European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

Delving into Security Horizons: A Study of EC-IoT Landscape

Dr. Aarti Rani[1]
Assistant Professor
Lucknow Public College of Professional Studies, Lucknow
Email: *aarti.singh18oct@gmail.com*
ORCID: 0000-0002-8081-6821

Ms. Rachna Sinha[2]
Head of Department
Karmadevi Smriti Mahavidyalaya, Basti
Email: *hod.bca@karmadevigroup.com*

Ms. Archita Singh[3]
Student
Indian Institute of Information Technology, Ranchi, Jharkhand
Email: *singharchita723@gmail.com*

Ms. Purnima Pandey[4]
Research Scholar
Babu Banarsi Das University, Lucknow
Email: *ppoornima621@bbdu.ac.in*

Abstract

The past several eons witnessed a leviathan proliferation in the sheer volume of data obtained from actuators, various Internet of Things (IoT) devices, and sensors. Contemporarily, cloud-based computing resources situated in remote data centers are cardinally used to manage IoT data. Network capacity and communication delay therefore turn into decisive constraints. Ergo, edge computing (EC) is emerging as a technologically advance approach that establishes storage and processing of data in close proximity to the end users, engendering the concept of EC-assisted IoT. Nevertheless, because of the prudent nature of the gathered data and the ingrained debility of edge nodes, there are still a number of security issues with EC-IoT. A thorough analysis of the security and privacy concerns that still exist in the EC-IoT ecosystem is conducted in this research. Precisely, the article begins with a concise overview of EC and IoT technologies and their respective use cases. The paper further offers an overview of the forces propelling EC-IoT and describes an edge-centric design that assists in surmounting the shortcomings of conventional IoT systems. Subsequently, the paper addresses beaucoup privacy and security issues that still exist in the redesigned architecture and offers a few defense mechanism against those risks. Lastly, suggestions for unsolved research issues and untapped research opportunities have been posited.

Keywords- Edge Computing (EC), Internet of Things (IoT), security, EC-IoT architecture, security architectures.

INTRODUCTION

Artificial Intelligence (AI) services and products have been accentuating in the recent past by dint of technological anabasis in deep learning. The internet connects billions of IoT (Internet of Things) and mobile devices, effectuating in a shedload of bytes of data at the edge of the network, primarily as a result of upswing in the Artificial IoT (AIoT) and mobile computing. With beaucoup data being generated by a multitude of smart and sensory devices, the cynosure of services and computations are now being driven to the network edge from the cloud as a consequence of amplifying computational capacity. As of now, there are more than 50 billion net-connected IoT devices, and it is anticipated that around 80 billion sensors and IoT devices would be online by 2025, in accordance with IDC predictions [1]. Such gadgets include handheld devices, sensors and wearables etc., stand out through their exiguous energy as well as computational resources. Contemporarily, devices with scanty resources may fathom these constraints by offloading computation and storage to the cloud [2]. The spontaneous and protractible characteristic of the cloud makes it an absolute solution for computational offloading. Regardless, resources for cloud computing are bivouacked in prodigious data hubs that are stationed far-off from the majority of clientele resulting in significant connection delay between the cloud and the end user. Withal, the network links of the cloud, are enduring an extreme amount of stress owing to the burgeoning magnitude of data being transferred. In order to munificently emancipate the prowess of big data, it is imperative to advance the AI bounds to the network's edge, a task made possible by the advancement of AI and IoT. As a way to reinforce computation-enrapt AI operations on edge devices, Edge Computing (EC) is a viable notion to actualise this trend [3].

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

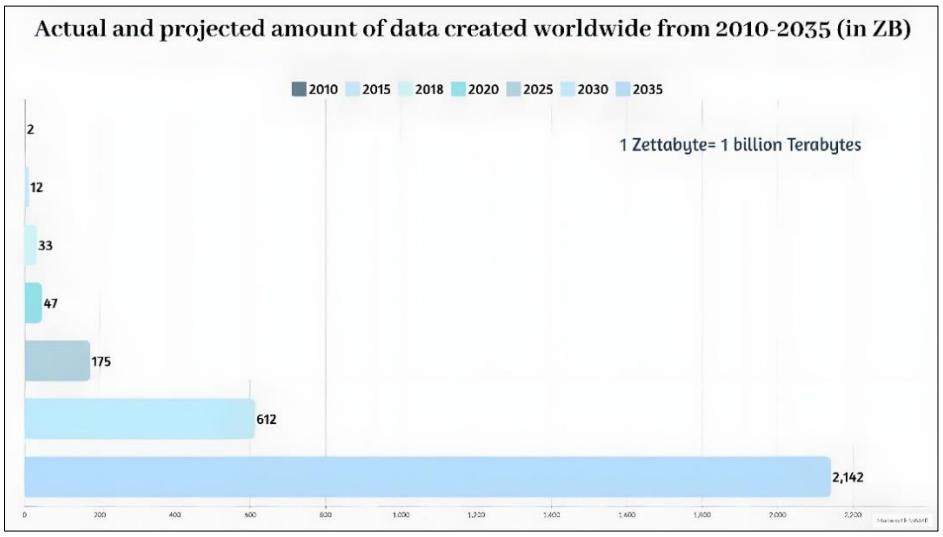

FIG.1 Estimated Global Data Generation

Embodying a distributed computing cogitation, EC is characterized by ameliorated response rate and bandwidth by schlepping data and computation hither to the customary IoT deployment locations. Thus, EC which is a dispersed computing paradigm relocates applications nearer to edge servers, local end devices, and IoT devices [4]. EC has matured into an augmented version of cloud computing that brings cloud facilities closer to end users [5-7]. Edge devices are endpoints, such as smartphones, IoT gadgets, embedded devices, which transmits service request to edge servers. Besides, edge servers are the resources that offer services to consumers; they might be routers, mini data centres generally found in mobile network base stations, on automobiles etc., or IoT gateways. A broad spectrum of technologies falls under the umbrella term edge computing, inclusive of fog and mist computing, cloudlet, and Mobile Edge Computing (MEC) [8]. The primary merits of EC can be summed up into 3 traits: -

i- **Energy conservation for end devices**: By delegating computational duties to edge servers, end devices would consume a significantly lesser amount of energy. End devices would thus have longer battery lives.
ii- **Scalability:** If in case, edge servers or devices burn through the resources, cloud computing still remains accessible. In such cases, cloud servers come into play of assisting the tasks. Furthermore, end devices with stagnant resources might confabulate with one other to fulfil a task collectively.
iii- **Ultra-low latency:** Computation often occurs in a close proximity to the source data, saving a significant amount of time during data transfer.

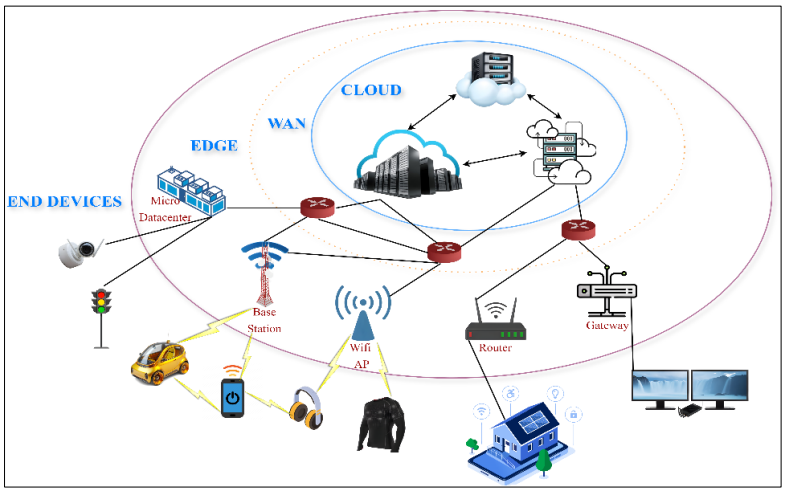

FIG.2 A generic concept of Edge Computing

A multitude of IoT-driven resources are ubiquitously facilitated by the cloud. An IEEE World Forum colloquy from October'23 asserts that comprehensive data processing and assessment of voluminous data, highly efficient computation, and depository infrastructure bestow resilience, nous, and automation features to the IoT [9]. Applications comprised of scraping, organizing, and analysing data at the edge of the network, are supported by cloud computing as well. Albeit, the cloud's potential to assist devices, consumers, and infrastructure at the edge is insubstantial. Most of this data will be transmitted to advanced centralized servers housed in the cloud under the conventional cloud computing paradigm, in order to be further examined, computed, or/and stored. After processing, the data must be retroceded to the end devices. The following factors lead to an inadequate quality of service (QoS) and ancillary load on the primary network when employing such a mechanism:

- The underconsumption of bandwidth and resources effectuates superfluous outlay for data transmission
- The accretion in data size significantly de-escalates the network performance
- The rapid proliferation of IoT devices will make network connectivity and traffic management extremely challenging.
- Time-dependent IoT services and applications, such as smart transportation, smart energy grid, and smart city, will be exorbitantly overdue.

