ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 7, July 2023

Design and Development of a Model for Security Enhancement in Edge Computing

Highiperformanceifog and edge computing, along with high bandwidth connections

[1] Vikas Shukla, [2]Prof.(Dr.)Rekha Agarwal, [3]Prof.(Dr.)Rajesh Kumar Tyagi

[1] Student, P. hd(IT), Amity Institute of information technology, Noida, India
[2] IT department, Amity Institute of information technology, Noida, India
[3] CSE Department, Amity University Haryana, Amity Education Valley, Gurgaon, Haryana, India
[1]vikasshukla@amity.edu, [2]ragarwal@amity.edu, [3]rktyagi@ggn.amity.edu

Abstract— Edge computing, along with high bandwidth connections, has transformed how Internet-of-Things (IoT) service designs are now able to process increasing volumes of high-quality data from their surroundings. However, recently enacted international rules and increased consumeri awareness have intensified the need for data security, and businesses who fail to secure customer data now face severe financial and reputational consequences. This research recommends using edge and fog computing to manage sensitive user data and reduce the quantity of raw sensitive data that is accessible at various levels of the IoT architecture. However, such a technique is vulnerable to device-level attacks. A suggested System Security Manager is utilized to tackle this problem by continually monitoring system resources and making sure private data is restricted to just those components of the device that need it. Critical data may be segregated during an attack, and the system can be notified, protecting data confidentiality.

Index Terms— Edge Computing, Edge Security, Active Security, Embedded System, and Data Protection.

I. INTRODUCTION

The Internet iof Things (IoT) has the potential to greatly benefit society. The IoT is a system of interconnected devices, appliances, and materials that share data and resources. “Consumers and businesses alike may put these tools to work enhancing and optimizing processes across industries including healthcare, property management, iand critical iinfrastructure. Security, functionality, usability, dependability, and affordability are just few of the areas that may benefit from these tools and services making use of supplied or inferred user and environmental data. Artificial Intelligence (AI), machine learning (ML), and data analytics may help firms make more informed decisions, provide superior service to customers, and identify untapped market niches. One trillion Internet of Things devicesi are expected to be in use by 2035 [1]. While sharing data across IoT devicesi opens up new avenues of exploration and potential, it also poses security and privacyi risks [2]. When dealing with sensitive data or critical infrastructure, there are several challenges that must be overcome before intelligentidevices and relatediservices can be integrated and deployed on a broad scale. These include design,isupply-chain, privacy, security, and safety. The way that most IoT services are now built makes them vulnerable to attacks and operational vulnerabilities that, if exploited, might lead to significant data loss. Organizations will almost certainly break the EU's General Data Protection Regulationi (GDPR), Japan's Act ion the Protection of Personal Information (APPI), California's Consumer Privacy Act (CCPA), and other foreign data management regulations [7], [8], and [9]. Artificial intelligence (AI) powered, data-driven decision-making systems may be hindered by fraudulent data manipulation, which might have catastrophic consequences. The need for networks, cloud storage, and processing has grown along with the proliferation of devices that may generate data. By 2021, it is expected that 847 Zettabytes (ZB) of data will be produced and transferred worldwide through the Internet of Things, up from 216 ZB in 2016 [10]. Data centers, the backbone of cloud computing, were anticipated to require 416 iterawatt-hours (TWh) of power in 2016, and by 2025, that amount is projected to treble [11]. The adoption of edge-based computing and other optimum techniques for data processing and storage are required since such consumption increase has been deemed unsustainable. Edge computing, when implemented correctly, may reduce workloads on the cloud that deal with a lot of extraneous personal idata while ialso offering low latency results that usei less inetwork bandwidth, all while preserving a crucial component of the basic architecture of IoT service design. In this article, the current status of Cloud to Edge security challenges will be examined from an architectural and infrastructure perspective. Using our suggested System Security Manager approach, which attempts to offer system-level isolation of data processing components within the device, the processing and storage of sensitive data is thus restricted to secure regions of the device. The issuesi IoT designs are running with are listed below:

- Growing need for real-time data processing.
- The use of AI/ML techniques to make crucial judgments that call for high quality data.
- Privacy iawareness among consumers.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 7, July 2023

• Prices for cloud and consumer data use in terms of bandwidth.
• A desire to keep raw data secure.
• An increasei in embedded devices' processingi power.
• Security concerns at all architectural levels - the need to minimize the information footprint.

