Advanced Encryption Standard based Secure IoT Data Transfer Model for Cloud Analytics Applications

Dinesh Kumar Anguraj
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Koneru Lakshmaiah (KL) University, Vaddeswaram, A.P, India

E-mail: adinesh@kluniversity.in

Abstract

The data surge caused by the increase in the use of IoT devices in our day-to-day activities requires careful storage and maintenance systems to ensure the protection and integrity of private information. Users are provided with prospects to use rule-based programs and services that can be interconnected with their devices thereby enabling automation in the prodigious IoT ecosystem. The sensitive IoT data is generally stored and processed in cloud services. This data may be vulnerable to several threats. It is crucial to protect rule-based programs and sensitive IoT information against cyberattacks. The rule-based program and IoT data integrity and confidentiality can be maintained with the help of the framework proposed in this work. An end-to-end data encryption model based on advanced encryption standard and Intel SGX are used to design the framework of the data privacy preservation model. Real as well as simulated IoT device data are used for securely executing the rule-based programs in the SGX to evaluate the proposed framework.

Keywords: IoT, data privacy, Intel SGX, advanced encryption standard, cloud analytics, rule-based IoT platform

1. Introduction

The way in which data is disseminated and shared all over the world is revolutionized with the evolution of Internet technology [1]. Seamless integration of things and digital devices is made possible with the inter-disciplinary advances and the introduction of the Internet of Things (IoT). Simply put, anything on earth can be integrated with the help of IoT [2]. Currently, IoT applications involve precision agriculture, smart transportation, smart home and smart cities. All domains and fields are affected by the introduction of IoT

DOI: https://doi.org/10.36548/jitdw.2022.2.006
Received: 10.05.2022, received in revised form: 26.06.2022, accepted: 10.07.2022, published: 20.07.2022

technology [3]. Real-time health monitoring is achieved with the dominant IoT sensor networks used in the healthcare industry. Data transfer with IoT has several associated security challenges. These challenges are broadly categorized into technical, organizational and methodological [4]. The technical category involves the comprehension of IoT architecture, data security, resource constraints, physical constraints, distributed systems and data flow. The organizational category involves third-party components, security, goals, standards, policies, human factors and other social engineering-related parameters [5]. The methodological category involves the security assurance mechanism, security controls prioritization, run time security and process model security.

In terms of interoperability, data-centric networking, standards, and security, the IoT-based developments are insufficient according to certain researchers [6]. Various aspects of IoT security are ensured by overcoming the privacy and security challenges and strengthening the IoT frameworks. Due to its heavy weight mechanism, IoT devices cannot use the conventional RSA (Rivest-Shamir-Adleman) algorithm [7]. ECDH, DH and other such lightweight key exchange protocols are vulnerable to attacks such as Man in the middle (MITM) and replay. Huge amounts of data can be mined, analyzed, processed and collected using cloud-based services with the advancement of cloud computing technology. This technology consumes lesser time and is cost-effective [8]. During data transmission and computation, the cloud service providers are exposed to several security threats despite ensuring data protection at rest. Public cloud services are often exposed to data breaches.

In this work, the IoT data is securely stored and processed with the help of Trusted Execution Environments (TEEs) and appropriate cryptographic techniques for privacy preservation [9]. Confidentiality and integrity of vulnerable automation policies, private user information and sensitive IoT data are ensured by the proposed framework [11]. This framework is empirically evaluated for its performance on the Intel Software Guard Extensions (SGX) TEE using rule-based analytics in the untrusted cloud. The data and code is stored safely and executed in an isolated secure memory container created by the Intel SGX [12].

The contents of SGX cannot be accessed by a virtual machine manager (VMM) or any operating system (OS) and other such higher privileged software or adversaries. The user information and delicate IoT data are stored in an encrypted format by the proposed framework [13]. Within the region, the IoT devices and their rule-based interactions are executed in a secure manner such that the information cannot be manipulated or stolen by

attackers. A robust end-to-end encryption method is followed to ensure safe data transfer to the cloud service provider from the IoT device with the SGX. Other than when in the SGX, the data in transit is always in an encrypted format.

2. Literature Review

Due to the diversified technology of Original Equipment Manufacturers (OEMs) involved, security in IoT systems is non-trivial. IoT security is analyzed systematically using the technique proposed by the authors in [14]. Several vulnerabilities are observed in each domain that is integrated with the IoT systems. These vulnerabilities are caused by several reasons such as diversified technology amalgamation and lack of security standards. The distributed ledger solutions are used for integrating blockchain technology with IoT systems [15].