Exacerbating IoT devices and paring down forenamed fetters, predominantly caused by transporting plethora of data to storage facilities from the IoT devices for processing and evaluation has become significant since the need for convoluted computation increases at these edge locations, as reported by TechRepublic [10]. Steady connection and imperious processing capacity are necessary to perambulate AI applications nigher to the edge. Presume the following hypothetical situation: an industrial facility yearns for integrating AI algorithms into their machinery to enable millisecond-accurate real-time decision-making. Transferring their data to a distant server for analysis and transferring back to the device is not feasible. These operations may now be carried out directly on the device, with the aid of edge computing. Grand View Research envisages that the edge computing industry would proliferate at a compound annual growth rate (CAGR) of 38.9%, or over 155.9 billion dollars, by 2030. The predicted driver of this market escalation is the amalgamation of AI into edge environment [11]. A broad spectrum of distributed, intelligent, time-sensitive, and credible application features is possible by coalescing EC with AI. This blend further aggrandizes the leeway for real-time, pronto data processing and decision-making. Last but not least, it has the forte to collect, maintain, and process massive amounts of IoT data. Aimed at optimizing resource utilization, offloading and scheduling data processing operations versatilely, potently, instantaneously and upon request at the nodes' edge, additionally satisfying functional specifications regarding temporal urgency and energy frugality during digital computations, AI-based Machine Learning (ML) is perceived as the prime pick considering the inherent characteristic of resource-deprived and mutations in EC [12,13].

Nevertheless, the EC-IoT system poses significant security perils resulting from its idiosyncratic characteristics and susceptibilities [14]. As a case in point, intruders may forge data obtained from sensing units in order to influence decision-making and manipulate upshots in IoT systems. In pursuit of carrying out malevolent actions like Distributed Denial of Service (DDoS), that seeks to hinder the appropriate employment of a facility, adversaries in the vicinage might interfere or infiltrate the edge nodes. Additionally, IoT services that handle user privacy, including smart homes and e-healthcare, gather and handle that data, which they expose to the possibility of being compromised by malevolent actors. Robust security defences in defiance of those risks needs to be formulated hastily, due to the marked uptick in attacks zeroing in on EC infrastructures recently [15]. On top of that, the crafting of security systems in EC-assisted IoT is exacerbated by the energy demarcations of IoT devices. The financial viability of IoT applications may be significantly influenced by the energy savings obtained via optimizing security techniques, in light of the profusion of equipment and servers involved in IoT. Currently available research portrays these two domains as highly segregated, and the methods created for one seldom ever deal with the problems in the other. A greater push is required to address security-related concerns due to the energy-security trade-off.

Profuse amount of data pertaining to sensitive and essential applications in a variety of industries, ranging from smart buildings to health surveillance, are administered and managed by EC-assisted IoT systems. As a result, it has become vulnerable for attacks from the agencies working under government, black hats, and cyber felons. Hackers may target IoT sensors and devices seeking to pilfer sensitive information, including bank account details, health and location information. Also, adversaries have the ability to snoop on people or even start dissent campaigns against an association. It has been chronicled that over 25% of botnet assaults came from IoT devices, such as televisions, infant monitoring systems, and household gadgets [16].

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

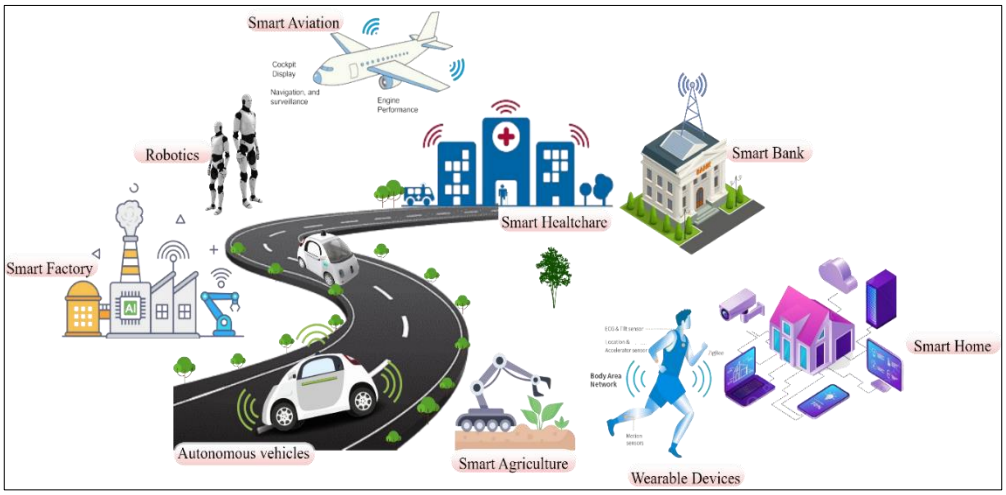

FIG.3 Applications of IoT

Paper Composition

1. Literature Review
- Conduct a Systematic Literature Review (SLR) focusing on essential elements of edge intelligence, edge-assisted IoT, and the development situation in this field.

2. Technology Overview
- Provide a detailed description of the major technologies involved, namely edge computing and IoT.
- Introduce the EC-IoT architecture.

3. Security and Privacy Challenges in EC-IoT
- Dive deep into the security and privacy challenges faced in the EC-IoT environment.
- Discuss potential threats and vulnerabilities.

4. Solutions and Countermeasures
- Present possible solutions and countermeasures at different layers for various security issues identified in previous section.
- Discuss techniques for enhancing security and privacy in EC-IoT systems

5. Open Challenges and Future Research Directions
- Highlight the open challenges in the EC-IoT paradigm.
- Provide insights into promising future research directions in the context of EC-IoT.

6. Conclusion
- Summarize the key findings of the research.
- Reiterate the contributions of the paper.
- Conclude with suggestions for further research in the field.

Systematic Literature Review

Y. Ai et al. [17] in his study demonstrated three categories of EC technologies— cloudlets, MEC, and fog computing (FC). The inquisition indoctrinates and contrasts architectures, precepts, efforts, implementations and homogenization. The qualities of Radio Access Network (RAN) -based FC are also addressed along with how FC differs from MEC in terms of RAN usage. Following the introduction of mobile edge networks encompassing their design, and benefits, S. Wang et al. [18] provide a thorough analysis of the communication, processing, and caching strategies used at the edge network. Future avenues and unaddressed research conundrums are also mentioned, along with the use cases and applications of edge networks.

Authors of [19] uses a three-layer non-intrusive framework formulated on a multilayer EC for IoMT (Internet of Multimedia Things). As demonstrated in the research, the suggested framework outperforms the current models apropos to protect the subjacent network, preserving data integrity, and managing nodes. Utilizing a revolutionary dynamic edge access system, the authors in [20] deals effectively with the existing concerns in eclectic device node reconfigurations, consolidation services for access programs, and protocol library management. In juxtaposition to conventional systems, it exhibits that the recommended methodology has curtailed duplication and subdues hardware expenditures.

The manuscript titled as "Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms"[21], illustrates on IoT architecture for automated residences. With the assistance of stereo matching technique, the researchers assess data transfer in smart living ecosystems considering both software and hardware vantage points. The beefed-up architecture of smart houses improves the user integrity and confidentiality plus it is fairly precise and has value for money. Along with amplifying the safety aspect, it also optimizes the viability of automated home systems.

