Cybersecurity Challenges and Solutions in Edge Computing for IoT

Dr. Sinciya P.O
Dept. of Computer Science & Eng.
Amal Jyothi College of Engineering
Kottayam, India
posinciya@amaljyothi.ac.in

Evelyn Susan Jacob
Dept. of Computer Science & Eng.
Amal Jyothi College of Engineering
Kottayam, India
evelynsusanjacob@gmail.com

Steve Alex
Dept. of Computer Science & Eng.
Amal Jyothi College of Engineering
Kottayam, India
stevealex365@gmail.com

***Abstract*— As the field of Internet of Things (IoT) continues to expand, it has created a newly connected environment, transforming physical objects that surround us into an ecosystem of information that is rapidly changing the way we live. Meanwhile edge computing architectures have introduced a new decentralised approach to computing by bringing the services closer to the data source and offering better performance and more security than traditional cloud centric IoT architectures. So, in this research paper, we discuss what exactly comprises an Internet of Things architecture. We will analyse the changes that edge computing brings about to the table. We will also explore how these architectures can be integrated to design better IoT solutions for society and industry.**

Keywords—IoT, Cyber Security, Edge computing, Security

I. Introduction

The Internet of Things (IoT) has brought about a transformation in modern society by being able to integrate devices, sensors and systems across various domains presenting a unified and connected experience to users. It has thus simplified tasks and helped us enhance our productivity.
Meanwhile the widespread adoption of IoT technologies has also led to the creation of significant cybersecurity challenges. The interconnected nature of IoT ecosystems itself and the huge number of devices and data that they generate create weaknesses that pose a serious risk to our society. Thus, it is crucial to protect them in order to maintain trust in these technologies.

One promising solution to improving the security of such systems is edge computing. Edge computing involves processing data at the edge of the network closer to the source than processing it through the cloud.
Such architectures can reduce latency to just a few milliseconds and minimise data transmission over external networks. Such an approach will reduce exposure to external threats and improve safety and security throughout the network.

Edge computing also presents some unique cybersecurity challenges as its decentralised structure introduces new patterns of attack requiring more careful consideration and preparation. It makes it absolutely critical to ensure the data is protected and other communication channels between the edge and the centre of the network and kept secure.

II. History

The term "Internet of things" was first coined by Kevin Ashton of Procter & Gamble in 1999 to refer to devices that could be identified by means of RFID (Radio-frequency identification) technology.
Although smart devices connected to a network were present as early as 1982 when a modified Coca-Cola vending machine [2] at the Carnegie Mellon University became the first ARPANET-connected appliance, the concept itself only gained more popularity after the "Six Webs" framework was presented at the World Economic Forum in 1999.
Cisco Systems, which in 2010 defined the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people" estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84.

III. Cybersecurity Challenges in IoT

The main cybersecurity challenges faced by IoT mainly have to do with the lack of standardisation of the equipment and the resulting lack of consistent security protocols.

Their main issues can be summarised as follows:

Unauthorised data access

IoT devices often tend to collect sensitive data which make them vulnerable to hackers gaining access to confidential information. It is also challenging to ensure secure communications between IoT devices and servers as they could be using a wide range of devices and protocols between them.

Device Security Concerns

Since there is no universal security standard for the various IoT devices that are manufactured by different

10.5281/zenodo.12515957

companies it leaves holes in their levels of security. Many IoT devices lack proper firmware security which leaves them susceptible to exploits and remote attacks.

Network Security

IoT networks also sometimes rely on insecure protocols like MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) etc. which makes them more susceptible to eavesdropping, spoofing and data manipulation. Attackers can intercept and manipulate the data exchanged between devices and the network thus compromising security.

Performance issues

There are also performance issues that can arise when many devices are connected, since IoT devices tend to operate with limited processing power and bandwidth. This can also complicate securing them and lead to system failure under heavy loads.

