stochasti		mothemat	ty in real			edge	enhancin	time edge	computati
	ر منطق	security	inauternat	ty III feal-			servers	g	computin	onal
	amerenti	in edge	1cal	world			in EIC	eliability	σ	resources
	al game	computin	toundatio	ımplemen			milit	and	5 scenarios	105001005
	theory	g by	n;	tation and					scenarios	
	for	modeling	effective	scalabilit				security		
	security	attack	in	У				in edge		
	analysis	and	revealing					intelligen		
	in	defense	security					ce cloud		
	blockcha	strategies	factors in					environm		
	in_	in	blockchai					ents		
	anablad	blockshei	nevetore							
	enabled	DIOCKCHIAI	n systems							
L		1	1	1	1					

International Journal of Innovations in Engineering and Science, www.ijies.net

[27]	Reputati	Reduced	Effective	Potential]	8	r Edge	by	ents:	operation
[27]	on	detection	in	vulnerabil			Computi	supportin	scalable	s
	incentive	overhead	reducing	ities if			ng	g re write	storage	5
	schama	while	overhead	reputation			ng	operation	solutions	
	(RIFTD)	maintaini	and	evetome				s and	solutions	
	(KILTD)	maintaini	incontiviz	systems				vorifiable		
	node	detection	ing	are				quarias		
	noue		ing han aat	comptom				queries		
	urusi	capability	hohovior	Ised		[31]	Privacy	Balanced	Effective	Potential
	evaluatio	by Lesson sin	benavior;			[31]	Protectio	privacy	protection	challenge
	n	leveragin	suitable				n	security	of	s in
		g	Ior .				Scheme	and	gradient	dynamic
		reputation	cooperati				for	efficiency	privacy:	edge
		-based	ve edge				Federate	in IoMT	resistant	environm
		incentives	environm				d	applicatio	to	ents with
			ents				Loorning	applicatio	collusion	vorving
[28]	Fromouv	Improved	Strong	May face	-		under	fodorated	attacks	data typos
[20]	ork for	socurity	onoruntio	limitation			Edgo	loorning	attacks	uala types
		and	encryptio	ain			Computi	learning		
	HoT task	nrivacy in	technique	anvironm			ng			
	nrocessi	HoT tasks	e.	ents with			(PPFI F			
	ng using	with	s, effective	extremely			(ITTLL C)			
	liohtwei	reduced	in	constrain			0)			
	oht	time	maintaini	ed		[32]	Privacy-	Enhanced	Strong	May
	encrynti	complexit	no	resources			preservin	privacy	security	require
	on and	v and	privacy	resources			g data	and	through	significan
	digital	latency	and				aggregati	reduced	cryptogra	t
	signature	futche y	security				on	computati	phic	computati
	schemes		in HoT				scheme	onal cost	technique	onal
	Sentennes						using	in IIoT	s;	resources
[29]	Secure	Provided	Compreh	Potential			Paillier	data	efficient	for large-
	batch	robust	ensive	complexit			cryptosy	aggregati	batch	scale IIoT
	authentic	security	security	y in			stem in	on	verificati	deployme
	ation	against	measures;	implemen			edge-		on	nts
	scheme	various	effective	tation and			supporte			
	for 5G-	attacks	in high-	scalabilit			d IIoT			
	enabled	while	bandwidt	y across						
	ITS	maintaini	h and	large ITS		[33]	Identity	Ensured	Strong	May face
		ng	real-time	networks			authentic	secure	security	challenge
		authentic	ITS				ated	and	proofs;	s in
		ation and	environm				protocol	anonymo	suitable	scalabilit
		continuit	ents				with	us	tor real-	y and
		y in MEC					provable	communi	time data	adaptatio
		environm					security	cation in	processin	n to
		ents					and .	MEC	g in MEC	diverse
[20]		F 1 1	TT' 1		-		anonymi	environm		MEC use
[30]	Acce-	Enhanced	Hıgh	Complexi			ty for	ents with		cases
	chain:	data	service	ty in			MEC	low		
	storage-	security	quality in	managing				computati		
	elastic	and query	latency-	DIOCKChai				onal		
	DIOCKCha	erriciency	sensitive	n storage				overhead		
	In for	in vec	VEC	and						
	Vehicula	systems	environm	rewrite						

International Journal of Innovations in Engineering and Science, www.ijies.net

	Interno	анопан зон	ırnaı oj 1n	novations	in En	igineeri	ng ana sc	ience, wn	vw.ijies.nei	
[34]	Certifica	Improved	Superior	May be			ng	detection		ents
	teless	security	security	less				accuracy		
	signcrypt	and	with	effective						
	ion	reduced	lower	in highly		[38]	Certifica	Enhanced	Strong	May
	strategy	computati	computati	dynamic			te-based	secure	cryptogra	require
	using	onal	onal and	or			ring	communi	phic	specialize
	hyperelli	requireme	communi	complex			signcrypt	cation in	security	d
	ptic	nts in	cation	vehicular			ion	UAV	with	infrastruc
	curve	VNDN	overheads	environm			scheme	networks	lower key	ture for
	cryptosy	environm		ents			for UAV	with	sizes;	implemen
	stem in	ents					networks	reduced	effective	tation and
	Vehicula						in	response	in	scaling
	r-NDN						private	times	dynamic	
							edge		UAV	
[35]	Blockch	Mitigated	Effective	Complexi			computi		environm	
	ain-	storage	in	ty in			ng		ents	
	based	burdens	securing	managing						
	fog	and	large	dual		[39]	Storage	Optimize	High	Complexi
	computi	enhanced	volumes	encryptio			resource	d storage	efficiency	ty in
	ng	transactio	of	n and			collabora	resource	and	solving
	service	n security	sensitive	steganogr			tion	allocation	performa	optimizat
	solution	in IoT	data; high	aphic			model	and	nce in	on
	using	and edge	transmissi	technique			for edge	collaborat	storage	problems
	IPFS and	computin	on	s			federatio	ion	managem	and
	stream	g	capacity				n	among	ent;	implemen
	cipher	environm	1 1				services	edge	scalable	ting
	encrypti	ents						nodes in	solution	across
	on							federated		federated
								environm		networks
[36]	Permissi	Balanced	Strong	May				ents		
	oned	security	performa	require					~	
	blockcha	and	nce in	significan		[40]	Al-	Provided	Strong	May face
	in and	energy	optimizin	t			driven	a	integratio	challenge
	DRL-	efficiency	g security	infrastruc			survey	comprehe	n of Al	s in real-
	empower	in H-IoT	and	ture			of	nsive	with	world
	ed H-IoT	systems	energy	support			security	analysis	MEC	applicatio
	system	for real-	usage;	for			and	of	security;	n and
	for	time	applicabl	deployme			privacy	security	addresses	integratio
	COVID-	pandemic	e in	nt and			in MEC	and	complex	n of AI
	19	response	health	scaling				privacy	and	with
			crises					issues in	emerging	MEC
								MEC,	threats	framewor
[37]	Per-edge	Reduced	Efficient	Potential				proposing		ks
	one-	communi	and	limitation				AI-based		
	round	cation	scalable	s in				solutions		
	EDI	overhead	EDI	adapting						
	scheme	and time	solution;	to diverse						
	(OR-	consumpt	addresses	mobile		Table ?	. Empirical I	Review of Fx	isting Metho	ds
	EDI) for	ion while	common	edge		1 4010 2	. Empirical I		isting metho	
	mobile	maintaini	EDI	computin		In parti	cular, Vehic	ular-NDN su	uffers from the	he presence
	edge	ng high	challenge	g		of delay	ys in data v	erification w	ithin vehicula	ar networks
	computi	corruptio	S	environm		in the n	ovel commu	inication arcl	hitecture of N	Named Data
		n								

International Journal of Innovations in Engineering and Science, www.ijies.net

Networking. The lightweight certificateless signcryption strategy based on hyperelliptic curve cryptography described in [34] resolves these challenges with very low computational and communicational complexities while ensuring better security in this regard. This strategy is well-suited for environments where speed and security are critical, such as vehicular ad-hoc networks. Leveraging blockchain in a Fog computing environment within the IoT and Edge Computing setting can be a way to attain data privacy and security. In [35], a dependable fog computing service solution was proposed using IPFS, including stream cipher encryption, for safe storage and transmission of sensitive data. In this paper, it is shown that dual encryption can reduce storage burdens while increasing the security of transaction data in edge computing. The application of DRL and blockchain for H-IoT systems has been researched in, where authors solved the challenge of security and energy efficiency to manage COVID-19. It provides a comprehensive solution for striking a balance in security and energy efficiency of H-IoT systems, in the wake of a global health crisis, by integrating permissioned blockchain and system performance optimization using DRL.