The following is a summary of the study's key contributions:

• Moving away from cloud-centric architectures and toward dispersed, edge-based processing of data is advocated for IoT services in order to meet security requirements and limit the amount of sensitive data handled and transported over the cloud. By decreasing the iattack surface area ifrom which personal data may be compromised, such a tweak would increase user trust in next-generation IoT services.
• Specifying active micro-architectural traits to protect upcoming edge computing technologies. These ifeatures will make it easier to monitor vital system iresources in real time for imalicious or unusual behaviors and to take active mitigation measures to protect the iedge device iand any sensitive information it may contain.
• The recommended iarchitectural characteristics provide cloud-based computing paradigms with strong security foundations, ensuring the iconfidentiality and integrity iof data created by the edge device.
[1]

II. BACKGROUND

There have ibeen significant ishifts between icentralised and decentralised control of computing technologies over the years [12]. These shifts began with the introduction of mainframes and have continued with the introduction of personal computers, local networks, and most recently the movement of control, data, and iintelligence of computer systems to the cloud. In contrast to the cloud, which is typically used for large-scale computing and centralised data processing, edge devices are typically smaller, less powerful, and offer less control.. This is due to the cloud's enhanced flexibility, scalability, dependability, computational capacity, and ability to give the service provider more control. However, there are a number of difficulties with cloud-centric designs, especially now that performance, power consumption, security, and privacy are becoming more and more crucial factors. Dependence on third-party providers for essential infrastructure components is a serious problem because several high-profile assaults have exposed substantial security and privacy flaws. Examples of recent, widely publicised common processor flaws include Spectre and Meltdown, which, if exploited, might provide an attacker access to the contents of a victim's memory [13], [14]. Use of openisource software components creates a comparable vulnerability since it provides adversaries with unfettered access to the system's source code. Exploiting a flaw in open-source software may be lucrative if the flaw could be used in several environments. Two prominent examples are the Heartbleed exploit in OpenSSL (CVE-2014-0160) [15] and the Dirty COW flaw in the Linux kernel (CVE-2016-5195) [16]. Separate research shows that assaults on communication networks and data in transit may cause communication delays, privacy breaches, and even denials of service [17, 18], [19]. Common human error and social engineering attacks on cloud services may potentially expose sensitive information [20]. Some well-known cloud hacks, such as thei leak of 24 imillion credit iand mortgage records [21], exposed unprotected Elasticsearch databases. In Figure 1, we see the physical cloud architecture, including data centres and virtualized services, as well as the network infrastructure used for communications, all the way down to the locali edge devices and the associated isensors, actuators, and central iprocessing units. Maybe efficiency and safety are being thought about as well. Many of the applications and technology that will comprise the next generation of intelligence won't focus on humans at all. Machine-to-machine (M2M) communication is expected to increase dramatically [22], which will generate more important data at the network's periphery rather than in the cloud. This shift from edge devices from data consumers to data producers paves the way for a wide irange of processing icapabilities, such ias signal processing, data collection, pattern recognition, ireal-time data ianalytics, and iedge inference [23]. This ishift is influenced iby a number iof variables, including ithe growth iof embedded itechnologies and the availability of idifferent computer iarchitectures like the heterogeneous imulti-core System-on-Chip (SoC). These designs tackle power footprints and form ifactors on the edge device, allowing for ihigh levels of iadaptability, flexibility, high-performance icomputation, and iconnection to irealise a wide range of iintelligent applications. Unlike early edge devices, which only gathered and relayed sensor data to the cloud for processing. This method of creating massive volumes of data from the actual world at the edge may exert a strain on cloud computing capabilities, resulting in challenges with data aggregation and increased ipricing [25]. Computing at the network's periphery, or ‘edge,’ is performed by several, geographically scattered nodes. Bringing processing and storage capacity closer to the point of use paves the way for ireal-time data exchange between devices and the digital world [26]. Next-generation edge computing relies heavily on cloud computing for centralised access and advanced data analytics, much as traditional computing platforms such as mainframes and personal computers rely on the cloud. Since AI and ML inference are used to guide decision-making, the advancement of edge computing capabilities will pave the way for a wide range of intelligent and smart technologies. The next igeneration of machine-to-machinei (M2M) communication will be able to provide greater iservice availability, quicker reaction times, and lower latency, allowing for a wide range of novel computational capabilities. By relocating compute resources

