Reviewing the Characteristics and Infrastructure Optimization of Peripheral Network Virtualization

P N Madhu Kumar Bobbili, Research Scholar, Department of CSE ,

J.S University, Shikohabad.

Dr. Badarla Anil ,Professor ,Supervisor, Department of CSE,

J.S University,Shikohabad.

Abstract - The designs of Internet-of-Things (IoT) services have evolved as a consequence of the development of high-performance fog and edge computing as well as high-bandwidth connections. These advancements have made it possible to gather and analyze greater quantities of information of a higher caliber from IoT devices' immediate environments. However, newly enacted international standards and growing consumer awareness have exacerbated the need for data security, and firms who fail to safeguard the data of their customers now risk serious penalties both financially and in terms of their image. This research advises using fog computing and edge computing in order to manage sensitive user data and reduce the quantity of raw sensitive data that is accessible at various levels of the IoT architecture. In the end, this not only reduces the attack surface area, but it also enhances the speed of the architecture by distributing processing over several nodes and only sending data that has already been processed. A method like this, however, leaves itself exposed to attacks on the device level. To solve this issue, a System Security Manager is recommended to be used. It does this by continuously monitoring system resources and making certain that access to private data is limited to just those aspects of the device that really need it. In order to prevent a breach of data confidentiality caused by an attack, it is possible to partition critical information and set off an alarm inside the system.

Key Words - Edge Computing, Cloud to Edge, Edge Security, IoT, GDPR, Data Protection, Active Security, Embedded System, Cyber Resilience, Security Micro-architecture.

1. INTRODUCTION

The Internet of Things (IoT), which is a network of networked devices and services that benefit from embedded computing and communication, presents society with a number of clear potential benefits. Consumers and businesses alike may put these technologies to use to enhance and perfect a wide range of tasks, such as those involved in the automotive and transportation industries, healthcare, the management of buildings, and the administration of essential infrastructure. These tools and services, when applied appropriately, have the potential to harness user and environmental data that has been provided or inferred in order to improve aspects like safety, performance, convenience, reliability, and cost. The application of Artificial Intelligence (AI), Machine Learning (ML), and Data Analytics may help organizations enhance the customer experience, make better informed decisions, and even find new business models and market opportunities using the data that is available to them. It is anticipated that there will be one trillion Internet of Things devices in use by the year 2035. The flow of data brought about by the Internet of Things has opportunities and benefits; nevertheless, it also puts users' safety and privacy at jeopardy. It is necessary to handle the considerable design, supply chain, privacy, security, and safety challenges that occur with the large-scale integration and deployment of intelligent devices and related services that deal with sensitive data or critical infrastructure situations. These issues may be broken down into five categories: design, supply chain, privacy, and security. Safety is the sixth category. The current designs of IoT services are vulnerable to attacks and operational vulnerabilities that, if exploited, might result in significant data loss. Businesses would very certainly be in breach of a number of international data control regulations, such as the California Consumer Privacy Act (CCPA), the Japan Act on the Protection of Personal Information, and the General Data Protection Regulation (GDPR) of the European Union. These laws are just a few examples. Furthermore, false data manipulation has the potential to further block AI-powered, data-driven decision-making processes, which may result in deadly consequences.

The proliferation of devices that generate data has resulted in a considerable increase in the need for internet connectivity, data storage in the cloud, and computing power. From 216 ZB (Zettabytes) in 2016, it is expected that by the year 2021, the total quantity of data created and transmitted worldwide by Internet of Things devices would grow. It was predicted that data centers utilized a total of 416 terawatt-hours (TWh) of power in 2016, and this number is anticipated to more than quadruple by the year 2025. Data centers are the foundation upon which cloud computing is built. It has been determined that such an increase in consumption is not sustainable, which calls for the implementation of edge-based computing as well as other optimum methods of data processing and storage. Edge computing, when utilized appropriately, may minimize cloud-based workloads that deal with vast volumes of unnecessary personal data while giving low-latency outcomes that require less network bandwidth. All of this may be accomplished while edge computing maintains a critical component of the underlying architecture of IoT service design.