An edge-based energy optimization system was put forward by Cicirelli et al. [22] to trim energy overhead of everyday domestic machinery. Utilizing reinforcement learning, they adduced a load appliance scheduling method. It considers time-varying profiles of energy output, cost, and appliance energy consumption. Through the utilization of a functional instance that yields reliable ramifications, the methodology is validated. Using a fog-based IoT architecture, Tom et al. [23] employed a fog-based IoT framework to craft an intelligent energy management system and devise a strategy to minimise every residence's demand in the vicinity amidst the busiest times. Post assessment of regular consumption patterns and running a discriminant analysis to ascertain the appliances that were significantly important, they were able to anticipate consumer utilization using Autoregressive Integrated moving Average a.k.a ARIMA.

P. Porambage et al. [24] in his study on multi-access EC provides a comprehensive analysis of this model pertaining to IoT. Additionally, the author examined and unveiled the synergies that result from integrating multi-access EC and IoT. Along with that, the functional aspects of this paradigm are probed to shed insight into a myriad of interface technologies in multi-access EC empowered IoT. Examining the armature of mobile EC, Ni et al. [25] delved into the merits and avenues of capitalizing on mobile EC to augment data analysis and operational streamlining for a spectrum of IoT solutions. The research "Future edge cloud and edge computing for internet of things applications" probes the core objectives, impetuses, crucial technologies along with the prominent utilizations of EC-assisted IoT [26].

The authors of [27], furnish a synopsis on the scholarly publications on EC- facilitated IoT from the year 2008 to 2018, comprising of services, ancillary technologies, and few uncharted research territories. Certain technologies, concerns, contingencies, and advantages inherent in EC-assisted IoT are addressed by Caprolu et al. [28]. Authors of [5], outline copious setbacks and future explorations while featuring a multitude of dossiers for EC-assisted IoT, including smart cities, homes and cloud offloading.

Medley of Edge Computing and Internet of Things

This section furnishes a succinct explanation of the core technologies, the edge-centric IoT architecture including a precise delineation of each layer, the advantages of EC-IoT and lastly its characteristics.

1. Technology Overview

Edge Computing (EC): There has always been periods encompassing both centralised and decentralised computing across the epochs of computer history. Mainframes blazed the trails for centralized computing. Soon enough, distributed computing transitioned to portable computers and local networks, ultimately cloud computing reinstated computing to a centralized form. Analysis, storage and data processing are all concentrated on servers in cloud computing. A revolutionary distributed IT framework known as "edge computing" involves peregrinating services, computer applications, and data storage from centralized nodes to the close vicinity of end user. Trimmed time lag and response time are two boons owing to EC that benefits real-time applications. Cloud and edge coalesce smoothly; the latter handles system administration while EC guarantees seamless service. Consequently, integrating EC into the network ameliorates it on multiple fronts:

1. Competence: By prorating control functions, processing and storage according to the availability of the resources that are accessible anywhere between the cloud and the end user, an edge device makes the most of the resources at its disposal [5]. As a result, pooled EC resources may be used effectively by the IoT devices.
2. Discernment: The edge devices are cognizant of customer's preferences [29]. In a digital healthcare platform, for instance, patients' health-risk grade determines how compute resources are allocated and how their corporeal wellness is examined with the help of IoT devices, particularly in acute medical emergencies [30].
3. Latency: EC facilitates data crunching and evaluation nearby to end user, allowing IoT to bolster rapid decisions on time-sensitive applications [31].
4. Dexterity: As per the fact that data handling and archival are effectuated proximate to the end-user, tinkering with edge devices and customers can be performed expeditiously and for a modest price [32].

Internet of Things (IoT): A system of linked, heterogeneous objects, much like vehicles and domestic equipment, with network-driven abilities encompassing communication and data transmission. In order to enrich social activities, industry

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

and level of affluence, these interconnected devices fill the breach between the virtual and the physical realm [33]. Let's examine the current IoT paradigm in order to have a better understanding of how such devices operate intelligently. The protocols, architecture and applications of the IoT have been outlined by Sarangi and Sethi in their research [34]. The typical IoT architecture is demonstrated in below.

FIG.4 Conventional IoT Architecture

Broadly speaking, this architecture consists of three main levels, although as research into enhancing the functionality of IoT devices progresses, these layers are maturing in intricacy. IoT gateways, cloud servers and IoT devices constitute these three tiers. In the contemporary setting, an assortment of sensors is interlinked with IoT devices that gather unprocessed data. Post-transformation of data into significant data stream at the gateway, it is then sent to the cloud server where it is used for processing, analysis and archiving. Cloud servers evaluate and scrutinize data, then transmit the results back to the appropriate IoT device allowing it implement requisite measures. The contemporary IoT paradigm has an influence on latency and bandwidth in the network. The data produced by these sensors is transferred to a cloud server for further manipulation and analysis, necessitating additional bandwidth throughout the process. Furthermore, there is additional latency since it takes longer to deliver raw data to a cloud server a receive a response. For certain IoT uses that require prompt decision-making to complete tasks, latency may occasionally be unacceptable.

2. EC-IoT architecture

EC is envisaged to perform the role of IoT's strategic acumen. Customers may now access cloud computing's features and services more conveniently [35]. The characteristic of EC affirms its status of central impetus for several technologies, including 5G, v2v communications (vehicle-to-vehicle), Augmented Reality (AR), and IoT [36]. The ability to establish an unmediated association between cloud computing infrastructure and end users (IoT devices) is attained by EC, and this helps to account for certain unique peculiarities like pliability, spatial cognition, high bandwidth [37], expedited processing, low latency, and prompt application responsiveness [38].Preponderantly, multi-faceted distributed framework with edge assistance in IoT solutions attempt to even out the task burden among different layers. However, a conventional trilaminar edge-centric IoT framework is depicted in Fig.5

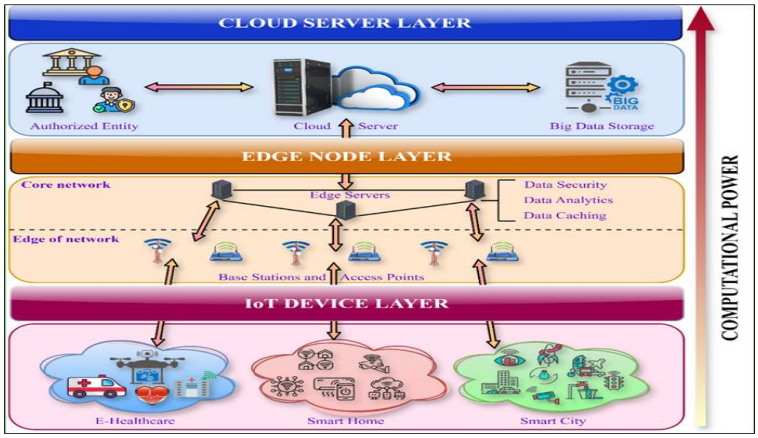

FIG.5 Edge-Assisted IoT Framework

2.1. Cloud server layer- The consolidated computing unit entailing data centres and cloud servers with formidable data processing prowess and abundant data storage, is harboured in this layer. Herein lies the usage of several machine learning algorithms to evaluate data and make decisions. This layer handles the most advanced credentialing, integration and administration of various tasks that are delegated to it from edges. In order to handle the data, it synergizes with edge nodes to evaluate it, make decisions, and provide feedback control to IoT gadgets.

2.2. Edge node layer- An indispensable component of IoT, the edge node layer connects the vast majority of IoT devices to the consolidated computing units. An eclectic network—which includes Wide Local Area Network (WLANs), Wide Area Networks (WANs), telecom network, Device-to-Device (D2D) communications etc.— connect edge nodes. EC-assisted IoT facilitates smooth transitions between assorted types of devices and networks. In pursuit of analysing data and relaying the control signal back to the controllers, edge nodes gather the data produced by IoT devices. In certain circumstances, where a task's complexity surpasses the current levels of edge nodes' computing capabilities, it is offloaded to nodes of higher level until it reaches the cloud servers.

2.3. IoT device layer- The Internet of Things device layer acts as the connection between the real and virtual worlds in edge-assisted IoT architecture. A variety of smart meters, wearables, smartphones, security surveillance camera, industrial sensors etc., are among the devices installed in this layer. This equipment, which measure and send data from tangible world objects to edge nodes, typically have limited battery life, computational power, communication capabilities, and storage. Essentially, IoT devices—like servo actuators, navigators, and smartphones etc., can also function as controllers. They accomplish this by using control objects and the centralized computing units' ideal selection to execute manoeuvres.