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 7, July 2023

closer to the network's periphery, communication bottlenecks may be alleviated and applications can continue to function in spite of intermittent or poor network connection [27]. Edge computing also encourages better management of sensitive and secret data by iprocessing it closer to its ipoint of origin," at the iedge. Then, only information that has been converted and anonymised has to be sent to the cloud.

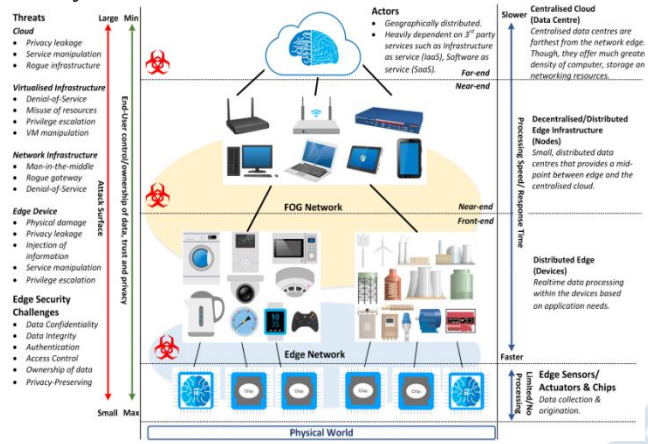

Figure 1. Cloud-to-Edge infrastructure capabilities, security risks, and edge security concerns at each tier

III. EMBEDDED RESILIENCE IN NEXT-GENERATION EDGE TECHNOLOGIES IS REQUIRED

Aspects including boot modes, secret debug ports, and side-channel analysis can be utilized to get further access to the device [28]. Key concerns with regard to embedded edge device security methods include the following:

- Lack of a run-time security system that is autonomous, active, and capable of detecting threats and malicious behavior in order to safeguard sensitive data in the event that existing security measures are breached and minimize the risk of information exposure or the introduction of fake data.
- Security designs provide ad hoc, passive micro-architectural defence methods. They were created to specifically combat certain attacks or weaknesses. Examples of times when these defence systems have been discovered to be weak, under assault, and compromised have been documented in open literature. For instance, pointer authentication to assure pointer integrity, memory protection extensions to guard against memory overflow. - Logical resource isolation or virtualization to stop information leaking through side channels. - Chain-of-Trust security measures to protect the apps' integrity
- Strong chain-of-trust construction & maintenance are essential to security architectures. This is made up of several stacked assumptions and is only as strong as its weakest connection. The security of the entire system is jeopardized if it is hacked.
- Lack of a run-time security system that is autonomous, active, and capable of detecting threats and malicious behaviour in order to safeguard sensitive data in the event that current security measures are breached and minimize the risk of information exposure or the introduction of fake data.
- Reusing third-party hardware and software components leads to insecure design and development practices, which in turn yields unreliable and fragile solutions.
- Vulnerabilities in hardware and software that allow an attacker to launch attacks might arise from intricate hardware-software co-design, security modelling, and integration processes.