This presentation will provide a comprehensive discussion of the infrastructure and architecture-related problems associated with cloud-to-edge security. After that, we'll talk about the method that we recommend for System Security Manager, which is an attempt to provide system-level segregation of data processing components inside the device. This is done in an effort to confine the processing and storage of sensitive data to secure areas of the device. The following is a synopsis of the challenges that are being encountered by IoT designs:

- An increasing need for processing of data in real time.
- Crucial decisions were made with the help of AI and ML algorithms, which need high-quality data.
- A heightened awareness of privacy

concerns among customers.

- Costs associated with the utilization of bandwidth for cloud storage and user data.
- A desire to keep raw data safe.
- An increase in the processing power of devices that have been implanted.
- A focus on reducing information footprint while maintaining a high degree of information security at all architectural levels

Background

Computing technologies have seen significant shifts between centralized and decentralized control from the introduction of mainframes, which were followed by the development of personal computers and local area networks, and the more recent centralization of computer systems, which included transmitting control, data, and intelligence to the cloud. The usage of edge devices, which are often less powerful and give less control than a centralized platform, has largely been supplanted by the use of the cloud for substantial computing activities and centralized data processing owing to the cloud's enhanced flexibility, scalability, dependability, redundancy, and computational capacity. Edge devices are typically lower powered than a centralized platform. Additionally, it provides the service provider with increased control.

However, cloud-centric architectures have a variety of challenges, which is particularly problematic in light of the fact that aspects such as performance, power consumption, security, and privacy are becoming more important. Since several high-profile attacks have revealed severe security and privacy issues, relying on third-party providers for vital components of essential infrastructure is a serious problem that needs to be addressed. Spectre and Meltdown are two examples of common processor faults that have received a lot of attention in recent years. If any of these problems were exploited, it would be possible for an attacker to access the contents of a victim's memory. A scenario quite similar to this one arises when open source software components are employed, which gives adversaries direct access to the internal code. An especially important vulnerability is one that exists in open-source software and has the potential to be exploited on several different kinds of computers. Both the "Heart-bleed" attack on OpenSSL (CVE-2014-0160) and the "Dirty COW" vulnerability in the Linux kernel (CVE-2016-5195) are examples of occurrences that are well-known and often utilized. In a separate line of research, it has been shown that attacks against data while it is in transit as well as connections between computers may result in total denial-of-service attacks, communication delays, and privacy breaches. Cloud services have the danger of being vulnerable to further operational failures and social engineering attacks, both of which have the potential to expose huge quantities of data. Certain high-profile cloud breaches, such as the one that revealed 24 million credit and mortgage details, exposed Elasticsearch databases that had been left unencrypted and were left open to the public.

Before reaching the local edge devices and the sensors, actuators, and processors that they are linked to, Figure 1 provides an in-depth look at the physical cloud infrastructure, which consists of data centers and virtualized services, in addition to the network infrastructure for communications. The transformation of edge devices from data consumers to data producers enables a vast array of processing capabilities, such as signal processing, data collection, pattern recognition, real-time data analytics, and edge inference. These capabilities are made feasible as a result of the changing roles of edge devices, which formerly included human users as data consumers. Two of the most important elements that have contributed to this shift are the growth of embedded technology and the availability of several computer architectures, such as heterogeneous multi-core System-on-Chip (SoC). These designs make it possible to implement a wide variety of intelligent applications while still meeting the power footprints and form size requirements of the edge device. Additionally, they provide adaptability, flexibility, high performance processing, and communication capabilities. Unlike early edge devices, which simply gathered and delivered sensor data to the cloud for processing, modern edge devices do more than merely collect data. This method of creating enormous volumes of data from the real world at the edge, however, may stretch the capabilities of cloud computing due to restrictions on processing, storage, network bandwidth, and latency. This may result in problems with data aggregation as well as increased expenses.