3. Challenges in EC-IoT environment Security and privacy threats

Due to the fact that data doesn't flow through a network, EC plays a beneficial role in cybersecurity. Conversely, a network becomes vulnerable in an agile environment near its edge. Exacerbated complications to the security situations arise from the intrinsic properties of edge, like flexible compute offloading and location awareness. In addition, energy limits necessitate that huge IoT devices and edge nodes operate Minimal energy utilization while preserving an adequate degree of security. A gallimaufry of security threats might arise from the intertwining of various devices in the IoT setup. Tremendous IoT device data is obtained by the edge layer, which uses it to retrocede control flows and supply local services. The gathered data may also be sent to a cloud server for additional analysis, task integration and perennial storage. In crowdsensing, for instance, sensing tasks are delegated to a crowd, and scads of IoT devices connected by edge networks assist task publishers in reporting real-time local area data. In order to gauge, assess, or appraise the crowd's congenial interest, the produced data and processing outcomes are combined in edge nodes. The majority of fundamental computing tasks, including data hoarding, task offloading, data processing, attestation, and ratification are handled by edge nodes in EC-assisted IoT environment. EC-IoT applications are thus vulnerable to major security risks from outré or smirched edge nodes, which can result in data alteration, malware implantation, service cessation, and privacy leaks.

Numerous studies have examined these kinds of risks. J. Ni et al. examined data processing's efficiency, security, and privacy issues in mobile EC [25]. The study also covers the propositions for increasing computational efficiency and safeguard data security while utilizing EC to support these goals. Secure computational offloading along with safe data mirroring and compilation are among the solutions they provide in their study. Diverse security and privacy procedures, standards, and strategies must be implemented in order to create an IoT ecosystem that is both safe and confidential with assistance from the EC. The significant security and privacy threats, their origins at various layers of EC-IoT network system, and varieties are covered in this section.

Classification of threats & attacks

Malicious Hardware & Software injections: With the aim of inoculating corrupt data into the EC servers, adversaries may install illegal hardware or software modules at the interface or EC node levels. Consequently, attackers will be able to beguile service providers to conduct hacking operations in their stead, including circumventing authentication, data siphoning, revealing database consistency, and fabricating data [39-41].

There are diverse classifications of hardware injection attacks, such as:

- Hardware Trojan- It refers to the illicit infiltration to the Integrated Circuits (ICs). This allows attackers to dominate the circuit and give them the permission to access the data or the software responsible for the functioning of ICs.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

- Node Cloning- It is a process when attackers introduce when attackers introduce an unauthorized additional EC node into the network by assigning it an ID number that is a simulacrum of an already-existing approved node. In this way, data packets can be misrouted to the malicious duplicate or be corrupted, stolen by attackers. Furthermore, by setting, node-revocation protocols in situ, node ectypes can even abrogate authentic EC nodes [40].
- Rogue or sabotaged EC nodes- Such type of nodes is designed to get unapproved access and command over the network, subsequently introducing deceptive data packets or obstructing the transmission of authentic and accurate data packets [39,40].
- Camouflage- In this technique, an attacker inserts a phony EC node into the network, imitating a legitimate one and using it to create, distribute, procure, hoard, manage, reroute the data packets [40].

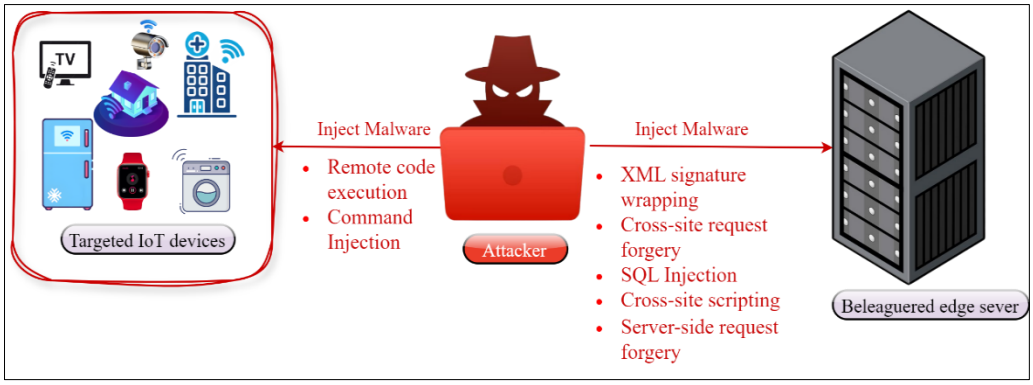

FIG.6 System model of malware injection attack

Forgery attacks*:* These attacks occur when an attacker imbue unfamiliar, bogus data packets into the receiver, interfering with it and potentially damaging or failing the system. The techniques used to implant these data packets into communication channels include:

1) introducing malicious packets that appear legal;

2) replicating packets that have already been transmitted between two EC nodes or devices; and

3) collecting and altering data packets [40][41][42].

Jamming attacks*:* These attacks occur when hackers purposefully overload the network with bogus messages seeking to drain out all available storage, computers and/or communication resources. This will prevent legitimate users from using the EC-IoT infrastructure [41].

Eavesdropping or Sniffing*:* It is an act where attackers surreptitiously overhear closed-door chats across communication lines, obtaining credentials and other personal information. The specifications, passwords, and identifiers of the communal network are examples of information that may be obtained by these adversaries through intercepting packets, which can provide them with vital network knowledge [39][40][42].

Integrity attacks against ML: The ML techniques employed in EC-IoT are also susceptible to chiefly two kinds of security vulnerabilities:

- Exploratory attacks, which exploit susceptibilities without altering the training procedure, and
- Causative attack, that modify the training mechanism of ML models by manoeuvring and introducing false training datasets [40].

Distributed Denial of Service (DDOS) attack: The eminent forms of DDoS attacks on EC nodes are power-depleting, sleep deficit, and service disruption attacks. In the event of the hindmost attack, EC nodes cease to function normally as they have been compromised by unauthorized breach. Attackers surfeit EC nodes with an inadvertent accumulation of legitimate solicitations when they are sleep deprived. Discerning such an intrusion is considerably more arduous. The process of battery draining conduces to a node shutdown or outage because the battery power of EC nodes, sensors, or other devices is consumed. The most frequent DDoS assault, however, occurs at the communication level when signals are jammed. This can be done in two ways: either continuously during all communications or intermittently, when EC nodes transmit and receive packets on a regular basis [16][24][25][40][42][44][47] An extensive system model for DDoS attack is shown in below figure .

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

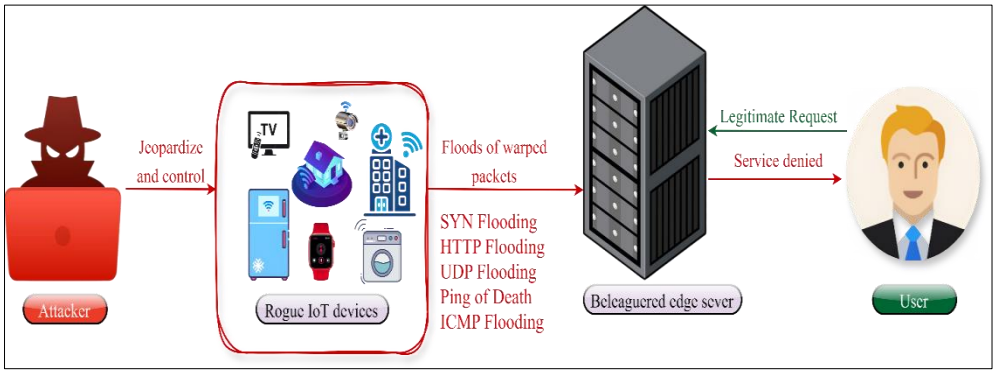

Fig.7 System Model for DDoS attack

Nonessential logging attacks: These kinds of attacks have the potential to harm Internet of Things systems that rely on EC support assuming log files are not protected. Designers of infrastructure and systems must thus keep tabs on events like application faults and accomplished/unaccomplished authorization/authentication processes [40].