IOTA, Hyper Ledger Fabric, and Ethereum are some of the technologies associated with IoT. High importance is given to end-to-end communication as several devices are connected in user-centric IoT that offers Machine to Machine (M2M) communications. Device attack, application attack, network attack, web interface attack, data integrity attack and several such cyber-attacks may occur while referring to the M2M phenomenon [16]. Without human intervention, the devices can be used for automating processes using IoT technology. Low cost, high accuracy and more operations are some of the conveniences offered by IoT automation [17].

The IoT devices interact with the physical environment with the help of embedded actuators and sensors. The physical states, also called events are collected by the sensors. Door lock state, dust level, temperature reading and so on are some examples of events [18]. These events are transferred and processed further at the hub or cloud. The device actuators receive appropriate action commands based on the event data and user-defined protocols [19]. Appropriate protocol supporting the limitations of the low-powered devices are used for transferring data between the hub or cloud and the IoT devices. OpenHAB 9, Zapier 8, Apple's HomeKit 7, IFTTT, Samsung's SmartThings etc. are some of the IoT programming platforms that are currently available [20]. These platforms can be used for several app-specific services such as device interactions, data collection, and managing and controlling devices. Various APIs can be used by the developers to perform automation and write applications using these tools.

3. Proposed System

3.1 Problem Formulation

There are three types of information which is passed between the user and the provider namely activity data (use of user interaction or automation rules to obtain information on device usage), sensor data (physical state information from sensors) and stored data (activity logs, user identifiers and device identifiers). This information is shared with the third party and the first party.

- The third party represents the organizations like analytics and cloud providers which give computing resources.
- The first party represents the companies that manufacture IoT devices used to enable the functionality of the devices.

Hence these parties have access to the data used in the IoT devices, thereby proving to be a potential data privacy issue. This has resulted in the need for a way to balance trust in these service providers. Though there are confidentiality agreements with the cloud service providers there are many security threats that the data is exposed to including breaches of public cloud service. Moreover, improper encryption methodologies will lead to important and sensitive data to be exposed.

3.2 Secure IoT platform

In this proposed work, an end-to-end encrypted data analytics platform based on advanced encryption standard which is specifically developed for an IoT environment is designed with a highly secure cloud server. With the help of trust, execution in environments and appropriate cryptographic techniques, the privacy issues and data security threats are addressed in this proposed work. Rule-based secure IoT platform is particularly focused on smart home automation in areas of untrusted cloud. In IoT automation, a rule-based trigger-action platform is used that balances the ubiquitousness and connectivity of the IoT devices. Company-owned data silos or untrusted cloud platforms are used to process and store these rules resulting in a major threat to the privacy and security of the users. With the help of enclave features present in SGX the delicate IoT data is secured such that it is not possible for any third party or breached to unlawfully access the data.

In general, an untrusted cloud platform used by the cloud provider will initialize the SGX enclave instance. Or initialization the enclave will authenticate itself and locate in a

remote application server using software attestation process. Here the enclave is now entrusted with certain specific sensitive information such as description and encryption keys using a secure communication channel. The IoT devices interact with the enclave via hubs or IoT gateways with HTTPS connection, which is encrypted with transport layer security (TLS). Moreover asymmetric key encryption is also used to establish end-to-end the secure system between the IoT hub and the cloud. Advanced Encryption Standard (AES) is one of the most widely used and popular key encryption methodologies. Hence the data transmitted is done so in a safe manner without any possibility of eavesdropping.

The SmartThings JSON rule structure is adopted in this proposed work. The smart devices are initially registered for this purpose thereby paving way to rule definition to automate the devices. In general a list of actions and list of conditions for trigger are placed in the rule. This will enable two types of data. The first data is the information received from smart devices with specification of the device elements received which catapult the rule. This includes sensor reading of the device or state of the device. The other data is that of action corresponding to a particular rule. This is nothing but the set of commands transmitted to the devices to activate or control them based on the triggering condition. Algorithm one represents a typical JSON format.

Algorithm 1: JSON format

```
{
"name": "Is the user home? If yes, turn on the lights and set the thermostate mode
,→ to cool",
"ruleID": "CmhdyUnheisKjah-75dkgiBHhmoiushGHYPOJ",
"userID": "AhysUh981ryGnduOe-23jpqmeJnnsogeuJHEPQ",
"actions": [
{
"if":{
"equals": {
"left": {
"device": {
"devices": ["850AG7TE-8496-5FD8-365D82567"],
```

"component": "main",

"capability": "PresenceSensor",

"attribute": "yes"

}

},

"right": {

"string": "present"

}

},

"then": [

{

"command": {

"devices": ["2584695-257Z-3IF8-TY9QW45A"],

"commands": [

{

"component": "main",

"capability": "Mode of Thermostat",

"command": "cool",

"arguments": []