Edge computing is a concept of decentralized and distributed computing in which most or all of the computation is carried out over a network of scattered nodes. Memory and processing capacity are going to be moved closer to the site of action in order to achieve the goal of allowing technology to interface with the actual world directly [26]. However, cloud computing will continue to play an important part in the future generation of edge computing. This function will be analogous to that of mainframes and personal computers in that it will provide a centralized point of access and complete data analytics. The advancement of computing capabilities at the edge of networks will provide the framework for a wide range of intelligent and smart technologies, with AI and ML inference serving as a guiding force in the process of decision-making. This will serve as the basis for a new generation of M2M communication, which will be the foundation for a broad range of new computing capabilities. This new generation of M2M communication will provide greater service availability, lowered response time, and reduced latency. By relocating computing closer to the edge of the network, communication bottlenecks may be avoided, and applications are given the capacity to continue working even in the event that they have occasional or defective network connection. Edge computing helps to improve data management by processing sensitive and secret data at the actual place of origination, which is known as the edge. This helps to keep such data more secure. Because of this, the only data that should be transported to the cloud are those that have been processed and anonymized.

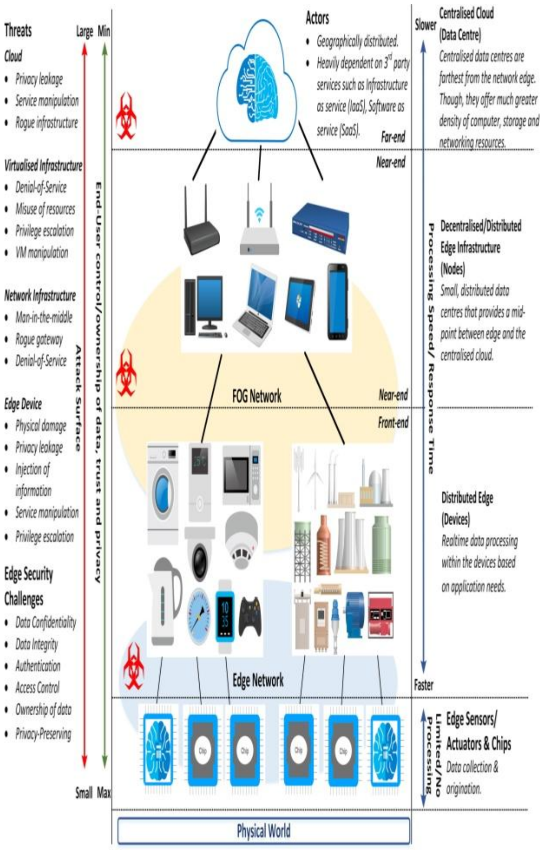
Threats
Cloud
Privacy leakage
Service manipulation
Rogue infrastructure
Virtualised Infrastructure
Denial-of-Service
Misuse of resources
Privilege escalation
VM manipulation
Network Infrastructure
Man-in-the-middle
Rogue gateway
Denial-of-Service
Edge Device
Physical damage
Privacy leakage
Injection of information
Service manipulation
Privilege escalation
Edge Security Challenges
Data Confidentiality
Data Integrity
Authentication
Access Control
Ownership of data
Privacy-Preserving
Large
Small
Min
Max
Attack Surface
End-User control/ownership of data, trust and privacy
Actors
Geographically distributed.
Heavily dependent on 3rd party services such as Infrastructure as service (IaaS), Software as service (SaaS).
Far-end
Near-end
FOG Network
Near-end
Front-end
Edge Network
Physical World
Slower
Faster
Processing Speed/ Response Time
Centralised Cloud (Data Centre)
Centralised data centres are farthest from the network edge. Though, they offer much greater density of computer, storage and networking resources.
Decentralised/Distributed Edge Infrastructure (Nodes)
Small, distributed data centres that provides a mid-point between edge and the centralised cloud.
Distributed Edge (Devices)
Realtime data processing within the devices based on application needs.
Edge Sensors/ Actuators & Chips
Data collection & origination.
Limited/No Processing
Chip

Fig. 1. An illustration of Cloud to Edge infrastructure capabilities, security threats and involved edge security challenges at each layer.