Physical attack or tampering: It takes place when attackers obtain hands-on access to EC nodes or devices. This kind of situation allows for the extraction of confidential and important cryptographic data, tampering with the circuit, and modification or alteration of the operating systems and software [40-44].

Non-network side channel attack: Fundamental intelligence might become apparent by EC nodes even if they do not transmit any kind of data. For example, the identification of recognized electromagnetic (EM) or acoustic signals/ protocols from healthcare equipment may result in significant privacy concerns as decisive patient and device data may be disclosed [40][42].

Routing information attacks: Data packets are dropped or redirected at the communication stage by hackers seeking to modify routing details. There are four types of nefarious EC nodes that could be present [40][42][44]:

- Worm Holes: where cybercriminals capture packets at a specific network location before moving them to another,
- Gray Holes: which consume only specific packets,
- Hello Flood: where a potent malicious EC node telecasts “HELLO PACKETS” to the nodes pretending to be their neighbourhood denizens,
- Black Holes: that consume all network packets.

Unauthorized control access: It occurs when nearby EC nodes exchange data with other nodes or gain access to it. On the other hand, all nearby nodes might be taken over by attackers in case they manage to infiltrate one of the unprotected EC nodes [40][42].

Privacy breach: It may be necessary for EC nodes' functionality to retrieve private data from user devices' produced data. Certain information, in particular private engagements, predilection, and medical condition, can possibly be classified; whereas other data like the pollution severity index, open data, and corroboree, may not be. However, all data must be the property of data owners. Lamentably, they are susceptible to hackers during data transfers or sharing as they may be exchanged with strangers or network organizations unlawfully. The perpetrators can espy and identify a device’s spatial orientation or similar confidential data from the physical position of these EC nodes by exploiting their geographical awareness, which is present in EC nodes like base stations and Wifi hotspots. Furthermore, positioning algorithms may be used to accurately determine the actual location if user devices connect to several EC nodes concurrently for the purpose of accessing specific services [25][41][44].

Replay or freshness attacks: In this type of attack attackers intercept and log data flow for a predetermined amount of time, after which they exploit the past data to substitute it for the latest information that is available. In addition to other negative consequences, doing so will result in EC nodes using more energy and bandwidth [42][43].

Security threats from/on IoT devices: Ransomware, mobile botnets, and IoT malware are some of the cyberattacks that can target EC gadgets. There were reports of around 1.5million attacks in 2017 that started with mobile malware [25]. These dangers raise security issues for edge users and programs, potentially resulting in data loss, damage, or application failure [25][41].

Other Attacks: The IoT paradigm with EC assistance consists of a blend of diverse assets and devices constructed by different suppliers. There are still several security and privacy risks that go unnoticed as there is no widely accepted structure or set of acceptable procedures for implementing this paradigm.

4. Countermeasures and Solutions

The fundamental techniques and resolutions designed to thwart the privacy and security risks and menace highlighted in the preceding section are described in this portion.

a. Classification of solutions based on attack type

This section provides the corresponding countermeasures for each of the aforementioned attack.

S.No	Attack_Name	Solution/s	Description
1.	**Malicious Hardware & Software injections**	i.Circuit modification or replacing i.Side-channel signal analysis i.Trojan activation methods	i.Resetting the circuit is one of the best way to thwart side-channel, trojan, and physical attacks [40]. i.Using timing, power, and spatial temperature testing analysis, this strategy can identify hardware Trojans. Alternatively, it can identify nefarious firmware or software deployed on IoT-EC nodes or tools by identifying anomalous characteristics such as a notable heat escalation, increased latency, or upsurge in energy usage [40]. i.In order to achieve expedite Trojan detection, Trojan activation tactics strive to partially or completely activate the Trojan circuitry. Exaggerating and identifying differences between the outputs, side-channel leaks, or performance of a circuit with no Trojan and one with one installed is the shared objective of these approaches [40].
2.	**Forgery attacks**	i.Cryptographic Schemes i.Intrusion Detection Systems (IDS)	i. The purpose of these robust and effective encryption countermeasure techniques is to protect communication protocols from several types of attacks, including routing and eavesdropping assaults. ii. IDS functions primarily as an auxiliary defense at the communication level, overseeing the network activities and communication channels and triggering an alarm in the event of any irregularity, such as an infringement of a pre-established policy.
3.	**Jamming attacks**	Secure Data deduplication	Getting rid of redundant data and making use of IoT network capacity necessitates getting rid of duplicate versions of data on intermediary EC nodes. Regretfully, this will expose private data to unauthorized individuals. Secure data deduplication is employed as a defensive measure to this problem, allowing proxies to access the copied data without being aware of it [25,41].
4.	**Eavesdropping or Sniffing**	Cryptographic Schemes	During their deliberation on sniffing and eavesdropping attacks, Fazeldehkordi and Gronli [53] suggest cryptographic techniques as a defense. By rendering the primary message or data obscure, cryptographic schemes are techniques and procedures that safeguard transmission and shield sensitive information from illegal access or alteration.
5.	**Integrity attacks against ML**	Outlier Detection	Reducing the impact of introducing erroneous data points to the outcome is the shared objective of nearly all defenses against integrity attacks on machine learning techniques. The training set considers these erroneous data points to be outliers. Based on solid facts, Rubinstein et al. have created a defensive framework against poisoning assaults that attenuate the consequences of poisoning.
6.	**DDoS attack**	i- IDSs ii- Securing firmware update	i- IDS functions as a sentry for the digital age, constantly monitoring the activities and communication channels in order to detect and promptly notify any unusual activity that could be a sign of an attack. By identifying

			anomalous queries to the node, it offers a dependable method of thwarting attacks that are the cause of sleep deprivation and battery depletion. ii- The goal of this strategy is to guarantee the firmware—the software that manages the functioning of EC systems and IoT devices—as well as its integrity, authenticity, and secrecy. Secure boot, firmware signing, and frequent upgrades are a few secure firmware development and deployment techniques that can help shield these systems from virus, illegal usage, and other attack vectors [53].
7.	**Inessential logging attack**	Pre-testing	Pre-testing aims to determine the range of potential instances of attack and mimics these circumstances to see the system's responses. It also indicates which data should be recorded and which data is too sensitive to be kept on file [41].
8.	**Physical attack/tampering**	Tamper proofing & self-destruction	In order to strengthen defense against physical assaults, nodes are sometimes coupled with hardware. In order to prevent tampering, various technical and electrical tamper-proofing approaches have been pitched for the physical node packages. These methods have been utilized in the past for home automation sensors, such as smoke detectors. Furthermore, employing self-destruction processes offers an additional line of defense against direct physical attacks.
9.	**Non-network side channel attack**	i- Secure & firmware update ii- De-patterning data transmission iii- Minimizing information leakage	i- Firmware updates for networks can be stably installed either directly—by utilizing USB connections, for example—or remotely—by using broadcast messages from EC servers to publicize and distribute current firmware versions. To guarantee hotfixes, both approaches need fidelity and authentication [41]. ii- This tactic stops side-channel assaults by purposefully altering the traffic pattern using fictitious packets [40,41]. iii- Annexing randomized delay [58], purposefully creating noise [98], balancing Hamming weights [99], employing constant execution path code [99], enhancing cache designs [100], and shielding are a few other well-known strategies for countering side-channel attacks.
10.	**Routing information attacks**	i- IDS ii- Reliable routing protocols	i- Information Detection Systems (IDS) are used to reduce security risks by identifying Black Hole and routing attacks, which include altering or faking data. ii- The fact that intermediary nodes or servers may need prompt access to transmit content prior to relaying it is a fundamental feature of IoT networks that makes the design of safe routing algorithms more difficult.
11.	**Unauthorized control access**	Role based authorization	This mechanism assesses whether an entity, such as a service provider, router, or an edge node may access, distribute, or alter the information for the purpose to prevent request responses from malicious nodes or intruder in the system.
12.	**Privacy breach**	i- Secure data aggregation ii- Secure data analysis	i- It is an utterly secure, discreet, and effective data compression technique. Under this strategy, each device will separately encrypt its unique data using homomorphic encryption algorithms (such the Brakerski-Gentry-