IV. Edge Computing in IoT

Edge computing is an architecture in which the data is processed at the periphery of the network, closer to the origin of the data collection. The term was first utilized in the 1990s to refer to content delivery networks which were used to deliver content to users from servers located closer to users. They were useful in enabling more real-time applications and offline operating capabilities. It moves some portion of storage and compute resources out of the central data centre and closer to the data source.
A central cloud computing infrastructure will run beyond its capabilities for analysing the data collected by IoT devices. Edge computing architecture has eliminated the processing burden at the centralized infrastructure [1].

Edge Computing Architecture

An edge computing architecture consists of:

Edge devices: These are the IoT devices that are located on the periphery of the network closer to the source data. These include the arrays of sensors that are part of smart home systems and wearables.

Gateways: These act as the intermediaries between the edge devices and the cloud. They usually preprocess the data before sending it to the cloud. They also help secure the communication channels.

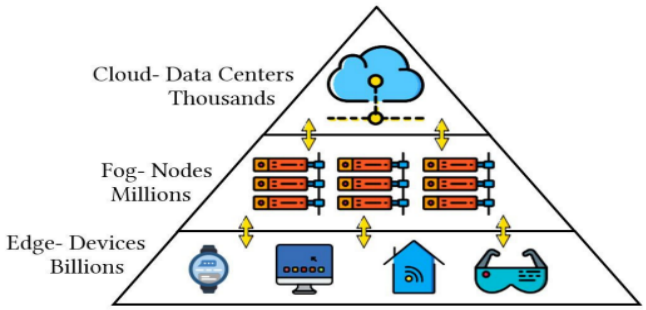

Fig. 1. Typical edge computing architecture.

Fig.1 Typical Edge Computing Architecture

This figure represents the communication from several IoT devices to fog nodes and then to cloud data centres [1].
Fog computing is a decentralized computing system which enhances cloud capabilities to accommodate IoT requirements. It acts as a computing layer between the cloud and the edge. The fog nodes decide whether the data received needs further processing or whether it should be sent to the cloud. For these reasons, fog computing is considered as a super division of edge computing.
The cloud storage provides a cost-effective, scalable solution for storing and managing data generated from IoT devices. It also provides the required infrastructure and processing power to carry out real time data processing.

Advantages of Edge Computing for IoT security

The processing of data closer to the source can filter out sensitive information before being transmitted to the cloud thus reducing the risk of unauthorised access.
Transmitting only the relevant data minimises the exposure of sensitive information thus reducing the risk. Processing data locally also reduces latency and enhances its real-time responsiveness.
It can also help us implement authentication at the device level, ensuring that only authorised devices can access it. These access control policies can be enforced locally thus reducing dependency on centralised servers.
Distributed Denial of Service (DDoS) attacks can disrupt IoT services that are dependent on centralised servers. Edge computing distributes tasks across multiple nodes thus making it harder for attackers to launch large scale DDoS attacks.

Use cases for Edge Computing
Some of the edge computing use cases are:

a) *Smart Grids:* Edge computing is one of the core technologies which help enterprises manage their energy consumption through a smart grid network. Sensors and IoT devices connected to edge platforms in factories,

plants and offices can be used to monitor energy use and analyse their consumption in real-time.

b) *Predictive maintenance:* Edge sensors that monitor machine health are used to perform analytics in real time with very little latency. It enables them to detect any changes which need to be made to their production lines before a failure can take place.

c) *In-hospital patient monitoring:* Data collected locally can be processed on an edge while maintaining data privacy. It is also capable of notifying practitioners in real time of unusual patient behaviours that needs to be observed.

d) *Smart Homes:* Smart homes are equipped with numerous IoT devices which help in the monitoring and metering of various utilities like water, gas and electricity. The data collected is send to the edge to provide real time analytics [4] .

e) *Video Surveillance:* Video content that is obtained and shared from several sensors and devices are analysed to extract the required data. Different video contents are obtained and are shared from several sensors and devices. Security applications use the archived video contents to extract the required data, and this is implemented with the help of cloud computing [4] .