Some critical challenges facing edge data integrity in mobile edge computing come from tremendous communication overhead that most of the existing schemes generate and suffer, and also from timeconsuming verification processes. To this respect, the OR-EDI scheme proposes a new verification structure, MVT, which dramatically reduces the communication overhead and at the same time decreases the time consumption while maintaining the corruption detection accuracy at a high level. The method thus manifests the power of effective verification techniques in ensuring data integrity within edge computing. Private edge computing is a developing paradigm wherein secure communication between unmanned aerial vehicles and edge clouds is important. The certificate-based ring signcryption scheme proposed by [38] used the logic of hyperelliptic curve cryptography for these communications; thus, with a single operation, this scheme provides both digital signatures and encryption. Formal and informal analyses validated the scheme's security and efficiency, showing its suitability for secure UAV communications in a private edge computing environment. Finally, the edge computing phase of edge federation service brings new challenges about the collaboration of storage resources between edge nodes. In [39], the authors proposed a storage resource collaboration model utilizing dynamic programming and

greedy auction algorithms to optimize storage resource allocation. Experimental results show the efficiency of mechanisms in handling edge node storage resources and underline the necessity of collaborative approaches in the Edge Federation service model. Finally, this integration of ML/DL models into edge computing systems has huge potential in terms of both security and scalability. The research done in this context proposes a myriad of new approaches toward mitigating some of the unique challenges of edge computing in security threats, resource constraints, and real-time processing. With the evolution of edge computing in full swing, ML and DL will play a very essential role in securing these systems and optimizing their performances for varied scenarios.

Refer ence	Method Used	Results	Efficien cy of Securit y and Scalabil ity in Edge Compu	Observat ions in terms of Enhanci ng Security and Scalabilit
			ting	y in Edge Computi ng
[1]	Smart and Secure eHealth Framework (SSEHCET)	Security: 95%, Usability : 92%, User Satisfact ion: 90%	High security and usability in eHealth applicati ons with efficient data handlin g	Effective integratio n of multiple technolog ies (IoT, 5G, BCT) for secure, scalable eHealth solutions
[2]	DRL-based Secure Offloading (DRLSO)	System Respons e Time: 85%, Energy Consum ption: 78%	Good balance of security and system efficien cy in mobile edge computi ng	Strong performa nce in optimizin g response time and energy consumpt ion, suitable for diverse