			Vaikuntanathan (BGV) cryptosystem) ahead of delivering it to the EC nodes. The latter will transmit the total findings to the central cloud servers after aggregating all the data to calculate the multiplication of each separate data point [25,39,41]. ii- A number of artificial intelligence (AI) capabilities have been moved to EC devices and nodes from centralized cloud owing to the rapid advancements in EC devices. This leads to the enhanced latency, security and anonymity [25,41].
13.	**Replay or freshness attacks**	Secure time stamp schemes	Cho et.al [54] proposed an RFID-oriented protocol which successfully prevents replay attacks along with spoofing and location tracking.
14.	**Security threats from/on IoT devices**	i- Authorization ii- Authentication iii- Decentralization	i- Responses to queries sent out by malevolent EC nodes or attackers are blocked by this approach. The process examines whether a particular entity—such as EC node or component, service provider, a router, etc.— has the ability to view, alter, share, or manage data [40,42,]. ii- Encouraging entities to co-authenticate spanning over various trust domains is necessary in the EC-augmented convoluted environment encompassing handover and single/cross-domain. iii- Using EC nodes for dispersing the confidential data such that none of the node has full cognizance of the details, this technique provides anonymity [41].
15.	**Other attacks**	i- Information flooding ii- Combining EC and blockchain technology	i- This scheme repels hackers from discovering and shadowing the demesne of the information. ii- A developing technique called blockchain offers a dependable, secure, and trustworthy basis for data regulation and information exchanges between different operational network edge units. With the use of voting and consensus algorithms, it establishes norms that allow decentralized systems to decide collectively how to carry out certain transactions. As a result, there will be no need for a central, trustworthy middleman to facilitate communication between the interconnected IoT edge equipment, and reliable audit-level tracing of EC-assisted IoT data flows would be guaranteed [27].

B. Tackling Security issues with security-based Architectures

IoT networks' inherent characteristics give rise to a number of security risks, including those with user data confidentiality and data authentication. Some of the security risks associated with IoT networks can be mitigated by EC technology; this section demonstrates concepts that address these risks both with and without Software-defined Networking (SDN).

— ***Security Architecture without SDN:***

- *EC-IoT Coalescing Virtual IoT Devices (ECV)*

An ECA-IoT was suggested by Kanti et al. [45] to zhoosh up smart metropolises. An intermediary layer for processing data from the IoT is furnished by this framework. The six primary constituents that make up this architecture are:

o collection proxies, that are responsible for linking all IoT devices to several other elements;

o data validation, entrusted with securing the authenticity of the data obtained;

o metadata annotation, which appends new data to the native data after affirming its accuracy to facilitate the processing of data at virtual IoT devices;

- security, which symmetrically encrypts IoT data prior to sending it to the cloud servers so as to safeguard its privacy;
- Virtual IoT device (VID), which processes IoT data and assists data annotation and validation;
- Actuation, lastly it is liable for initiation an actuation only in certain pre-define conditions.

- *SIOTOME: Edge-ISP Joint Architecture for IoT Security*

With an eye towards precocious recognition of IoT- induced perils and loopholes, Haddadi et al. [46] conjoined Internet Service Provider and the network edge to achieve this goal. SIOTOME is an IDS that attains understanding form several disciplines (like a single home network, cloud network, or ISP) to discern diverse categories of cyberattacks, in contrast to typical networks where the system shields only a singular domain from an attack. The two upper echelons domains that embody the SIOTOME system architecture are SIOTOME/cloud and SIOTOME/edge. The ensuing constituents are potentially present in the system framework which was deployed in a smart home:

- the edge controller, elicited from SDN supervises gateway configuration;
- the edge data collector, that amasses data from IoT devices;
- the edge analyzer, that assays collected data and functioning of IoT devices;
- and the gateway, which links the home network to the internet via ISP and compels the in-home network to function under a single controller.

The building block of SIOTOME/cloud components include:

- the cross-domain controller, which is responsible for managing the traffic between domains;
- the cloud collector, which gathers the record from the data collector at edge and stays alert for any nefarious activity on the ISP network;
- the cloud analyser, has same functioning as the edge analyser and assesses data curated by the collector,
- the cloud controller, is a SDN controller that regulates data at the ISP stage also counters against threats discovered by the analyzer;
- lastly, a reliable communication component that upholds protected transmission between multiple elements of the system.

- *Edge-Computing Architecture for Mobile Crowd Sensing (MCS)*

Four levels make up the framework that Marjanovic et al. [47] put forward in his research to assist mobile crowd sensing:

- the user equipment layer, which includes on-body sensors and other IoT tools;
- the EC layer, which manages workers in defined zones;
- the cloud-computing layer, which processes dense data;
- and the application layer, who's main purpose is analysing the data.

Among the various advantages of this architecture are its ability to reduce latency by notifying mobile devices in the event of a mobile crowd-sensing situation and safeguard data privacy through the division and distribution of data to servers.

- *Lightweight Security Architecture Based on Embedded Virtualization and Trust Mechanisms for IoT Edge Devices (LSV)*

Through the integration of embedded virtualization and trust mechanisms, the authors of the research [48] presented a safe ECA-IoT in order to safeguard edge devices bereft of re-engineering the installed applications in edge devices. Fidelity of executed code, run-time state integrity, and confidentiality of items perpetually retained are among the security needs that are guaranteed by the suggested design. The four security methods that make up the security framework are secure boot, secure key storage, secure interdomain transmission, and security by separation. The two pillars of edge device security are:

1. Chain of Trust (CoT), which means that the edge device can only start up if public-key cryptography is used to execute cryptographically signed software that has been verified by a reliable source,
2. Root of Trust (RoT), which ensures that the running software at the edge device is authentic, irrefutable, and unclonable.

Furthermore, the keys are kept in distinctive, invulnerable hardware that manages the verification and ROT procedures. Consequently, the embedded virtualization design comprises of many virtual machines (VMs) from various manufacturers, enabling an additional layer of safe boot verification.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

- *Privacy Preservation While Aggregating the Data (P2A)*

A design that manages communication and compute overhead, composite aggregation is suggested by Yang et al. [49] for the protection of sensory data privacy. The four primary components of this architecture — fog nodes, sensors, fog centres, and a cloud server are illustrated in Fig.8. Intelligent devices have sensors to gather information. The data gathered is split into two halves and delivered to two distinct fog nodes to maintain the privacy. The aggregation requests originating from fog centres are stockpiled in these fog nodes. Subsequently, fog nodes' requests are routed through fog centers to collate their findings. Following calculation procedure, the primary query results are transmitted to the cloud center. A service provider presides over the cloud center, which functions as data aggregator.
Cloud Centres and fog centres are categorized as dubious elements in the architecture proposed by them, as these entities attempt to accumulate clandestine information. Since fog nodes cannot engage in collusion, they show an inquisitive nature towards the original data and thus can only be partially trusted. A ML-based comprehensive aggregation system was presented by Yang et al. to aggregate data while maintaining privacy. The model is trained to anticipate different query answers, but it only provides a projected value—not the underlying data. The information gathered from every region serves as the training set.
An explanation of the protocol's operation is provided below. Query types that are authorized to be sent to fog centres from cloud centres include q-percentile, average, max, min, medium, and summation aggregate. All the aforementioned queries are forwarded to the fog center via the cloud center. Fog centers formulate their own suite of catechizes based on the source queries they get from cloud centers, as they are incapable of responding to cloud-center requests. After splitting sensory input into two halves, the sensors report the fog-node sensory data. On the basis of the fresh set of requests that the fog center produced, the procured data is coached and forecasted. After receiving the anticipated values, the fog center retransmits them to the cloud center.