2. THE NEED FOR EMBEDDED RESILIENCE INNEXT-GENERATION EDGE TECHNOLOGIES

Localizing data processing does drastically reduce the attack surface area from which sensitive data can be attacked, but it should be noted that these edge devices are vulnerable to many of the same flaws that affect other aspects of the cloud service architecture, including those that were mentioned earlier. This is something that should be taken into consideration. Edge devices, on the other hand, are susceptible to new types of attacks, in part because attackers may get total physical access to these devices. In order to get further access to the device, it may be necessary to exploit certain features, such as boot modes, hidden debug ports, and side channel analysis. Concerns of primary importance with relation to the following embedded edge device security techniques are as follows:

The lack of an independent, active run-time security system that can recognize threats, harmful activity, and preserve critical data in the event that existing security measures are penetrated, therefore minimizing the chance of information exposure or the introduction of false data. This is because such a system would be able to identify threats, hostile conduct, and secure crucial data. Micro-architectural defenses that are ad hoc and passive may be provided by security designs. They were designed from the ground up to counteract certain assaults or vulnerabilities. The research literature has a number of examples demonstrating instances in which certain defensive systems were found to be vulnerable, subjected to attacks, and otherwise compromised. For example, there are extensions for memory protection to avoid memory overflow.

Authentication of the pointer, so that the integrity of the pointer may be maintained. The isolation or virtualization of logical resources to prevent information from leaking out via side channels.

Security methods based on the concept of a Chain-of-Trust to ensure the applications' completeness.The creation and maintenance of robust chain-of-trust systems are critical components of security architectures. This is built on several presumptions piled on top of one another, and the argument is only as robust as its most tenuous relationship. If the code is cracked, the integrity of the whole system's security is called into question. The lack of security standards and methods that suppliers may use to evaluate the safety of their own created hardware and software components both before and after integrating them into the system in order to guarantee a secure product development life-cycle.

A lack of security-aware design and development processes brought on by the reuse of hardware and software components sourced from third parties, which leads to the construction of unpredictable and insufficient solutions. This lack of security-aware design and development procedures causes a lack of security-aware design and development procedures. Vulnerabilities in both the hardware and the software may be the consequence of complicated co-designing of the hardware and the software, security modeling, and integration processes. These vulnerabilities allow an adversary to launch attacks.

In order to meet the security concerns described above, the underlying data that is handled and processed by the edge device, as well as the service inside which it is operating, need to be protected by security measures. In IoT systems that use edge processing to manage sensitive data, there is an essential need for an additional layer of data protection to be implemented prior to any processing taking place when handling sensitive data. The existing micro-architectural security measures will be enhanced by the layer that has been presented. This layer will also allow the detection and prevention of harmful activity before it can cause harm or major damage. Potentially useful for future edge devices that deal with sensitive data and rely on AI to establish their trustworthiness in complex M2M situations, this layer might be of tremendous assistance to such devices. This proposed layer would offer an independent, active run-time security mechanism that provides platform-level visibility of the underlying edge device. This would allow for the detection of threats and the protection of the M2M ecosystem.

3. CHARACTERISTICS OF ADAPTIVE SYSTEM-ON-CHIPPLATFORM

As has previously been shown, embedded micro-architectures do not provide any active approaches that may be used to create or maintain the security of a device after the device's trust has been breached. This may have an impact on the underlying system and the users of the system by making it possible for personal data to be accessed, edited, or deleted, often without leaving a trace.

Embedded Security Requirements for Next-Generation Edge Technologies

In light of the fact that the built-in defenses of embedded systems are often insufficient, security functionality should not be limited to protection alone. In order for the device to be able to maintain vital service operations, it must be able to recognize harmful cyber activities and attacks, put active countermeasures into action in reaction to those attacks, and then restore the system. The following is a list of critically important additional security services that are required to protect embedded edge microarchitectures:

Detection -the capability of autonomously monitoring important system resources and identifying activity patterns that signal manipulation or compromise of such resources.