International Journal of Innovations in Engineering and Science, www.ijies.net

131 Deep Learning- basedify Network Security: Moderat is bocurity: Demonstr ates bigh Security: Demonstr ates based 75% ed edge devices implemen tation 131 Deep Learning- based Security: Poto ates ates 10 Potomistr ates 10 10 Potomistr ates 10 10 10 Potomistr athoog 10 10 10				5	applicatio]	8		ment:	distribut	n. though
Image: security based is Security: based is Security: based is Security: Transfer Network is Security: c to sates potential is security of a security of a security of a security is security of a security of a security is security in in lot rechardle is security in reduced is security in reduced is security in in lot rechardle is security in reduced is security in reduced is security in in lot rechardle is security in reduced is security in in lot resource is security in reduced is sec					ns				75%	ed edge	implemen
[3] Deep Learning- based Network Moderat e Demonstr e Complexit yis complexit yis [4] Biockchain Node Maliciou e High socurity: Strong security scalable efficient furnamer Strong security Masage could be optimized further Efficient security Efficient security Efficient security Efficient security [4] Blockchain Node Maliciou securati High socurati Strong security Strong security Strong security Strong security Maliciou security High security Strong security [4] Blockchain Node Maliciou socurati High security Strong security Strong security Strong security Maliciou security High security Strong security Maliciou security High security Strong security Stro										devices	tation
Learning- based Security: e to 88%, security: e to 88%, security: e to 88%, security: e to 88%, security: e to 88%, security: e to 88%, security: for secure and char based 107 e date security: for secure and char based 107 for secure and char based 107 for secure computing: for secure and based 107 for secure and char based 107 for secure computing: for secure based 107 for secure and char based 107 for secure and based 107 for secure and based 107 for secure and based 107 for secure based 107 for secure basecurity 107	[3]	Deep	Network	Moderat	Demonstr						complexit
based Scure Data Trunsfer 88%, Encryy User S5-62% high Encryy with scurity S5-62% high Encryy with and scalable efficient trunsfer potential for scure and scalable trunsfer (7) Edge Computing- based Security 90%, 90%, 90%, 90%, 90%, 90%, 90%, 90%,		Learning-	Security:	e to	ates						vis
Secure Data Transfer Energy Usage: Usage: 55-62% socurity for secure and data based for in hor in hor in hor in hor in hor in torwork, threads base in computation in potention in transfer Efficien application application in transfer Efficien application application in transfer Efficien application in transfer Efficien atom in transfer Efficien in transfer Efficien in		based	88%.	high	potential						significan
Image: with and and and cerrgy- scalable efficient in b5 network and and and adat scalable efficient in b5 network and and adat scalable efficient in b5 network Image: scalable data applicatio in b5 network Image: scalable transfer in b5 network <th></th> <th>Secure Data</th> <th>Energy</th> <th>security</th> <th>for secure</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>significan</th>		Secure Data	Energy	security	for secure						significan
[4] Blockchain (T2A2vec) Maliciou s Node Detection (T2A2vec) High Accurac g Strong efficient in IoT Strong accurac g edge optimized further [7] Edge Computing- Based Message Confide Security Efficient in vehicle Efficient in vehicle [4] Blockchain (T2A2vec) Maliciou s Node Detection (T2A2vec) High Accurac g Strong accurac g Strong edge edge security Strong accurac g Mobility- acrons Latency security Balance focus on though accurac Strong accurac g [5] Intrusion Accurac g Accurac g edge edge security accurac g edge edge security Mobility- accurac Latency security Balance and overhead technolo gy Strong accurac [5] Intrusion Accurac g Accurac g Excerpti and overhead technolo High accurac Accurac gy concern and overhead technolo Strong accurac [6] Intrusion Accurac Accurac gy Excerpti and accurac High accurac High accurac Fificient further Good and ein dynamic [6] Ubiquitous furdavar Attack furdavar High accurity in IIOT Focus on accurity systems Focus on accurac Fificient further Addresse accurity in Voticular [6] Ubiquitous further Attack further g High accurac Focus on gystems Focus on gystems Focus on		Transfer	Usage:	with	and						ι
[4] Blockchain Node Detection Node Detection (T2A2vec) Maliciou and Node Detection Node Node Node Node Node Node Node Node		Tunster	55-62%	energy-	scalable		[7]	Edge	Message	Efficien	Effective
[4] Blockchain Node Detection Maliciou s High scurrac s strong eduction n Strong scurring scurring s Computing based Computing based Computing scurring scuring scurring scuring scurring scuring scurring scurring scu			55 0270	efficient	edge-		[,]	Computing_	Confide	t	in
[4] Blockchain Node S Node (T2A2vec) Maliciou n High s Strong scurac energy usage could be optimized further Strong s Strong				data	based IoT			based	ntiality	socurity	socuring
Image: Intermediate approximation of the section o				transfor				Socurity		protocol	in vahiala
Image: Instruction of the security in the secu					applicatio			Droto col	50%, Enomenti	protocol	
Image: Security in threatsInducation of though in the security in threatsImage in the security in threatsImage in though in though in the security in threatsImage in though in though in the security in threatsImage in though in though in the security in threatsImage in though in though in the security in threatsImage in though in though in the security in threatsImage in though in the security in the security in threatsImage in the security i					118,			Protocol	Енстури	with	communi
[4] Blockchain Node Detection (T2A2vec) Maliciou s Node Detection (T2A2vec) High s Node Detection (T2A2vec) High s Node Detection (T2A2vec) Strong s currac Accurac y: 93% Strong s ecurity security with computati blockch ain security with computati blockch ain blockch Maliciou s Node security y in security security with computati blockch ain security with computati blockch in IIOT systems Mobility- security networks, threats security with computati blockch ain security with computati blockch in IIOT systems Mobility- security networks, threats security with computati blockch in IIOT systems Latency security networks, threats blockch in IIOT systems Latency security it a robusti in IIOT systems Latency security it a robusti in IIOT systems Latency security security it a robusti in IIOT systems Latency security it a robusti in IIOT systems Intrusion security it a robusti in IIOT systems Accurac security it a robusti in IIOT systems Focus on security it a robusti in IIOT systems Data security security it a robusti security it a robusti in IIOT systems OcoAB- security it a robusti in IIOT systems Data security security it a robusti in IIOT systems Mobility- security it a robusti in IIOT systems Data security it a robusti in IIOT systems Data security it a robusti it a robu				network	though				on	moderat	cations,
[4]Blockchain Node s Node Detection (T2A2vec)Maliciou s Node s Node potentioHigh cacurac capability in in in edgeStrong accurac capability in <th></th> <th></th> <th></th> <th>S</th> <th>energy</th> <th></th> <th></th> <th></th> <th>Overhea</th> <th>e</th> <th>though</th>				S	energy				Overhea	e	though
Image: security in the securit					usage				d: 15%	overhea	additional
Image: book of the section of the s					could be					d	resources
[4]Blockchain Node Detection (T2A2vec)Maliciou s Node s Node Detection (T2A2vec)High accurac g g edge security networks, thrats though with computati blockch onal ain overhead technoloStrong accurac g g edge security networks, thrats though with computati blockchMobility- aware Task Offloading n: 35%, SchemeBalance d d metworks, metworks, thratsStrong accurac the edge overhead technolo[5]Intrusion using ML (PSO+PCA +MARS)Accurac profer scurityExcepti and efficienty in IIoT solution environ for real- mentsFigh potentia in IIoT solution environ for real- mentsStrong aware Task offloading motworks, that accuracy and motworks, scurityIntrusion potentia in IIoT solution environ for real- mentsIstact potentia in IIoT solution environ for real- mentsIstact potentia in IIoT solution environ in IIoT solution environ <th></th> <th></th> <th></th> <th></th> <th>optimized</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>may be</th>					optimized						may be
[4]Blockchain Node DetectionMaliciou s Node betectioHigh accurac y inStrong capability y infor high performa nce[4]Blockchain DetectionNode DetectionHigh scurac y inStrong accurac g edge withMobility- aware TaskLatency adware TaskBalance approacStrong accurac y escurity measures[4]Blockchain Detectionndetectin security with ecomputati blockch onal accurac gyconverhead technolo[8]Mobility- aware TaskLatency adware TaskBalance approac measuresStrong ascurat measures[5]Intrusion Detection y: 100%, Latency Models (PSO+PCA +MARS)Accurac y: 25%Excepti vith efficienty reduced in IIoT solution environ for real- mentsMobility- taskLatency offloading n: 25%Balance accuracy scurity and accuracy scurity in IIoT solution environSchemeEatency offloading n: 25%Strong aware Task advare accuracy it a robust in IIoT solution environ[9]COAB- For Privacy: SecurityScood advare security scurity[6]Ubiquitous Hardware ScurityAttack potentia hardware y scurityHigh potentia hardware y scurityFor cos on potentia hardware y scurity y scurityData potentia potentia hardware y scurity y scurity robustComputing potentiaCoad- potentiaCoad- potentia[further						needed