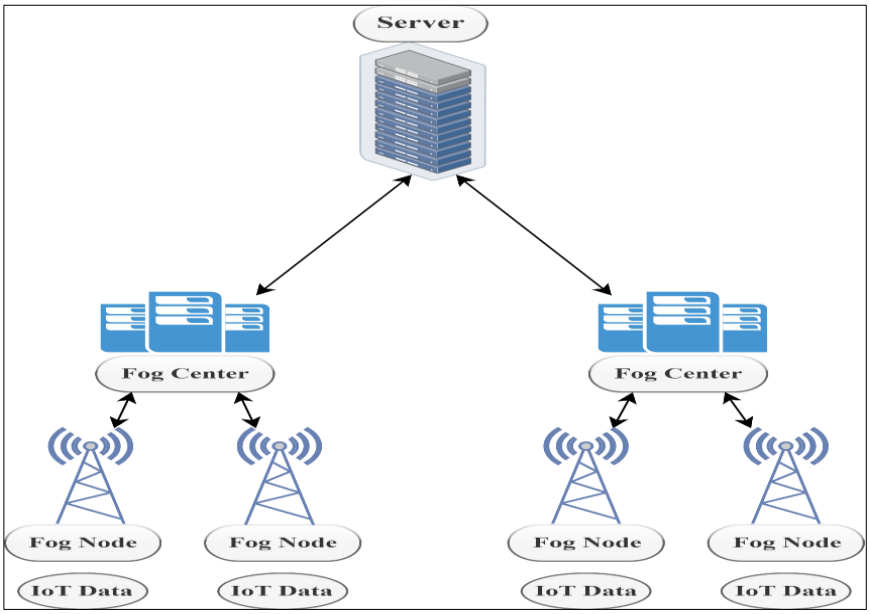

Fig.8 Privacy Enhancing Framework

- *A Secure IoT Service Architecture with Efficient Balance Dynamics Based on Cloud and Edge Computing (SBDC)*:

IoT device constraints prevent standardized security solutions from thwarting IoT threats. To fend off attacks like these and analogous service demands or repeated handles, Wang et al. [50] adopted the dispersed edge devices across the network to formulate a reliable architecture centered around trust mechanisms. The service and service-parsing templates make up the service template. The edge platform, the edge network, and the cloud comprise the three fundamental building blocks of this design. The above constituents are further broken down into three layers—app-service layers, data processing layers, and data gathering layers. Cloud computing resides at the application-service layer, whereas the edge network and edge platform are positioned in the data-collection, data-processing, and application-service levels. This framework satisfies end-user criteria including authenticity and accuracy, erratically modifies IoT strain, and establishes

a trust state of IoT devices before selecting an authorized device to execute services. The responsibilities of this edge platform include: executing virtualization procedures by transforming tangible gadgets into virtual devices; adapting cloud load spontaneously by executing certain functions on the edge layer; guaranteeing IoT credibility by collaborating with the network's edge at the data level; and creating the service-parsing template, which is liable for stowage of the parsing techniques and cognate information. Service-parameter templates must be developed and preserved on the cloud, along with matching data and parsing procedures to locate matching services. Services Requisitioning additional resources than the ones found in the edge-processing layer must be processed, outdated information must be logged for future analysis, and data mining is accomplished by the cloud. Their architecture was assessed by a series of extensive tests conducted with the aid of MATLAB. There is one cloud and four IoT networks proposed in this architecture. The outcomes demonstrate that this design may improve data fidelity and operational effectiveness.

— **Security architecture with SDN**

The ECAs-IoT that manage security concerns in IoT networks and use SDN in their designs are covered in this part.

- *Blockchain-SDN-Enabled Internet-of-Vehicles Environment for Fog Computing and 5G Networks (BSDNV)*

The integration of blockchain technology with SDN for VANET (Vehicular Ad-hoc Network) networks that utilize 5G and fog computing was suggested by Gao et al. [51] as a way to ameliorate veracity of the networking platforms. SDN cinches the completion of control procedures, fog computing prevents recurrent abnegations, and blockchain fosters trust amongst components of the system. Following are the elements that make up the BSDNV-

i. RSUs: they establish connection with the BBU or broadband unit;
ii. Base stations: are coupled with BBU;
iii. Vehicles: are constructed from OBU a.k.a on-board unit that functions as an end-user and is linked with the SDN. Packet transmission and vehicle telematics, including environmental and speed data are under the purview of OBUs;
iv. Fog nodes: SDN controller is responsible for manoeuvring the fog nodes;
v. Fog Zones: A profusion of fog nodes is represented by fog zones;
vi. RSU hubs (RSUH): based on their locale acumen, these systems make judgments that regulate vehicle overhead, bind fog zones together and with the SDN controller, along with minimizing the outlay on SDN controllers.
vii. SDN controller: regarded as the principal element of this design, it is amenable to manage mobility, craft protocols, preprocess and analyze data, and allocate resources;
viii. Blockchain: The servers that administer policies, data, authentication, and access are called nodes in the blockchain.

The efficacy and coherency of the network are ensured by the collaboration between the blockchain and SDN. Based on simulation results, this design enhances the security and orchestration of a VANET.

- *Software-Defined Fog-Node-Based Distributed Blockchain Cloud Architecture (SDNDB)*

For a safe way to increase latency, Sharma et al. [52] suggested a tripartite fog framework built on SDN and blockchain:

i. Device Layer: it comprises of IoT devices that detect and relay data to the uppermost layer;
ii. Fog Layer: encompasses a SDN controller based on Blockchain. Every node oversees a tiny related community that is in charge of prompt service delivery and IoT data analysis. By utilizing the packet migration and flow rule analysis functions, each fog node bolsters the network’s defenses from saturation attacks.
iii. Cloud Layer: Substantial event detection, behavior analysis, and prolonged pattern recognition are the functions of the cloud layer, which is made up of a decentralized cloud built on blockchain.

Induced latency, reaction time, and the precision of identifying the saturation attack via a testbed are used to assess this framework’s potence. The outcomes demonstrated competence of this infrastructure in comparison to a traditional core-based cloud computing architecture.

5. Open Challenges & Future Scope

The article has already outlined a multitude of attacks on the security of entities and people, along with defense mechanisms. Hereunder, a few recently discovered security issues that sparse coverage has been explored and also offer suggestions for emerging areas of investigation.

- *Precarious edge devices:* The potential for attacks widens as a result of the edge layer's requirement for safety protection, even while it gives us a new space to implement innovative IoT security measures. Fortifying the edge layer is a formidable task since, unlike cloud data centers, most edge nodes perhaps not be physically guarded and managed by a robust staff of cybersecurity professionals. This necessitates intensified exploration in order to provide edge device security solutions.

- *Rapid proliferation of weak links:* Prevalent IoT services operate on bijou, battery-operated devices with constrained processing and storage capacity. Numerous products on the market today do not endorse stringent secure cryptographic protocols because of their unique features and cost considerations that the makers deemed significant. As a result, there are now a great deal of weak links in the infrastructure or network that an attacker may use to target other purportedly safe points in the network. Therefore, developing innovative, low-power security and privacy strategies at various IoT infrastructure entities supported by ECs might be a fruitful research avenue.
- *Holistic Trust Management Frameworks:* Due to the diversity of infrastructures and edge device types that make up EC aided IoT networks, they are eclectic. Furthermore, the capacity of some edge nodes and servers to do intricate computational tasks has incentivized engineers to shift trust modeling and assessment from cloud-based servers to edge nodes. Diverse trust domains belonging to different functional units will therefore co-abide in IoT networks supported by EC, presenting a number of unexplored research questions. Developing vigorous and nuanced transdisciplinary access control framework that comprehends inter-group hierarchical access control methods and the inter-domain nature of the EC- IoT network is necessary to rectify these concerns.
- *Unconventional data usage:* Nowadays, Internet-connected sensors are widely used in everyday life due to the increasing usage of ubiquitous computing made possible by IoT technology. A few studies have endeavoured over the past few years to illuminate hitherto unanticipated applications of various kinds of user-specific or environmental data obtained by Internet-connected sensors. For instance, a list of confidentiality-focused such as the number of occupants, individual habits, and daily schedules, has been supplied by McKenna et al. based on data acquired by smart meters on the power usage in smart homes [55]. Although prior studies have been conducted, it is still unclear how much private information may be deduced from data that is ostensibly unimportant.

6. Conclusion

The allure of EC technology is on the rise since it can process data in a close proximity to end-users, which is imperative for IoT implementations, especially those that require expedited processing. The research explicitly presented the benefits of EC abetted IoT architecture in comparison to traditional IoT. Following that, a variety of significant EC-IoT security concerns have been unveiled. This study aimed to provide a progressive summary of various EC-IoT security risks aiming for an individual being or a component. Numerous innovative edge-based security concepts for IoT security have been made possible by the emergence of edge computing. Our thorough assessment focuses on the many categories and forms of potential threats to IoT network security and privacy, along with the appropriate defenses. In conclusion, a thorough overview of unresolved security research queries and difficulties is provides, along with potential research routes, within the framework of EC-assisted IoT.