Informing -This allows for the independent disclosure of sensitive data as well as the independent informing of components of the architecture that are responsible for decision-making.

Mitigation - This necessitates covert operations carried out by the embedded microarchitecture in order to mitigate the negative impacts of compromise. It's possible that this will include deleting sensitive data or turning off devices.

Recovery -When operating conditions are very precarious, having the ability to maintain core tasks like safety is absolutely essential. The ability to physically disable compromised device components makes it possible for the remaining components to operate securely.

Architectural Components to Secure Next-Generation Edge Technologies

Taking into account the derived security requirements of cyber resilient embedded systems, the following core micro-architectural elements are suggested in order to enable the establishment of ongoing device activities through the continuous monitoring of system resources and activities, as well as the keeping track of events in order to achieve system-level visibility:

An Independent Active Runtime System Security Manager, which is in charge of security functions such as protection, detection, response, and recovery while upgrading existing security mechanisms. This manager is responsible for the overall security of the system. It will continuously monitor system resources, use the data it obtains to determine whether or not the system is behaving appropriately, initiate active countermeasures in response to behaviors that are identified as being damaging to the system or particular resources, and bring the system back to a healthy state. In order for the System Security Manager to have access to the general-purpose CPU's memory resources, it is necessary for it to be physically isolated from and isolated from the general-purpose CPU. Because of the physical restrictions placed on the attack surface, the system will be far less susceptible to software flaws and attacks. This is in contrast to the TEE, which shares the same physical processor and memory resources as the general purpose processor. The necessity for visibility at the resource level and monitoring of the system's vital components was a need for the successful implementation of this system security manager, which led to the development of the second feature.

Active Runtime Resource Monitors, which are responsible for keeping a watch on resource-specific behaviors and searching for suspect behaviour in order to report it to the System Security Manager. These active runtime monitors are required because embedded systems are becoming more intricate and various capabilities are being merged into a single program. These capabilities frequently include the mixing of sensitive data with non-sensitive data and physical actuation. With the assistance of these active runtime monitors, which will offer information on a granular level that is particular to individual resources, the system security manager will be able to define, analyze, and evaluate system-level behaviors in addition to initiating the appropriate mitigation and recovery processes. In addition, the information obtained would be helpful in maintaining the data stream and would give essential data that could be used to provide evidence of any abnormal activity.

The mitigation and recovery demands of a cyber-resilient embedded system are implemented by an active response manager, who works under the command of the

System Security Manager. This involves beginning any active countermeasures that may be taken to decrease the risk that has been detected inside the system. Additionally, depending on the microarchitecture of the active runtime resource monitors, the active response manager could implement numerous system-level security measures, one of which being the ability to physically disconnect a compromised resource from the system. This would make it possible to maintain critically vital services in the next-generation of critical infrastructure while at the same time slowly diminishing the functionality of the system.

CONCLUSION

The performance of edge computing has substantially increased, which has opened up the prospect of carrying out complex processing locally as opposed to in the cloud, which is where it is now carried out. The limitations of cloud computing in terms of real-time performance and resource consumption, as well as issues over the regulation of data privacy, have all contributed to a rise in the chance that processing power would be transferred to edge devices. However, there would be issues with carrying out such a technique, particularly with respect to the safeguarding of sensitive information or with regard to operations that rely on acquiring accurate information. In light of the various worldwide data protection regulations, some of the many security requirements and problems have been examined in this research. Because of these challenges, embedded security criteria have been developed, which will ultimately lead to an improvement in the resilience of M2M systems. The essay claims that there is a compelling need for embedded cyber resilience as a result of the present lack of active detection, response, and recovery security capabilities that are included within existing embedded security systems. This is achieved by suggesting runtime monitoring and system-level visibility of resource activities, in addition to active response functions, which together enhance, maintain, and insure the secure working of intelligent technologies throughout the device's life cycle.

REFERENCES:

[1] P. Spark, “White Paper: The route to a trillion devices: The outlook for IoT investment to 2035,” ARM, Tech. Rep., 2017.