[4] Blockchain Maliciou High Strong accurac capability in nce performa nce Node S Node Detection Detection security in detectin security aware Task Reductio d security minimizia [5] Intrusion Accurac Excepti High orceracy security and aditon, aditon, aditon, aditon, applicabl e in gy consumpt aditon, applicabl e in gy aditon, applicabl e in dynamic applicabl e in gy aditon, applicabl e in gy security in, </th <th>5.47</th> <th>D1 1 1 .</th> <th>26.12.2</th> <th>TT' 1</th> <th><u> </u></th> <th>-</th> <th></th> <th></th> <th></th> <th></th> <th>for high</th>	5.47	D1 1 1 .	26.12.2	TT' 1	<u> </u>	-					for high
Nodes NodeaccuraccapabilityneceDetectionDetectioy ininnnece(T2A2vec)ndetectinsecuringedgeReductiodsecurityAccuracgedgenetworks,threatsthoughneasuresReductiodsecurityy: 93%sccuritynetworks,threatsthoughneasuresReductiodsecuritywithcomputatiblockchonalainoverheadcomputatiSchemeConsumsecurefocus on[5]IntrusionAccuracExceptiHighaccuracyautonoconsumptautonoconsumpt[5]IntrusionAccuracExceptiHighaccuracyautonoconsumptautonoconsumpt[6]IntrusionAccuracecurityandmg ineenergyapplicable in(PSO+PCAn: 25%reduced, makingit a robustin IIoTsystems[9]COABDataGoodAddresse[6]UbiquitousAttackHighFocus onmentsfimesecurityskeyopticable in[6]UbiquitousAttackHighfocus onnetworks,fineSecurityskeyopticable in[7]UbiquitousAttackHighfocus onnetworks,fineSecurityskeyopticable in[6]UbiquitousAttackH	[4]	Blockchain	Maliciou	High	Strong						performa
DetectionDetectiony inininin(T2A2vec)ndetectinsecuringedgeaware TaskReductiodsecurityy: 93%securitynetworks,threatsthoughwithconsumsecurityaware TaskReductiodsecurityy: 93%securitynetworks,threatsthoughwithconsumsecurityaware TaskReductiodsecurityinoreheadinoverheadinoverheadinoverheadinfileinfileinisIntrusionAccuracExceptiHighonalaccuracyautonoconsumptautonoconsumptisIntrusionAccuracExceptiHighaccuracyinonalaccuracyinautonoconsumptisIntrusionAccuracExceptiHighonalaccuracyininonalaccuracyinautonoconsumptisIntrusionAccuracExceptiHighrobustin <t< th=""><th></th><th>Node</th><th>s Node</th><th>accurac</th><th>capability</th><th></th><th></th><th></th><th></th><th></th><th>nce</th></t<>		Node	s Node	accurac	capability						nce
(T2A2vec)ndetectinsecuring[8]Mobility-LatencyBalanceStrongy: 93%securitynetworks,threatsthoughaware TaskReductiodsecurityy: 93%securitynetworks,threatsthoughwithcomputatiOffloadingn: 35%,approacmeasureswithcomputatiblockchonalainoverheadicchnolomadminimiziandminimiziainoverheadtechnolomay be agyconcern70%efficientngandjoingModelsAccuracExceptiHighaccuracyandng inenergyconsumpt[5]IntrusionAccuracsecurityandaccuracyandng inenergyion,ModelsReductiowithefficiencyin a robustin IloTsolutionenindynamicenin(PSO+PCAn: 25%reductioin IloTsolutionin IloTsolutionenindynamicenits[6]UbiquitousAttackHighFocus onin IloTsystemsfilCOAB-DataGoodAddresse[6]UbiquitousAttackHighfocus onin IloTsecuritysecuritysecuritysecuritysecurity[6]UbiquitousAttackHighfocus onmentgoodsecuritysecuritysecurity[6]UbiquitousAt		Detection	Detectio	y in	in						
Accuracgedgey: 93%securitynetworks,threatsthreatsthoughwithcomputatiblockchonalainoverheadtechnolomay be agyconcern[5]IntrusionAccuracusing MLLatencyy: 100%,onalusing MLLatencyy: 00%,reduced(PSO+PCA)n: 25%+MARS)n: 25%reducedin loTsolutionenvironmentstimesecurityin loTsolutionsecurityin loTsolutionenvironfor real-in loTsystems[6]UbiquitousHardwareSurfaceReductiol forn: 80%,sustainasecuritylofersysecurityysecurityin loTsolutionenvironforesgsecuritylatencyin loTsystems[6]UbiquitousHardwareSurfacesecuritylofersysecuritybe differsysecurityysecurityin lorsecurityin lorsecurityin lorsecurityin lorsecurityin lorsecurityin lorsecurityin lor <t< th=""><th></th><th>(T2A2vec)</th><th>n</th><th>detectin</th><th>securing</th><th></th><th>[8]</th><th>Mobility-</th><th>Latency</th><th>Balance</th><th>Strong</th></t<>		(T2A2vec)	n	detectin	securing		[8]	Mobility-	Latency	Balance	Strong
y: 93%security threatsnetworks, threatsOffloading threatsn: 35%, Energyaproac measuresmeasures with a secure[5]Intrusion Detection using ML (PSO+PCA +MARS)Accurac securityExcepti onal accuracy securityHigh accuracy and efficiency it a robust in IIoT solution environ for real- timeN: 35%, securityaproac measures with a consumpt efficient minimizid and minimizid autono consumpt energy autono consumpt mousn: add minimizid and minimizid autono consumpt mous ion, applicabl e in dynamic vehiclesn: add minimizid autono consumpt mous ion, applicabl e in dynamic vehicles[6]Ubiquitous Hardware SecurityAttack Reductio n: 80%, sustaina SecurityHigh accuracy systemsFocus on ments[6]Ubiquitous Hardware SecurityAttack Reductio n: 80%, sustaina securityFocus on hardware securityFocus on hardware securityFocus on hardware security[6]Ubiquitous Hardware SecurityAttack Reductio n: 80%, sustaina securityHigh socurity robustFocus on hardware security[6]Ubiquitous Hardware SecurityAttack potentia hardware securityHigh socurity robustFocus on hardware hardware securityFocus on hardware hardware security[6]Ubiquitous systemsAttack potentia hardware securityHigh socurity robust <th></th> <th></th> <th>Accurac</th> <th>g</th> <th>edge</th> <th></th> <th></th> <th>aware Task</th> <th>Reductio</th> <th>d</th> <th>security</th>			Accurac	g	edge			aware Task	Reductio	d	security
Image: book of the security of			y: 93%	security	networks,			Offloading	n: 35%,	approac	measures
Image: secure biological secure				threats	though			Scheme	Energy	h for	with a
Image: blockchonal ainoverhead overhead technolooverhead ainption:andminimizi ng70%efficient reductiomg radtomaddmg radtomaddmg radtomadd[5]Intrusion using ML ModelsAccurac y: 100%, using ML HARS)Excepti reduced latencyHigh and ecurity in IIoT solution environaddmdmg in energy consumpt mous[6]Ubiquitous Hardware SecurityAttack rudeHigh reduced in radtom in IIoT solution environ environfor real- ments[9]COAB- PRE for Cloud-Edge ComputingData reduced security efficient environm environ environGood skeyAddresse skey[6]Ubiquitous Hardware SecurityAttack rudeHigh roduced in IIoT sustaina security in IIoTFocus on hardware rude[9]COAB- PRE for ComputingData rude security rude rudeGood skey scurity rudeAddresse skey rude[6]Ubiquitous Hardware SecurityAttack rudeHigh rodus rude rudeFocus on hardware rude[9]COAB- rude rude rude rudeGood rude rude rude rudeAddresse rude[6]Ubiquitous rude y securityAttack rude rude rudeHigh rude rude rude rude rude rudeFocus on rude rude rude rude rude rudeIntercy rude rude rude rude rude rude 				with	computati				Consum	secure	focus on
[5]Intrusion Detection using ML ModelsAccurac ExceptiExcepti High accuracy and efficiency making in IIOT for real- imentsHigh accuracy and efficiency making it a robust in IIOT solution for real- time securityFocus on hardware70% making efficient mous ion, wehicles vehiclesefficient and erency autono consumpt mous ion, applicabl e in dynamic vehicles[6]Ubiquitous Hardware SecurityAttack ReductioHigh potentia hardware Surface potentiaFocus on hardware security robust in Solution for real- time security[9]COAB- PRE for Cloud-Edge SwfmData security security skey with privacy: scurityGood Addresse security skey offloadi e in dynamic vehicles[6]Ubiquitous Hardware SecurityAttack Reductio I for sustaina y scurity in Be offers in IIoTFocus on hardware security scurity robust[9]COAB- conputingData scalabilit genesGood concerns, ment in IIoT scalabilit scalabilit y scurity[6]Ubiquitous y y scurityAttack potentia hardware scurity y scurityFocus on hardware scurity scurity robustMata concerns, ment in IIoT in IIoT scalabilit scalabilit scalabilit scalabilit scalabilit scalabilit in IIoT in IIoT i				blockch	onal				ption:	and	minimizi
Image: securitytechnolomay be a gyitechnolomay be a gyitechnoloitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnoloitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnolomay be a gyitechnoloitechnolomay be a gyitechnoloitechnolomay be a gy[5]IntrusionActackMideif itechnoloif a robust in IIOTif a robust in IIOTif a robust in IIOT[9]COAB- gyDataGoodAddresse gyAddresse[6]UbiquitousAttackHigh potentiaFocus on hardwarement in IIOTsecurity in IIOTFocus on hardwarement in scalabilitscalabilit gy acrossgel diverse gy acrossgel diverse gy acrossgel diverse gy across </th <th></th> <th></th> <th></th> <th>ain</th> <th>overhead</th> <th></th> <th></th> <th></th> <th>70%</th> <th>efficient</th> <th>ng</th>				ain	overhead				70%	efficient	ng
Image: section of the section of th				technolo	may be a					task	latency
Image: constraint of the constra				gy	concern					offloadi	and
[5]IntrusionAccuracExceptiHigh accuracyDetectiony: 100%, y: 100%,onalaccuracy andandmousion, wehiclesUsing MLLatencysecurityandefficiency reduced, making it a robustvehiclesapplicabl e in dynamic(PSO+PCAn: 25%reduced, making it a robustin IIoTsolution environfor real- mentsin IIoTsolution environ(PSO+PCAN: 25%reducedin IIoTsolution environfor real- in IIoTin IIoTsolution environ(PSO+PCAAttackHighsecurity in IIoTin IIoTsolution environfor real- in IIoTfor ceal- in IIoTfor ceal- in IIoT[6]UbiquitousAttackHigh sustainaFocus on hardwarefor-backedFificienc securitygeotentia is security[6]UbiquitousAttackHigh sustainaFocus on hardwaresecurityif for is sustaina-backedif for is securitysecurity[6]UbiquitousAttackHigh sustainasecurityif for is sustainasecurityif for is securityif for is securitysecurity[6]UbiquitousAttackHigh sustainasecurityif for is securityif for is securitysecurityif for is securityif for is securitysecurityif for is securityif for is securityif for is securityi						-				ng in	energy