}

]

}

},

],

"else": []

}

}

]

}

The rules formulated are encrypted and then transmitted to the untrusted cloud enclave. Using our methodology the encrypted data which is stored in the database is secure and can be decrypted within the SGX enclave only. This technique prevents manipulation and access of information by attackers. The procedure of the proposed protocol is as follows:

- The sensor values and device states are sent to the cloud using gateways or hubs by the IoT devices.
- Before transmitting, the information is encrypted at the gateway or hub.
- When streaming the data, the associated rule is decrypted by the SGX.
- MQTT (Message Queuing Telemetry Transport) is used as the connectivity protocol to transmit messages with multiple data streams from different devices.
- The condition of the rule is compared with the device event and accordingly, a response is generated.
- Further, the command-action sequence is encrypted and also transmitted to the right gateway or hub.

4. Result and Discussion

There are three test cases considered for this experiment namely with SGX which ensures total security guarantee, without SGX and without SGX encryption to ensure data integrity as shown in Fig.1. A comparison is drawn for the execution time recorded for the 2500 simulated device events.

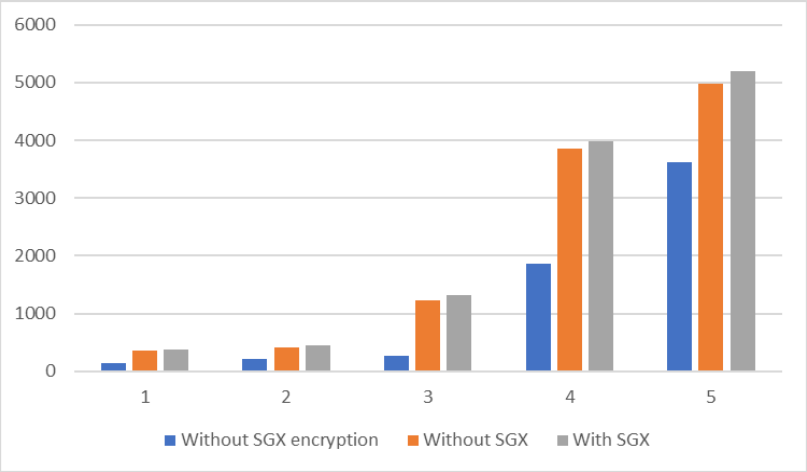

Figure 1. Execution time for 2500 device events based on three scenarios: with SGX, without SGX and without SGX encryption

Table 1. Experimental Setup

Case	Type	Ruleset	No. of Devices	Cache size
SGX SGX (w/o encryption) No SGX	Simulation	2500	46	200
		2000		
		1500		
		1000		
		500		
	Real	10		

The observation is made for several number of rules and the corresponding readings are tabulated in Table.1. Similarly, the no. of bits used for the key size will also increase with respect to the type of methodology incorporated as shown in Fig.2.

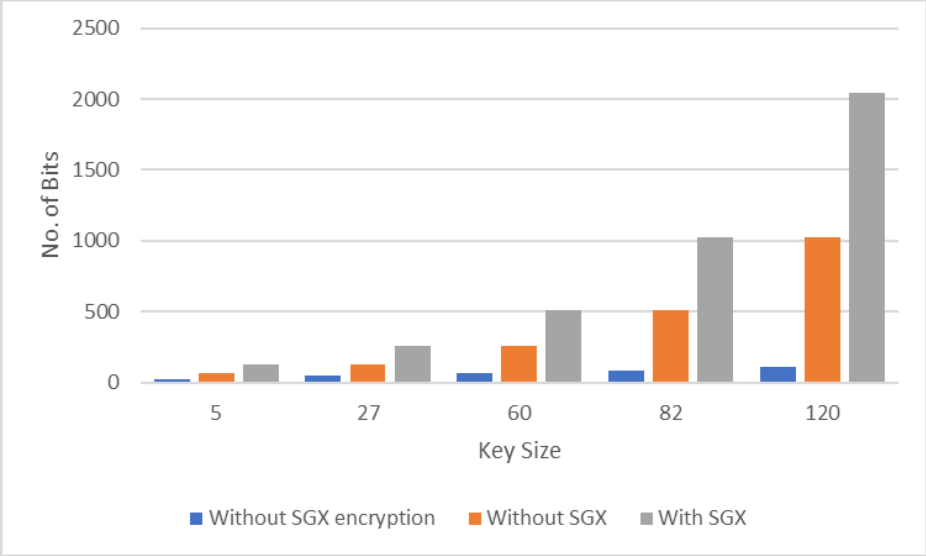

Figure 2. No. of Bits Vs. Key size

5. Conclusion and Future Scope

It is crucial to protect the automation policy rules and sensitive user data from malicious attacks with the increase in the use of IoT devices. Strong cryptographic techniques and the Intel SGX are leveraged to provide a secure data analytic framework in this paper. Confidentiality, data integrity and user privacy are ensured by means of automation in the