[2] V. Sharma et al., “Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A survey,” CoRR, 2019. [Online]. Available: http://arxiv.org/abs/1903.05362

[3] S. Ravi et al., “Security in Embedded Systems: Design Challenges,” ACM Trans. Embed. Comput. Syst., vol. 3, no. 3, pp. 461–491, Aug. 2004.

[4] N. Apthorpe et al., “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic,” CoRR, vol. abs/1708.05044, 2017. [Online]. Available: http://arxiv.org/abs/1708.05044

[5] D. N. Serpanos and A. G. Voyiatzis, “Security Challenges in Embedded Systems,” ACM Trans. Embed. Comput. Syst., vol. 12, no. 1s, pp. 66:1– 66:10, Mar. 2013.

[6] Council of European Union, “Council regulation (EU) no 2016/679,” 2016.

[7] Personal Information Protection Commission, Japan, “Amended act on the protection of personal information,” 2016. [Online].

Available: https://www.ppc.go.jp/files/pdf/Act on the Protection of Personal Information.pdf

[8] California Office of Legislative Counsel, "Assembly bill no. 375:"the california consumer privacy act of 2018"," 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill id=2017 20180AB375

[9] Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper," Tech. Rep., 2016. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

[10] Tom Bawden, "Global warming: Data centres to consume three times as much energy in next decade, experts warn," Tech. Rep., 2016. [Online]. Available: https://www.independent.co.uk/environment/global- warming-data-centres-to-consume-three-times-as-much-energy-in-next- decade-experts-warn-a6830086.html

[11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[12] P. Kocher et al., "Spectre Attacks: Exploiting Speculative Execution," CoRR, vol. abs/1801.01203, 2018. [Online]. Available: http://arxiv.org/abs/1801.01203

[13] M. Lipp et al., "Meltdown: Reading Kernel Memory from User Space," in 27th USENIX Security Symposium, USENIX Security, Aug. 2018, pp. 973–990. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/lipp

[14] Ghafoor, I. Jattala, S. Durrani, and C. M. Tahir, "Analysis of OpenSSL Heartbleed vulnerability for embedded systems," in Proc. IEEE Inter- national Multi Topic Conference 2014, Dec. 2014, pp. 314–319.

[15] J. Qiu, L. Gao, S. Ranjan, and A. Nucci, "Detecting bogus BGP route information: Going beyond prefix hijacking," in Proc. IEEE International Conference on Security and Privacy in Communications Networks and the Workshops, Sep. 2007, pp. 381–390.

[16] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," in Proc. IEEE Symposium on Security and Privacy (SP), May 2017, pp. 375–392.

[17] N. J. AlFardan and K. G. Paterson, "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols," in Proc. IEEE Symposium on Security and Privacy, SP, May 2013, pp. 526–540.

[18] L. H. Newman, "Microsoft Email Hack Shows the Lurking Danger of Customer Support," Wired, Tech. Rep., 2019. [Online]. Available: https://www.wired.com/story/microsoft-email-hack-outlook-hotmail-customer-support/

[19] D. Olenick, "24 million credit and mortgage records exposed on Elas- ticsearch database," SC Magazine, Tech. Rep., 2019. [Online]. Avail- able: https://www.scmagazine.com/home/s

ecurity-news/data-breach/24-million-credit-and-mortgage-records-exposed-on-elasticsearch-database/

[20] GSMA (Organisation), “Cellular m2m forecasts: Unlocking growth,” Tech. Rep., 2015. [Online]. Available: https://www.gsmaintelligence.com/research/?file=9c1e1fd ff6453869427581 85ceed941

[21] W. Wolf, A. A. Jerraya, and G. Martin, “Multiprocessor System-on-Chip (MPSoC) Technology,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 27, no. 10, pp. 1701–1713, Oct. 2008.

[22] S. Sarkar, S. Chatterjee, and S. Misra, “Assessment of the Suitability of Fog Computing in the Context of Internet of Things,” IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 46–59, Jan. 2018.

[23] W. Shi et al., “Edge Computing: Vision and Challenges,” IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, Oct. 2016.