Detectiony: 100%,onalaccuracymousion,using MLLatencysecurityandefficiencywithefficiencyapplicablModelsReductiowithefficiency, makingieindynamic(PSO+PCAn: 25%reduced, makingiatencyit a robustwithefficiency+MARS)n: 25%reduced, makingiatencyit a robustwithenvironmenvironenvironfor real-in IIoTsolutionenvironmenvironmenvironenvironfor real-in IIoTsecurityin IIoTsecurityin IloTsystemssecurityin IIoTsystemsCooAB-DataGood[6]UbiquitousAttackHighFocus onPRE forPrivacy:securitys keyIfolUbiquitousAttackHighFocus onmentdeploythoughKardwareSurfacepotentiahardwaresecurityin ardwarey: 82%cloud-y acrossSecurityReductioI for-backediii <iiiiiiiiiiiiiiiiiiiiiiiiiiiiiii< th=""><th>[5]</th><th>Intrusion</th><th>Accurac</th><th>Excepti</th><th>Hıgh</th><th></th><th></th><th></th><th></th><th>autono</th><th>consumpt</th></iiiiiiiiiiiiiiiiiiiiiiiiiiiiiii<>	[5]	Intrusion	Accurac	Excepti	Hıgh					autono	consumpt
using MLLatencysecurityandvehiclesapplicablModelsReductiowithefficiency, makinge indynamic(PSO+PCAn: 25%reduced, makingit a robustit a robuste indynamic+MARS)latencyit a robustin IIoTsolutionenvironenvironmenvironmenvironenvironfor real-mentstimesecurity[9]COAB-DataGoodAddresseenvironenvironsecurityin IIoTsystems[9]COAB-Privacy:securitys key[6]UbiquitousAttackHighFocus onhardwareEfficiencmentdeploythough[6]UbiquitousAttackHighFocus onhardwarein scalability: 82%cloud-y across[6]UbiquitousAttackHighfocus onhardwarein scalability: 82%cloud-y across[6]UbiquitousAttackHighfocus onhardwarein scalability: 82%cloud-y across[6]UbiquitousAttackHighfocus onhardwarein scalability: 82%cloud-y across[6]UbiquitousAttackHighfocus onhardwarein scalability: 82%cloud-y across[6]UbiquitousAttackHighoffersin scalability: 82%cloud-y acrossedge		Detection	y: 100%,	onal	accuracy					mous	ion,
Models (PSO+PCA +MARS)Reductio n: 25%with reduced in IoT solution environ for real- mentsefficiency it a robust in IIoT solution environ for real- mentsefficiency it a robust in IIoT solution environ for real- mentsefficiency it a robust in IIoT solution environ for real- mentsefficiency it a robust in IIoT securityefficiency it a robust in IIoT securitye in dynamic vehicular environm environm ents[6]Ubiquitous Hardware SecurityAttack Reductio n: 80%, LongevitHigh tor tor tor bleFocus on hardware tor <br< th=""><th></th><th>using ML</th><th>Latency</th><th>security</th><th>and</th><th></th><th></th><th></th><th></th><th>vehicles</th><th>applicabl</th></br<>		using ML	Latency	security	and					vehicles	applicabl
(PSO+PCA +MARS)n: 25%reduced latency in IIoT environ ments, making it a robust solution environ for real- mentsdynamic vehicular environm environm for real- ments[6]Ubiquitous Hardware SecurityAttackHigh potentia 1 for sustaina security in 80%, sustainaFocus on hardware security in 80%, sustaina security[9]COAB- potentia computingData solution environm environm environm environm environm securityGood skeyAddresse skey[6]Ubiquitous hardware securityAttack potentia hardware securityFocus on hardware securitySurface potentia hardware securityFocus on hardware securityIf or real- securitySurface potentia hardware securityIf or real- securitySurface potentia hardware securityIf or real- potentia hardware securityIf or real- ble offersIf or real- bleIf or real- securityIf or real- ble offersIf or real- bleIf or real- real- bleIf or real- real- bleIf or real- real- real- bleIf or real- real- real- real- real- real- real- real- real- real-If or real- real- real- real- real- real- real- real- real-If or real- real- real- real- real- real- real- real- real- real- real- real-If or real- real- real- real- real- real- real- real- real-If or real- re		Models	Reductio	with	efficiency						e in
+MARS)latencyit a robustin IIoTsolutionin IIoTsolutionenvironfor real-in IIoTenvironmentstimesecurityin IIoTsecurity[9]COAB-DataGoodMarchKatackHighsecurityin IIoTPRE forPrivacy:securityskey[6]UbiquitousAttackHighFocus onMardwareMentdeployefficientconcerns,[6]UbiquitousAttackHighFocus onmentdeploythoughIfor-backedin for-backedin 80%,sustainasecurityiscurityedgediversein S0%,sustainasecurityin Berloyforsecurityiscurityedgediverseysecuritybleoffersysecurityin berloyin odesnodesin moreysecurityrobustin securityin securityin securityin securityin securityin securityin securityin securityin securityin morein securityin securityin securityin securityin securityin securityin securityin securityin securityin morein securityin secu		(PSO+PCA	n: 25%	reduced	, making						dynamic
Image: security in the security is the security in the security is the security in the security is the securit		+MARS)		latency	it a robust						vehicular
Image: security in the securit				in IIoT	solution						environm
Image: securitymentstimementstimeImage: securitysecuritysecuritysecurity[9]COAB-DataGoodAddresseImage: securityin IIoTsystemssystemsSecuritySecuritysecuritysecuritysecurityImage: securityAttackHighFocus onSecurityCloud-Edge88%,withprivacyImage: securityAttackHighFocus onmentdeployefficientconcerns,Image: securityReductio1 for-backedinSecurityget acrossget acrossget acrossget acrossget acrossinodesImage: securityysecurityrobustinoffersinodesinodesinodesinodesImage: securityimage: secu				environ	for real-						ents
Image: security in the security in the security in the security in the systems[9]COAB-DataGoodAddresseImage: security in the systemsin the systemsin the systemsPRE forPrivacy:securitys keyCloud-Edge88%,withprivacyConcerns,Image: securityAttackHighFocus onmentdeployefficientconcerns,Image: securityReductio1 for-backedin the securityin the securityin the securityy: 82%cloud-y acrossImage: securityLongevitbleoffersoffersin the securityin the securityin the securityin the securityImage: securityysecurityrobustin the securityin the securityin the securityin the securityImage: securityin the securityin the securityin the securityin the securityin the securityin the securityImage: securityin the securityin the securityin the securityin the securityin the securityin the securityImage: securityin the securityin the securityin the securityin the securityin the securityin the securityImage: securityin the securityin the securityin the securityin the securityin the securityin the securityImage: securityin the securityin the securityin the securityin the securityin the securityin the securityImage: securityin the sec				ments	time						
Image:					security		[9]	COAB-	Data	Good	Addresse
Image: securityImage: securitySustainaSecurityCloud-Edge88%,withprivacy[6]UbiquitousAttackHighFocus onComputingDeployefficientconcerns,[6]UbiquitousAttackHighFocus onmentdeploythoughHardwareSurfacepotentiahardwareEfficiencment inscalabilitSecurityReductio1 for-backediscurityiscurityedgediverseImage: securitybleoffersofferssecurityiscurityiscurityiscurityiscurityImage: securityindexysecurityrobustiscurityiscurityindexindexImage: securityindexprotectioiscurityiscurityiscurityiscurityiscurityiscurityImage: securityindexprotectioiscurityiscurityiscurityiscurityiscurityImage: securityindexprotectioiscurityiscurityiscurityiscurityiscurityImage: securityindexprotectioiscurityiscurityiscurityiscurityiscurityImage: securityindexprotectioiscurityiscurityiscurityiscurityiscurityImage: securityiscurityiscurityiscurityiscurityiscurityiscurityiscurityImage: securityiscurityiscurityiscurityiscurityiscurity<					in IIoT			PRE for	Privacy:	security	s key
Image: constraint of the securityImage: constraint of the securityComputingDeployefficientconcerns,[6]UbiquitousAttackHighFocus onmentdeploythoughHardwareSurfacepotentiahardwareEfficiencment inscalabilitSecurityReductio1 for-backedy: 82%cloud-y acrossin: 80%,sustainasecuritybleoffersedgediverseysecuritybleoffersnodesnodesimproveacrossprotectioindextindextnodes					systems			Cloud-Edge	88%,	with	privacy
[6]UbiquitousAttackHighFocus on hardwarementdeploythough scalabilitHardwareSurfacepotentiahardwareEfficiencment inscalabilitSecurityReductio1 for-backedy: 82%cloud-y acrossn: 80%,sustainasecurityLongevitbleofferssystemsedgeysecurityrobustnodesnodesnodesImproveacrossprotectioneedsneedsneeds								Computing	Deploy	efficient	concerns,
Hardware SecuritySurface Reductiopotentia 1 for 1 forhardware -backed securityEfficienc y: 82%ment in cloud- edge systemsscalabilit y acrossNote: Note	[6]	Ubiquitous	Attack	High	Focus on				ment	deploy	though
SecurityReductio1 for-backedn: 80%,sustainasecurityLongevitbleoffersysecurityrobustImproveacrossprotectio		Hardware	Surface	potentia	hardware				Efficienc	ment in	scalabilit
n: 80%,sustainasecurityedgediverseLongevitbleofferssystemsedgeysecurityrobustnodesImproveacrossprotectioneeds		Security	Reductio	1 for	-backed				y: 82%	cloud-	y across
LongevitbleofferssystemsedgeysecurityrobustnodesImproveacrossprotectioneeds			n: 80%,	sustaina	security				-	edge	diverse
y security robust Improve across protectio			Longevit	ble	offers					systems	edge
Improve across protectio needs			у	security	robust						nodes
needay			Improve	across	protectio						needs