V. Implementing Edge Computing for IoT Security

Security Considerations in Edge Computing Deployments

Figure 2 depicts how each edge deployment has five core areas of exposure that makes it vulnerable: data, network, operating system (OS) platform, software and hardware [5].

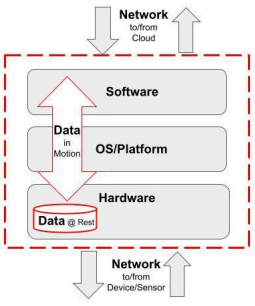

Fig.2. Edge Technology Components

Edge deployments are all about capturing, collecting and processing raw data at the point where it is generated by some event. Data is said to be in motion when it is moving from a source to the destination. One effective way to protect data in motion or at rest is by using encryption techniques [5].

The RedHat OpenShift is such a platform which provides features like configured cipher suites, encrypted east/west traffic, volume encryption etc. for data protection [5].

An automated, consistent, scalable, policy driven network configuration is required for protecting against network attacks. Zero Trust Network Access (ZTNA) is one such technology which can be used to avoid unwanted edge access to data or cloud services [5].
ZTNA provides remote access to applications and data by having clear access control policies. The major difference between ZTNA and VPN is that VPN allows access to an entire network whereas ZTNA grants access only to specific services and resources. It also offers protection against lateral attacks so that even if attacker gains access, they would not be able to scan to locate any other services [6]. An estimated 60% of businesses would have embraced zero trust as a starting point for security by 2025, according to Gartner [7][8].

The RedHat Ansible Automation Platform also supports policy driven network configuration with automated network configuration, network infrastructure awareness and network validation [5].

Another major threat that needs to be considered are imposter devices. One way to resolve this threat is by device attestation [5]. This helps in identifying devices that have been tampered with or has any outdated insecure software running on them. The security threats faced are not always external, it can also be individuals within organisations who can accidently or intentionally introduce software that could cause security issues.

Edge Computing Platforms

Edge computing platforms help in maximizing the power of edge computing at distributed locations and on remote devices. This enables us to achieve ultra-low latency, better performance and lower cloud costs for IoT systems [9] .
Features of an Edge Computing Platform:

1. Edge Application Support
2. Analytics insights
3. Cloud to edge infrastructure
4. Edge Security
5. IoT enablement

Edge computing platforms can be used for a wide range of use cases, and they can be paid or open source. Some commonly used platforms are:

a) *Alef Private Edge Platform*: Alef is a New York based edge computing company founded in 2009. They were reportedly the first API Platform company to give organisations and developers the freedom to create, control and customize their own private network infrastructure.

b) *Azure IoT Edge*: Azure IoT Edge is part of Microsoft's intelligent cloud-to-edge computing solutions suite. It helps in scaling out and managing IoT solutions from the cloud.

c) *ClearBlade:* It is an Austin based company founded in 2007. It provides features like edge application support, analytics insights, edge security, IoT enablement as well as code portability.

d) *Eclipse ioFog*: It is an integrated development environment developed by the Eclipse Foundation, supported by IBM. ioFog provides a standardized way to develop and remotely deploy secure microservices to edge computing devices.

e) *Google Distributed Cloud Edge*: Google Distributed Cloud Edge was launched in October 2021. It equips enterprises and communication service providers to deliver edge-enabled apps.

Strategies for Securing Edge Computing Environment

It is important to have a proper environment for edge computing. Some strategies which can help achieve this are:

a) *Zero Trust Architecture*: This is a cybersecurity approach used to deny access to an organisation's digital resources [10]. In this architecture both the user and the devices need to be authenticated to receive access. Zero Trust Architecture reduces unauthorized access to users and thus minimises the risk of data breaches.

b) *Encrypted Communication*: End-to-end encryption for communication ensures that the data transmitted across the network remains secure. Concepts like symmetric encryption, public-key cryptography etc are used to ensure data security.

c) *Edge device security*: This involves employing security measures such as device hardening, regular software updates, and the use of secure boot mechanisms [12]. The trusted execution environment (TEE) is a widely used technology to protect content and payment applications. Processor based security features are enabled by integrating security IP blocks. These provide physically unclonable functions (PUFs), unique IDs, secure sockets layer (SSL) and programmable root of trust cores [11].