The security challenges mentioned above can only be overcome by protecting both the service that the edge device is running in and the iunderlying data handled iand processed iby the device. An extra layer of defense is essential, especially with IoT systems that use edge processing to deal with sensitive data. The proposed layer would provide an additional layer of security on top of the existing micro-architectural protections, allowing for the early detection and mitigation of malicious attacks before they cause severe damage to the system. To overcome these security issues, it is necessary to protect both the service in which the edge device is operating and the underlying data that is being handled and iprocessed by the idevice. The need for an extra layer of defense prior to processing sensitive data is especially pressing in IoT systems that use edge processing to deal with such data.
[2]

IV. CHARACTERISTICS OF ADAPTIVE SYSTEM-ON-CHIP PLATFORM

As already established, embedded micro-architectures lack any active techniques for establishing or maintaining a device's security once its trust has been violated. This might affect the iunderlying system and its users by allowing personal data to be exposed or modified, frequently without leaving a trace.

4.1. Embedded Security Requirements for Next-Generation Edge Technologies

I. Given the weaknesses of embedded systems' built-in defences, security functionality shouldn't be restricted to only protection. In order to preserve essential service functions, the device must be able to recognize harmful cyber activity and assaults, react by putting in place active countermeasures, and restore the system. "Important additional security features needed to protect embedded edge microarchitectures include the following actions:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 7, July 2023

II. Detection - The ability to continuously watch over important system resources and spot patterns of behaviour that point to manipulation or compromise.

III. Informing - This enables the independent disclosure of possibly inaccurate data or the exposure of sensitive data to decision-making parts of the architecture.

IV. Mitigation - This entails evasive action by the embedded microarchitecture to lessen the effects of compromise. Sensitive data erasure or device disablement may be part of this.

V. Recovery - In the event of critical operating events, it is crucial to be able to retain core functionality, such as safety. Secure functioning of the remaining components is made ipossible by the iability to physically disable compromised portions of the device.

4.2. Architectural Components to Secure Next-Generation Edge Technologies

To make it possible to create ongoing device operations by continuously tracking system resources and activities, achieving system-level visibility via event tracking, and taking into account the inferred security requirements of cyber resilient embedded systems.

I. A separate active runtime system security manager, tasked with enhancing current security measures while performing protection, detection, response, and recovery security responsibilities. It is required to continually monitor system resources, use the data acquired to identify good or bad system behaviour, apply active countermeasures in response to any discovered harmful (system or resource-specific) actions, and restore the system to a healthy condition. System Security Manager must be physically separate from and segregated from the general-purpose CPU in order for it to have access to its memory resources. Due to the physical limitation of the attack surface compared to the TEE, iwhich shares the isame physical processor and imemory resources as ithe general purpose processor, the system will be far less susceptible to software faults and attacks. For the system security manager to be implemented effectively, resource-level ivisibility and monitoring iof key isystem components are inecessary. This ileads to the second feature.

II. Active iRuntime Resource iMonitors to track resource-specific ibehaviours and look for suspicious activity; these monitors then report that activity to the System iSecurity Manager. These active iruntime monitors are iessential as embedded systems get more icomplex, with multiple capabilities packed into a single programme, usually including the imixing of sensitive idata with non-sensitive idata and physical iactuation. With the iaid of these iactive runtime monitors, which will provide ifine-grained resource-specific information, ithe system security manager will be able to recognise, analyse, and ievaluate system-level ibehaviours as well as iinitiate the required mitigation and irecovery procedures. Additionally, the information acquired would help maintain the data stream iand provide crucial idata for establishing proof of any aberrant behaviour.

III. An active response manager, working under the guidance of the system security manager, implements the mitigation and recovery requirements for a cyber resilient embedded system. In order to lessen the danger that has been recognised inside the system, active countermeasures must be initiated. In addition, depending on the microarchitecture of the active runtime resource monitors, the active response manager may enforce a number of system-level security measures, where a compromised resource can be physically isolated from the system. In the next generation of critical infrastructure, this would provide opportunities to maintain essential services while gradually diminishing the system's functionality. A detailed SoC platform design [29], [30], and security modeling approach [31] have been used to realize the given features and embedded security requirements.