International Journal of Innovations in Engineering and Science, www.ijies.net

			Ŭ	further]	[13]	AADEC	Anonym	Balance	Offers
				explorati			Framework	ity: 85%,	d	strong
				on				Confide	security	security
								ntiality:	with	with the
[10]	Edge	Attack	Detailed	Provides				90%,	auditabi	added
	Computing	Surface	insights	a solid				Auditabi	lity in	benefit of
	Security	Analysis	into	foundatio				lity: 80%	dynamic	auditabili
	Literature	:	security	n for					edge	ty,
	Review	Compre	challeng	understan					computi	though it
		hensive	es and	ding and					ng	may
			defense	addressin					environ	introduce
			mechani	g edge					ments	some
			sms in	computin						overhead
			edge	g						
			computi	security,		[14]	Max-Min	Secure	Efficien	Strong
			ng	though			Optimizatio	Informat	t	focus on
				lacks			n in VEC	ion	security	fairness
				experime				Capacity	with	and
				ntal				:92%,	minimiz	security,
				validation				Local	ed	though
					_			Computa	computa	the
[11]	Secure	Authenti	Low	Ensures				tion	tion	complexit
	Video	cation	overhea	real-time				Delay:	delay in	y of the
	Reporting	Overhea	d with	security				30%	vehicula	optimizat
	in 5G-	d: 15%,	efficient	with					r edge	ion
	enabled	Delay	security	reduced					computi	problem
	Vehicular	Reductio	in	delays,					ng	is a
	Networks	n: 20%	vehicula	though						limitation
			r	challenge						
			network	s may		[15]	PSDC-CVF	Energy	Efficien	Balances
			S	arise with			Security	Consum	t	energy
				scaling to			Evaluation	ption	security	and
				larger			Model	Reductio	evaluati	performa
				networks				n: 20%,	on with	nce well,
[12]	Committy	Accuron	High	Effective				Model	reduced	though
[12]	Assumance	Assuran	nigii	in				Adaptabi	energy	may
	Assurance	Levela	assuranc	III				lity:	consum	require
	III JUII S	Levels:	e with	providing				High	ption in	fine-
	INCLWOIKS	Multiple		security					edge	tuning for
			ovoluoti	certificati					systems	different
			evaluati	though						edge
			011 mathed	mool						scenarios
			alogios	Ical-		[16]	Socurity	Enorgy	Strong	Effective
			ologies	world		[10]	and Load	Source	Sublig	in large
				applicatio			Balancing	17 5	with	in large-
				Norv			in FCC	20.3%	significe	FCC
				val y			mecc	20.3%,	significa	Anvironm
				different				Reductio	III onorgy	onto
				ITC				n: 12	and	though
				anvironm				1. 1.3-	anu latonov	scalabilit
				ente				1770	improvo	scalabilit v to
				CIIIS					ments in	y w diverse
									Incins in	

International Journal of Innovations in E	ngineering and Science,	www.ijies.net
---	-------------------------	---------------

			, v	
			edge-	applicatio
			cloud	ns may
			environ	require
			ments	additional
				considera
				tion
[17]	Security-	Time	High	Balances
	aware Task	Efficienc	efficien	time and
	Scheduling	y: 85%,	cy with	security
		Security	improve	well,
		Ranking	d	though
		Improve	security	real-
		ment:	in edge-	world
		80%	cloud	validation
			task	across
			scheduli	different
			ng	IoT
			115	systems
				is needed
				is needed
[18]	Secure	Deduplic	Flexible	Provides
L - J	Deduplicati	ation	security	a scalable
	on Scheme	Efficienc	with	solution
	on benefite	v· 75%	efficient	for data-
		Security	data	heavy
		Loval	dedunlic	environm
		A diustab	ation at	chvitolilli
		Aujustau	the edge	though
		le	the edge	mough
				may
				require
				careful
				tuning of
				security
				levels
[10]	Morblo	Authonti	Strong	Effective
[17]	Troo	Autienti	socurity	for socure
	Signatura	Socurity	with	
	based	Loval	monogo	continuit
	Authoricat	0.00%	abla	though
	ion	9070, Timo	timo	ontimizin
	1011	Dolory	dologio	opunizin a the
		250/	adas	g uie
		23%	euge	hotmore
			network	between
			S	security
				and delay
				1s crucial
[20]	Secure	Security	High	Strong in
[20]	Edge aided	Complia		socurine
	Computatia	raa	security	securing
	Computatio		with	complex
	1	High,	efficient	computati

gineeri	ng unu sciel	ice, www	v.ijies.nei	
	n Scheme	Computa	computa	ons,
		tional	tion for	though
		Efficienc	resource	scalabilit
		y: 85%	-	y across
			constrai	various
			ned IoT	IoT
			devices	applicatio
				ns may
				be
				challengi
				ng

Table 3. Comparative Analysis of Existing Methods

The different methods applied to improve edge computing environments in terms of security and scalability make the scope and complexity of this field huge. Each of these methods offers some strengths in terms of high accuracy of security, low latency, or efficient resource management. However, there are limitations to these methods, including probably high implementation complexity, scalability problems, and security-performance metric trade-offs. Future research will be directed toward the integration of these strengths with mitigation of limitations to the reach comprehensive solutions that may enjoy wide applications across a wide array of edge computing scenarios. In particular, this comparative analysis delivers valuable insights to researchers and practitioners working for the advancement of security and scalability of edge computing systems. This paper is aimed at providing a comparative review of different techniques proposed to enhance the security and scalability of edge computing. In the process of analysis, every method will be evaluated against certain performance metrics that consider efficiency in security implementation, scalability across distributed systems, and overall system performance. The comparison approach is followed to underline the effectiveness of each method in solving the specific challenges in edge computing, mostly related to the IoT, IIoT, and other relevant emerging paradigms of distributed computing.

Refer	Method	Results	Efficienc	Observat
ence	Used		y of	ions in
			Security	terms of
			and	Enhanci
			Scalabili	ng
			ty in	Security

International Journal of Innovations in Engineering and Science, www.ijies.net

[21]	Batch Authenti cation Scheme for IIoT	Authentic ation Efficienc y: 85%, Computat ional Overhead Reductio n: 30%	Edge Computi ng High efficienc y in message authentic ation with reduced computat ional load	and Scalabilit y in Edge Computi ng Demonstr ates significan t improve ment in IIoT security with efficient batch processin g, ideal for	[24]	ID-based Key Agreeme nt Protocols	Side- Channel Attack Resistanc e: 88%, Computat ional Overhead : 20%	ents Efficient security protocols with resistance to specific attacks	y may limit scalabilit y Strong security for blockchai n- powered intelligen t edge, though some computati onal overhead is noted
[22]	Lightwei ght Privacy- Preservin g Medical Diagnosi s (LPME)	Privacy Preservati on: 90%, Latency Reductio n: 25%	Effective privacy preservati on with low computat ional overhead	of resource- constrain ed environm ents Offers robust security in real- time medical diagnosti cs with minimal	[25]	Federate d Learning for VEC in 6G	Privacy Protectio n: 80%, Training Time Reductio n: 20%	Balanced security with efficient resource managem ent in vehicular edge computin g	Enhances privacy and reduces training time, but challenge s remain in maintaini ng real- time performa nce
[23]	Blockcha in-based Stochasti c Different ial Game Theory	Attack Detection Accuracy: 92%, Security Enhance ment: 85%	High security with comprehe nsive threat detection in edge computin g environm	latency, suitable for edge- cloud systems Provides strong security through blockchai n and game theory, though computati onal complexit	[26]	Online Algorith ms for AI Service Chains (AISC)	Throughp ut Maximiza tion: 90%, Deploym ent Cost Reductio n: 15%	High efficienc y in deployin g secure AI service chains	Demonstr ates strong potential in securing AI service chains, though complexit y in deployme nt could affect scalabilit y

International Journal of Innovations in Engineering and Science, www.ijies.net

[07]			TIC:	D 1	1	0		· · · ·	j	CC
[27]	Reputati	Detection	Efficient	Reduces			ain for	Improve	secure	efficient
	on	Overhead	managem	detection			VEC)	ment:	data	blockchai
	Incentive	Reductio	ent of	overnead				75%,	storage	n-based
	Scheme	n: 60%,	detection	while				Storage	and	storage,
	(RIEID)	Tamperin	overhead	maintaini				Overhead	retrieval	though
		g Rate	with	ng				: 20%		scalabilit
		Managem	reputatio	security,						y in
		ent: 10%	n-based	though						resource-
			incentive	effectiven						constrain
			S	ess						ed
				depends						environm
				on						ents may
				accurate						pose
				reputatio						challenge
				n						s
				managem		[21]	D :		xx: 1	D
				ent		[31]	Privacy	Efficienc	High	Demonstr
[20]	a		XX: 1	D 11	-		Protectio	У	efficienc	ates
[28]	Secure	Time	High	Provides			n	Improve	y 1n	strong
		Complexi	security	secure			Scheme	ment:	privacy	privacy
	I ask	ty D 1	with	and			for	40%,	protectio	protectio
	Framewo	Reductio	reduced	efficient			Federate	Privacy	n with	n in
	rĸ	n: 15%,	computat	task			d .	Enhance	low	federated
		Latency:	ional	managem			Learning	ment:	computat	learning,
		10ms	complex1	ent,			(PPFLE	80%	ional	suitable
			ty in 1101	though			C)		requirem	for
			environm	further					ents	unstable
			ents	optimizat						edge
				10n of						computin
				latency is						g .
				needed						environm
[29]	Secure	Authentic	Efficient	Ensures	-					ents
[27]	Batch	ation	hatch	high		[32]	Robust	Communi	Highly	Offers
	Authenti	Overhead	authentic	security		[32]	Privacy-	cation	efficient	robust
	cation	· 10%	ation	in 5G-			Preservin	Efficienc	data	security
	for 5G-	Security	with	enabled			σ Data	v: 16.9%	aggregati	and
	enabled	Enhance	strong	ITS with				Computat	on with	efficiency
	ITS	ment:	security	minimal			ion for	ional Cost	strong	though
	115	85%	in	overhead			IIOT IOI	Reductio	nrivacy	real-
		0570	vehicular	though			1101	n: 27.8%	protectio	world
			networks	scalabilit				11. 27.070	n	applicatio
			networks	v in					11	n may
				y III Jarger						require
				networks						adaptatio
				may						n for
				roquiro						diverse
				additional						HoT
				resources						scenarios
				resources						scenarios
[30]	Acce-	Query	High	Provides	1	[33]	Efficient	Overhead	High	Ensures
	chain	Efficienc	efficienc	secure			Identity	Reductio	security	strong
	(Blockch	у	y in	and			Authenti	n: 20%,	with	anonymit