d) *Container Security*: This offers a flexible and portable way to run applications by securing all components of containerized workloads, including container images and repositories as well as the container infrastructure.

e) *Behavioural Analytics*: This can help in analysing abnormal activities within the edge environment. When the normal behaviour is established, any deviations can be identified, and actions can be taken for potential security incidents [12].

f) *Regulatory compliance*: Following relevant cybersecurity regulations and standards is crucial for maintaining a proper environment for edge computing. It ensures that security measures are taken to protect sensitive data and that the organisation has met their legal requirements.

VI. SUMMARY

Through this analysis of IoT architectures and edge computing, it is evident that the integration of these modern technologies presents several significant enhancements for the security of connected devices. This research highlights the importance of addressing cybersecurity challenges present in IoT systems.

Edge computing has truly emerged as a promising solution by offering decentralized processing closer to the source of data which thus reduces latency and exposure to external threats. Edge computing architectures have contributed to increasing security by filtering out sensitive information locally, enforcing device-level authentication and mitigating Distributed Denial of Service (DDoS) attacks.

Moreover, this analysis has helped in highlighting various use cases where edge computing can be effectively applied, which ranges from smart grids to predictive maintenance and in-hospital patient monitoring. These use cases demonstrate the potential impact of edge computing in different domains, enabling real time analytics and improved operational efficiency.

The implementation of edge computing for IoT security requires encryption techniques, network security measures like Zero Trust Architecture and service attestation, and the optimal utilization of edge computing platforms. By adhering to regulatory compliance standards and advanced security strategies, organisations can create efficient environments for

edge computing deployments while safeguarding sensitive data.

VII. CONCLUSION

The analysis highlights the potential of integrating edge computing into IoT architectures to address cybersecurity challenges and innovate new possibilities in the industry. We also discuss the edge computing paradigm which extends services to the edge of the network. By using edge computing principles and implementing security measures, stakeholders can build secure IoT systems that empower society as a whole.

References

[1] M. Alrowaily and Z. Lu, "Secure Edge Computing in IoT Systems: Review and Case Studies," 2018 IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, USA, 2018, pp. 440-444, doi: 10.1109/SEC.2018.00060. keywords: {Edge computing;Task analysis; Computer architecture; Internet of Things;Sensors;Password;Edge computing, Security, Internet of Things (IoT)}K. Elissa, "Title of paper if known," unpublished.

[2] https://www.cs.cmu.edu/~coke/history_long.txt - "The "Only" Coke Machine on the Internet" Carnegie Mellon University. Retrieved 10 November 2014.

[3] https://stlpartners.com/articles/edge-computing/10-edge-computing-use-case-examples/

[4] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob and M. Imran, "The Role of Edge Computing in Internet of Things," in IEEE Communications Magazine, vol. 56, no. 11, pp. 110-115, November 2018, doi: 10.1109/MCOM.2018.1700906. keywords: {Edge computing;Cloud computing;Taxonomy;Real-time systems;Classification;System-on-chip;Medical services}

[5] https://www.redhat.com/en/blog/5-security-considerations-edge-implementations

[6] https://www.vmware.com/topics/glossary/content/zero-trust-network-access-ztna.html/

[7] https://cradlepoint.com/resources/blog/enterprise-zero-trust-implementation-from-poc-to-deployment/

[8] https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

[9] https://www.spiceworks.com/tech/edge-computing/articles/best-edge-computing-platforms/

[10] https://www.ptc.com/en/blogs/iiot/implementing-zero-trust-iot-solutions

[11] https://www.spiceworks.com/tech/iot/guest-article/security-for-iot-edge-processors/

[12] https://www.spiceworks.com/tech/iot/guest-article/security-for-iot-edge-processors/

[13] https://kanooelite.com/securing-edge-computing-environments-cybersecurity-for-decentralized-networks/