V. CONCLUSION

The performance of edge computing has significantly improved, opening up the possibility of performing complicated processing locally rather than in the cloud, where it is now done. The constraints of real-time performance and resource consumption in cloud computing, as well as data privacy regulation concerns, have all increased the likelihood of transferring processing power to edge devices. But there would be problems with such a procedure, especially with regards to the protection of sensitive information or with procedures that depend on getting accurate linformation." Some of the isecurity needs and issues have been discussed in this study in ilight of international idata protection laws. These difficulties have led to the development of embedded security requirements that will increase the robustness of M2M systems. Due to a presentilack of active detection, response, and recovery security capabilities within existing embedded security systems, the research argues a strong necessity for embedded cyber resilience. This is done by suggesting runtime monitoring and system-level visibility of resource operations," coupled with active response features to enhance, maintain, and ensure secure functioning of

intelligent technologies over 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. [Online]. Available: https://community.arm.com/iot/b/blog/posts/white-paper-thero ute-to-a-trillion-devices

[2] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in Proc. IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), March 2011, pp. 1–6.

[3] 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

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

[5] 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

[6] 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.

[7] Council of European Union, "Council regulation (EU) no 2016/679," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] 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 Inf ormation.pdf

[9] 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?b ill id=2017 20180AB375

[10] 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/servicepro vider/global-cloud-index-gci/white-paper-c11-738085.html

[11] 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/globalwarming-data-centres-to-consume-three-times-as-much-energy-in-next decade-experts-warn-a6830086.html

[12] 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.

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

[14] 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/present ation/lipp

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

[16] A. P. Saleel, M. Nazeer, and B. D. Beheshti, "Linux kernel os local root exploit," in 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), May 2017, pp. 1–5.

[17] 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.

[18] 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.

[19] 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.

[20] 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-outlookh otmail-customer-support/

[21] D. Olenick, "24 million credit and mortgage records exposed on Elasticsearch database," SC Magazine, Tech. Rep., 2019. [Online]. Available: https://www.scmagazine.com/home/security-news/data-breac h/24-million-credit-and-mortgage-records-exposed-on-elasticsearc h-database/

[22] GSMA (Organisation), "Cellular m2m forecasts: Unlocking growth," Tech. Rep., 2015. [Online]. Available: https://www.gsmaintelligence.com/research/?file=9c1e1fd ff645386942758185ceed941

[23] A. Al-Fuqaha et al., "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[24] 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.

[25] 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.

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

[27] G. Lewis et al., "Tactical Cloudlets: Moving Cloud Computing to the Edge," in Proc. IEEE Military Communications Conference, Oct. 2014, pp. 1440–1446.

[28] A. Kliarsky, "Detecting Attacks Against The Internet of Things," SANS Institute, Tech. Rep., 2019. [Online]. Available: https://www.scmagazine.com/home/security-news/data-breac h/24-

million-credit-and-mortgage-records-exposed-on-elastic search-database/

[29] F. Siddiqui, M. Hagan, and S. Sezer, "Embedded policing and policy enforcement approach for future secure IoT technologies," in Living in the Internet of Things: Cybersecurity of the IoT - 2018, Mar. 2018, pp. 1–10.

[30] F. Siddiqui, M. Hagan, and S. Sezer, "Pro-Active Policing and Policy Enforcement Architecture for Securing MPSoCs," in 2018 31st IEEE International System-on-Chip Conference (SOCC), Sep. 2018, pp. 140– 145.

[31] M. Hagan, F. Siddiqui, and S. Sezer, "Policy-Based Security Modelling and Enforcement Approach for Emerging Embedded Architectures," in 31st IEEE International System-on-Chip Conference (SOCC), Sep. 2018, pp. 84–89.