International Journal of Innovations in Engineering and Science, www.ijies.net

[24]	cation Protocol for MEC	Anonymit y Maintena nce: 85%	efficient identity authentic ation in mobile edge computin g	y and security, though some overhead is associate d with implemen tation		19	85%	healthcar e IoT	energy managem ent, though real- world scalabilit y may require further validation
	vivDN- based Certificat eless Signcryp tion Strategy	Enhance ment: 75%, Computat ion Reductio n: 30%	security with reduced computat ional requirem ents in vehicular networks	effective security with fewer computati onal demands, though suitability for highly dynamic networks may vary	[37]	OR-EDI Scheme for Mobile Edge Computi ng	Communi cation Overhead Reductio n: 50%, Time Consump tion Reductio n: 40%	High efficienc y in ensuring data integrity with reduced communi cation overhead	Offers strong security and efficiency , though effectiven ess may vary with different edge computin g architectu
[35]	Blockcha in-based Fog Computi ng Service	Transmis sion Capacity Enhance ment: Up to MB, Privacy Protectio n: High	High efficienc y in secure and private data transmiss ion	Demonstr ates strong potential in enhancin g transmiss ion capacity and privacy, though implemen tation complexit y may be a limitation	[38]	Certificat e-based Ring Signcryp tion for UAV Network s	Computat ion Cost Reductio n: 25%, Security Level: 80%	Efficient security with reduced computat ional costs in UAV networks High	res Provides strong security with minimal computati on, though adaptatio n to rapidly changing environm ents may be necessary
[36]	DRL- empower ed H-IoT System for COVID-	Energy Efficienc y: 35%, Security Enhance ment:	High efficienc y in balancing security and energy in	Provides a balanced approach to security and		Resource Collabor ation in Edge Federatio n	y Improve ment: 20%, Balanced Storage Allocatio	efficienc y in storage resource managem ent across	ates strong potential in collaborat ive storage,

		n: High	edge nodes	though scalabilit y across diverse networks may require further study
[40]	AI- enhanced Security in MEC	Security Efficienc y: 85%, Privacy Preservati on: 80%	High efficienc y in managing security and privacy through AI in MEC	Offers a promisin g approach to security and privacy managem ent, though complexit y in AI integratio n may pose challenge s

Table 4. Comparative Analysis of Existing Methods

The different methods are found to excel in quite a number of ways concerning security and scalability issues in edge computing environments. Some approaches provide a very high level of security but offer low computational overhead, while others balance security and system efficiency, particularly in resourceconstrained environments. While blockchain, AI, and federated learning techniques are promising in terms of improving security and scalability, every method comes with its problems in terms of real-world scalability, implementation complexity, and adaptation across diverse network conditions. From this comparative analysis, what can be noticed is that research and development into these methods are not yet holistic and optimized with regard to secure and scalable edge computing process.

IV. RESULT & DISCUSSION

Among various models and methods put forward to improve security and scalability for edge computing, the leveraging of the latest advanced technologies seems to be a common trend in blockchain, federated learning, and AI-enhanced algorithms. Such methods would principally mean solving dual problems of security and scalability intrinsic to the edge computing environment characterized by distribution and resource constraints. Among the models investigated, blockchain-based approaches, such as [23] and [30], have been in prevalent use, for some inherent characteristics in blockchain support tamper-proof data management and decentralized security. These models show great strengths in applications that require high levels of data integrity and security, such as in Industrial IoT and Vehicular Edge Computing. It means that blockchain, through its decentralized architecture and consensus mechanisms, is quite suitable for scenarios in which high security should be maintained across a widely dispersed network, even considering potential increases in computational overheads. This is something federated learning models are also highlighting, too, for edge computing. Federated learning models are particularly very good in scenarios that require security and efficiency. This is due to the fact that they are able to optimize resources while at the same time ensuring data privacy. However, some issues related to the model's scalability have been analyzed in highly dynamic and verv heterogeneous networks. Therefore, AI-empowered security models, like the ones described in [40], are increasingly adopted since they are able to handle the complex, and often unpredictable, security threats in real time. They are based on the ability of AI to adapt to the emerging threats, making them very effective in rapidly changing security conditions-like what happens in Mobile Edge Computing. AI integrated with conventional safety measures improves the system's capability in threat detection and its response time with low human intervention, hence improving security efficiency as a whole. Conversely, on equal ground, analysis also shows that AI integration can bring about an increase in computational complexity and large data processing power challenges all at once. These models and methods for enhancing security and scalability in edge computing clearly indicate a strong preference for blockchain, federated learning, and AI-empowered approaches. Each of these would bring extra benefits depending on the very requirements of the application: blockchain will be required if decentralized data management is necessary, federated learning for privacy-preserving computations, and AI for adaptive security measures. The great use that these models have found in users touting their efficiency in solving problems unique to edge computing is attested

International Journal of Innovations in Engineering and Science, www.ijies.net

to by the citations and analysis attached in the process. Further research would optimize these models for better scalability and ease of fit within an increasingly complex and dynamic edge environment sets. Future studies must be oriented toward hybrid models in which the salient features of both approaches can be integrated with new algorithms and architectures so that edge computing systems further improve in security and scalability levels.

REFERENCES

- Humayun, M., Alsirhani, A., Alserhani, F. et al. Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency. J Cloud Comp 13, 37 (2024). https://doi.org/10.1186/s13677-024-00602-2
- [2] Tong, Z., Liu, B., Mei, J. et al. Data Security Aware and Effective Task Offloading Strategy in Mobile Edge Computing. J Grid Computing 21, 41 (2023). <u>https://doi.org/10.1007/s10723-023-09673-y</u>
- [3] Boopathi, M., Gupta, S., Zabeeulla, A.N.M. et al. Optimization algorithms in security and privacypreserving data disturbance for collaborative edge computing social IoT deep learning architectures. Soft Comput (2023). <u>https://doi.org/10.1007/s00500-023-08396-2</u>
- [4] Wang, S., Liu, Z., Wang, H. et al. Ensuring security in edge computing through effective blockchain node detection. J Cloud Comp 12, 88 (2023). <u>https://doi.org/10.1186/s13677-023-00466-y</u>
- [5] Tiwari, R.S., Lakshmi, D., Das, T.K. et al. A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security. Telecommun Syst (2024). <u>https://doi.org/10.1007/s11235-024-01200-y</u>
- [6] M. Alioto, "Aggressive Design Reuse for Ubiquitous Zero-Trust Edge Security—From Physical Design to Machine-Learning-Based Hardware Patching," in IEEE Open Journal of the Solid-State Circuits Society, vol. 3, pp. 1-16, 2023, doi: 10.1109/OJSSCS.2022.3223274.
- [7] D. Yu, R. -H. Hsu, J. Lee and S. Lee, "EC-SVC: Secure CAN Bus In-Vehicle Communications With Fine-Grained Access Control Based on Edge Computing," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1388-1403, 2022, doi: 10.1109/TIFS.2022.3152405.
- [8] J. Qin and J. Liu, "Multi-Access Edge Offloading Based on Physical Layer Security in C-V2X System," in IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 6912-6923, July 2022, doi: 10.1109/TVT.2022.3164896.
- [9] Z. Song, H. Ma, R. Zhang, W. Xu and J. Li, "Everything Under Control: Secure Data Sharing Mechanism for Cloud-Edge Computing," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2234-2249, 2023, doi: 10.1109/TIFS.2023.3266164.
- [10] K. Shang, W. He and S. Zhang, "Review on Security Defense Technology Research in Edge Computing Environment," in Chinese Journal of Electronics, vol. 33, no. 1, pp. 1-18, January 2024, doi: 10.23919/cje.2022.00.170.
- [11] H. Zhong, L. Wang, J. Cui, J. Zhang and I. Bolodurina, "Secure Edge Computing-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," in IEEE Transactions on Information Forensics and Security, vol.