References

1. Chart: Global Data Creation is About to Explode | Statista
2. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2017). Mobile edge computing: A survey. *IEEE Internet of Things Journal*, *5*(1), 450-465.
3. Read more at: https://viso.ai/edge-ai/edge-intelligence-deep-learning-with-edge-computing/
4. Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing," in *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738-1762, Aug. 2019, doi: 10.1109/JPROC.2019.2918951.
5. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, Oct 2016.
6. T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, “Collaborative mobile edge computing in 5g networks: New paradigms, scenarios, and challenges,” IEEE Communications Magazine, vol. 55, no. 4, pp. 54–61, 2017.
7. P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, “Edge-centric computing: Vision and challenges,” ACM SIGCOMM Computer Com munication Review, vol. 45, no. 5, pp. 37–42, 2015.
8. Ren, J.; Zhang, D.; He, S.; Zhang, Y.; Li, T. A survey on end-edge-cloud orchestrated network computing paradigms: Transparent computing, mobile edge computing, fog computing, and cloudlet. ACM Comput. Surv. (CSUR) 2019, 52, 1–36.
9. October 2023 IEEE World Forum discussion.
10. https://www.techrepublic.com/article/iot-edge-work-together/
11. Edge Computing Market Size To Reach $155.90Bn By 2030 (grandviewresearch.com)

12. Bajaj, K.; Sharma, B.; Singh, R. Implementation analysis of IoT-based offloading frameworks on cloud/edge computing for sensor generated big data. Complex Intell. Syst. 2022, 8, 3641–3658.
13. Saeik, F.; Avgeris, M.; Spatharakis, D.; Santi, N.; Dechouniotis, D.; Violos, J.; Leivadeas, A.; Athanasopoulos, N.; Mitton, N.; Papavassiliou, S. Task offloading in Edge and Cloud Computing: A survey on mathematical, artificial intelligence and control theory solutions. Comput. Netw. 2021, 195, 108177.
14. Shirazi S N, Gouglidis A, Farshad A, et al. The extended cloud: review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE J Sel Areas Commun, 2017, 35: 2586–2595
15. Antonakakis M, April T, Bailey M, et al. Understanding the Mirai botnet. In: Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), 2017. 1093–1110
16. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, Oct 2017.
17. Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: a primer," *Digital Communications and Networks*, vol. 4, no. 2, pp. 77–86, 2018.
18. S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: convergence of computing, caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779, 2017.
19. Usman, M., Jan, M. A., & Puthal, D. (2019). Paal: A framework based on authentication, aggregation, and local differential privacy for internet of multimedia things. *IEEE Internet of Things Journal*, *7*(4), 2501-2508.
20. Wu, H., Sun, D., Peng, L., Yao, Y., Wu, J., Sheng, Q. Z., & Yan, Y. (2019). Dynamic edge access system in IoT environment. *IEEE Internet of Things Journal*, *7*(4), 2509-2520.
21. Yang, A., Zhang, C., Chen, Y., Zhuansun, Y., & Liu, H. (2019). Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms. *IEEE Internet of Things Journal*, *7*(4), 2521-2530.
22. Cicirelli, F.; Gentile, A.F.; Greco, E.; Guerrieri, A.; Spezzano, G.; Vinci, A. An Energy Management System at the Edge based on Reinforcement Learning. In Proceedings of the 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Prague, Czech Republic, 14–16 September 2020.
23. Tom, R.J.; Sankaranarayanan, S.; Rodrigues, J.J. Smart Energy Management and Demand Reduction by Consumers and Utilities in an IoT-Fog-Based Power Distribution System. IEEE IoT J. 2019, 6, 7386–7394.
24. P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for internet of things realization," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2961–2991, Fourthquarter 2018.
25. J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," IEEE Network, vol. 33, no. 2, pp. 50–57, March 2019.
26. J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439–449, Feb 2018.
27. B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues," IEEE Internet of Things Journal, 2018.
28. M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, "Edge computing perspectives: architectures, technologies, and open security issues," in 2019 IEEE International Conference on Edge Computing (EDGE). IEEE, 2019, pp. 116–123.
29. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K. Mobile edge computing: Survey and research outlook. arXiv 2017, arXiv:1701.01090.
30. Chen, M.; Li, W.; Hao, Y.; Qian, Y.; Humar, I. Edge cognitive computing based smart healthcare system. Future Gener. Comput. Syst. 2018, 86, 403–411. [CrossRef]
31. Shi, W.; Dustdar, S. The promise of edge computing. Computer 2016, 49, 78–81.
32. Yi, S.; Qin, Z.; Li, Q. Security and privacy issues of fog computing: A survey. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications, Qufu, China, 10–12 August 2015; pp. 685–695.
33. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.
34. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, https://doi.org/10.1155/2017/9324035.
35. I. Ahmed, G. Jeon, and F. Piccialli, "A deep learning-based smart healthcare system for patient's discomfort detection at the edge of internet of things," IEEE Internet of Things Journal, 2021.
36. W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.

37. J. Ren, Y. He, G. Huang, G. Yu, Y. Cai, and Z. Zhang, “An edge computing-based architecture for mobile augmented reality,” IEEE Network, vol. 33, no. 4, pp. 162–169, 2019.
38. Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A survey on mobile edge computing: The communication perspective,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017.
39. Y. Lu and L. D. Xu, “Internet of things (IoT) cybersecurity research: A review of current research topics,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103–2115, April 2019.
40. A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, Oct 2017.
41. D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, “A survey on secure data analytics in edge computing,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4946–4967, June 2019.
42. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct 2017.
43. D. He, S. Chan, and M. Guizani, “Security in the internet of things supported by mobile edge computing,” IEEE Communications Magazine, vol. 56, no. 8, pp. 56–61, August 2018.
44. R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,” Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.
45. S. K. Datta and C. Bonnet, "An edge computing architecture integrating virtual IoT devices," 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 2017, pp. 1-3, doi: 10.1109/GCCE.2017.8229253. keywords: {Edge computing;Computer architecture;Data processing;Cloud computing;Actuators;Intelligent sensors;Edge Computing;IoT;Local Data Processing;Virtual IoT Device},
46. Haddadi, H.; Christophides, V.; Teixeira, R.; Cho, K.; Suzuki, S.; Perrig, A. SIOTOME: An edge-ISP collaborative architecture for IoT security. In Proceedings of the IoTSec, Orlando, FL, USA, 17 April 2018.
47. Marjanovi´ c, M.; Antoni´ c, A.; Žarko, I.P. Edge computing architecture for mobile crowdsensing. IEEE Access 2018, 6, 10662–10674.
48. Tiburski, R.T.; Moratelli, C.R.; Johann, S.F.; Neves, M.V.; de Matos, E.; Amaral, L.A.; Hessel, F. Lightweight Security Architecture Based on Embedded Virtualization and Trust Mechanisms for IoT Edge Devices. IEEE Commun. Mag. 2019, 57, 67–73.
49. Yang, M.; Zhu, T.; Liu, B.; Xiang, Y.; Zhou, W. Machine learning differential privacy with multifunctional aggregation in a fog computing architecture. IEEE Access 2018, 6, 17119–17129.
50. Wang, T.; Zhang, G.; Liu, A.; Bhuiyan, M.Z.A.; Jin, Q. A secure IoT service architecture with an efficient balance dynamic based on cloud and edge computing. IEEE Internet Things J. 2018.
51. Gao, J.; Agyekum, K.O.B.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A Blockchain-SDN enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. IEEE Internet Things J. 2019, 7, 4278–4291.
52. Sharma, P.K.; Chen, M.Y.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 2017, 6, 115–124.
53. E. Fazeldehkordi and T.-M. Grønli, “A Survey of Security Architectures for Edge Computing-Based IoT,” IoT, vol. 3, no. 3, pp. 332–365, Jun. 2022. [Online]. Available: https://www.mdpi.com/2624-831X/3/3/19.
54. Cho, Chang-Hyun, et al. "Design of RFID mutual authentication protocol using time stamp." *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*. IEEE, 2009.
55. E. McKenna, I. Richardson, and M. Thomson, “Smart meter data: Balancing consumer privacy concerns with legitimate applications,” Energy Policy, vol. 41, pp. 807–814, 2012.