18, pp. 3774-3786, 2023, doi: 10.1109/TIFS.2023.3287731.

- [12] J. Mongay Batalla et al., "Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-Criteria Decision Making," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 5, pp. 3496-3512, May 2024, doi: 10.1109/TITS.2023.3325908.
- [13] X. Zhou, D. He, J. Ning, M. Luo and X. Huang, "AADEC: Anonymous and Auditable Distributed Access Control for Edge Computing Services," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 290-303, 2023, doi: 10.1109/TIFS.2022.3220030.
- [14] H. Xiao, J. Zhao, J. Feng, L. Liu, Q. Pei and W. Shi, "Joint Optimization of Security Strength and Resource Allocation for Computation Offloading in Vehicular Edge Computing," in IEEE Transactions on Wireless Communications, vol. 22, no. 12, pp. 8751-8765, Dec. 2023, doi: 10.1109/TWC.2023.3265458.
- [15] Z. Guo et al., "A Security Evaluation Model for Edge Information Systems Based on Index Screening," in IEEE Internet of Things Journal, vol. 11, no. 12, pp. 21585-21603, 15 June15, 2024, doi: 10.1109/JIOT.2024.3375077.
- [16] W. Almuseelem, "Energy-Efficient and Security-Aware Task Offloading for Multi-Tier Edge-Cloud Computing Systems," in IEEE Access, vol. 11, pp. 66428-66439, 2023, doi: 10.1109/ACCESS.2023.3290139.
- [17] H. Sun, H. Yu, G. Fan, L. Chen and Z. Liu, "Security-Aware and Time-Guaranteed Service Placement in Edge Clouds," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 711-725, March 2023, doi: 10.1109/TNSM.2022.3213761.
- [18] Q. Xie, C. Zhang and X. Jia, "Security-Aware and Efficient Data Deduplication for Edge-Assisted Cloud Storage Systems," in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 2191-2202, 1 May-June 2023, doi: 10.1109/TSC.2022.3195318.
- [19] H. Xiao, Q. Pei, X. Song and W. Shi, "Authentication Security Level and Resource Optimization of Computation Offloading in Edge Computing Systems," in IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13010-13023, 1 Aug.1, 2022, doi: 10.1109/JIOT.2021.3139222.
- [20] H. Zhang et al., "Secure Edge-Aided Computations for Social Internet-of-Things Systems," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 76-87, Feb. 2022, doi: 10.1109/TCSS.2020.3030904.
- [21] J. Cui, F. Wang, Q. Zhang, C. Gu and H. Zhong, "Efficient Batch Authentication Scheme Based on Edge Computing in IIoT," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 357-368, March 2023, doi: 10.1109/TNSM.2022.3206378.
- [22] Z. Ma et al., "Lightweight Privacy-Preserving Medical Diagnosis in Edge Computing," in IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1606-1618, 1 May-June 2022, doi: 10.1109/TSC.2020.3004627.
- [23] Wang, H., An, J. Dynamic stochastic game-based security of edge computing based on blockchain. J Supercomput 79, 15894–15926 (2023). https://doi.org/10.1007/s11227-023-05289-x
- [24] J. Zhang and F. Zhang, "Identity-Based Key Agreement for Blockchain-Powered Intelligent Edge," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6688-6702, 1 May1, 2022, doi: 10.1109/JIOT.2021.3111552.
- [25] M. K. Hasan et al., "Federated Learning for Computational Offloading and Resource Management of Vehicular Edge Computing in 6G-V2X Network," in IEEE

International Journal of Innovations in Engineering and Science, www.ijies.net

Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3827-3847, Feb. 2024, doi: 10.1109/TCE.2024.3357530.

- [26] Y. Qiu, J. Liang, V. C. M. Leung and M. Chen, "Online Security-Aware and Reliability-Guaranteed AI Service Chains Provisioning in Edge Intelligence Cloud," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5933-5948, May 2024, doi: 10.1109/TMC.2023.3314580.
- [27] Z. Zhao, S. Zhao, F. Lv, S. Si, H. Zhu and L. Sun, "RIETD: A Reputation Incentive Scheme Facilitates Personalized Edge Tampering Detection," in IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14771-14788, 15 April15, 2024, doi: 10.1109/JIOT.2023.3344709.
- [28] A. S. M. S. Hosen, P. K. Sharma, I. -H. Ra and G. H. Cho, "SPTM-EC: A Security and Privacy-Preserving Task Management in Edge Computing for IIoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6330-6339, Sept. 2022, doi: 10.1109/TII.2021.3123260.
- [29] M. Kim et al., "A Secure Batch Authentication Scheme for Multiaccess Edge Computing in 5G-Enabled Intelligent Transportation System," in IEEE Access, vol. 10, pp. 96224-96238, 2022, doi: 10.1109/ACCESS.2022.3205001.
- [30] Y. Lu et al., "Accelerating at the Edge: A Storage-Elastic Blockchain for Latency-Sensitive Vehicular Edge Computing," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 11862-11876, Aug. 2022, doi: 10.1109/TITS.2021.3108052.
- [31] R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar and M. Karuppiah, "Privacy-Preserving Federated Learning for Internet of Medical Things Under Edge Computing," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 854-865, Feb. 2023, doi: 10.1109/JBH1.2022.3157725.
- [32] S. Shang, X. Li, K. Gu, L. Li, X. Zhang and V. Pandi, "A Robust Privacy-Preserving Data Aggregation Scheme for Edge-Supported IIoT," in IEEE Transactions on Industrial Informatics, vol. 20, no. 3, pp. 4305-4316, March 2024, doi: 10.1109/TII.2023.3315375.
- [33] Y. Xu et al., "An Efficient Identity Authentication Scheme With Provable Security and Anonymity for Mobile Edge Computing," in IEEE Systems Journal, vol. 17, no. 1, pp. 1012-1023, March 2023, doi: 10.1109/JSYST.2022.3185258.
- [34] C. N. A. Cobblah, Q. Xia, J. Gao, H. Xia, G. A. Kusi and I. A. Obiri, "A Secure and Lightweight NDN-Based Vehicular Network Using Edge Computing and Certificateless Signcryption," in IEEE Internet of Things Journal, vol. 11, no. 16, pp. 27043-27057, 15 Aug.15, 2024, doi: 10.1109/JIOT.2024.3399031.
- [35] Y. Cao, J. Li, K. Chao, J. Xiao and G. Lei, "Blockchain Meets Generative Behavior Steganography: A Novel Covert Communication Framework for Secure IoT Edge Computing," in Chinese Journal of Electronics, vol. 33, no. 4, pp. 886-898, July 2024, doi: 10.23919/cje.2023.00.382.
- [36] L. Liu and Z. Li, "Permissioned Blockchain and Deep Reinforcement Learning Enabled Security and Energy Efficient Healthcare Internet of Things," in IEEE Access, vol. 10, pp. 53640-53651, 2022, doi: 10.1109/ACCESS.2022.3176444.
- [37] J. Li, Q. Zhao, H. Cheng, S. Teng, N. Wu and Y. Liang, "OR-EDI: A Per-Edge One-Round Data Integrity Verification Scheme for Mobile Edge Computing," in IEEE Transactions on Network Science and Engineering, vol. 11, no. 2, pp. 2074-2086, March-April 2024, doi: 10.1109/TNSE.2023.3337075.

- [38] M. Asghar Khan et al., "A Certificate-Based Ring Signcryption Scheme for Securing UAV-Enabled Private Edge Computing Systems," in IEEE Access, vol. 12, pp. 83466-83479, 2024, doi: 10.1109/ACCESS.2024.3409359.
- [39] W. Li, Q. Li, L. Chen, F. Wu and J. Ren, "A Storage Resource Collaboration Model Among Edge Nodes in Edge Federation Service," in IEEE Transactions on Vehicular Technology, vol. 71, no. 9, pp. 9212-9224, Sept. 2022, doi: 10.1109/TVT.2022.3179363.
- [40] C. Wang, Z. Yuan, P. Zhou, Z. Xu, R. Li and D. O. Wu, "The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22008-22032, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3304318.