SGX region using the basic trigger-action rule-based program execution. During data storage and transmission, data privacy is guaranteed by a strong encryption mechanism. This ensures the end-to-end encryption of the system. Data from real and simulated IoT devices are used for evaluating the performance of the proposed framework. In a secure SGX enclave, rule-based decision-making is performed. The results show that the SGX-based processing and encryption do not result in significant overhead despite offering improved data security.

References

[1] Ahmed, Q. W., & Garg, S. (2019, December). A Cloud computing-based Advanced Encryption Standard. In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 205-210). IEEE.

[2] Duraipandian, M., & Vinothkanna, R. (2019). Cloud based Internet of Things for smart connected objects. Journal of ISMAC, 1(02), 111-119.

[3] Alabdulatif, A. (2021). Practical hybrid confidentiality-based analytics framework with Intel SGX. Journal of Systems and Software, 181, 111045.

[4] Wang, H. (2020). IoT based clinical sensor data management and transfer using blockchain technology. Journal of ISMAC, 2(03), 154-159.

[5] Anajemba, J. H., Iwendi, C., Mittal, M., & Yue, T. (2020, April). Improved advance encryption standard with a privacy database structure for IoT nodes. In 2020 IEEE 9th international conference on communication systems and network technologies (CSNT) (pp. 201-206). IEEE.

[6] Shakya, S. (2021). IoT based F-RAN architecture using cloud and edge detection system. Journal of ISMAC, 3(01), 31-39.

[7] Ahamed, J., Zahid, M., Omar, M., & Ahmad, K. (2019). AES and MQTT based security system in the internet of things. Journal of Discrete Mathematical Sciences and Cryptography, 22(8), 1589-1598.

[8] Kirubakaran, S. S. (2020). Study of Security Mechanisms to Create a Secure Cloud in a Virtual Environment with the Support of Cloud Service Providers. Journal of trends in Computer Science and Smart technology (TCSST), 2(03), 148-154.

[9] Alabdulatif, A. (2020, September). Secure Data Analytics for IoT Cloud-enabled Framework Using Intel SGX. In 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (pp. 54-57). IEEE.

[10] Madhura, S. (2021). IoT based monitoring and control system using sensors. Journal of IoT in Social, Mobile, Analytics, and Cloud, 3(2), 111-120.

[11] Hidayat, T., & Mahardiko, R. (2020). A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. International Journal of Artificial Intelligence Research, 4(1), 49-57.

[12] Smys, S., & Raj, J. S. (2019). Internet of things and big data analytics for health care with cloud computing. Journal of Information Technology, 1(01), 9-18.

[13] Pawar, A. B., & Ghumbre, S. (2016, December). A survey on IoT applications, security challenges and counter measures. In 2016 international conference on computing, analytics and security trends (CAST) (pp. 294-299). IEEE.

[14] Sivaganesan, D. (2019). Design and development ai-enabled edge computing for intelligent-iot applications. Journal of trends in Computer Science and Smart technology (TCSST), 1(02), 84-94.

[15] Sood, S. K. (2020). Mobile fog based secure cloud-IoT framework for enterprise multimedia security. Multimedia Tools and Applications, 79(15), 10717-10732.

[16] Smys, S., Basar, A., & Wang, H. (2020). CNN based flood management system with IoT sensors and cloud data. Journal of Artificial Intelligence, 2(04), 194-200.

[17] Kocabaş, Ö., & Soyata, T. (2016). Medical data analytics in the cloud using homomorphic encryption. In E-Health and Telemedicine: Concepts, Methodologies, Tools, and Applications (pp. 751-768). IGI Global.

[18] Bestak, R., & Smys, S. (2019). Big data analytics for smart cloud-fog based applications. Journal of trends in Computer Science and Smart technology (TCSST), 1(02), 74-83.

[19] Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications, 80(14), 21165-21202.

[20] Bashar, A. (2020). Sensor cloud based architecture with efficient data computation and security implantation for Internet of Things application. Journal of ISMAC, 2(02), 96-105.

Author's biography

Dinesh Kumar Anguraj is currently working as Associate Professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Andhra

Pradesh, India. He received his Doctor of Philosophy in Information and Communication Engineering from Anna University, Tamil Nadu in 2018 and received his Master of Engineering in Computer Science and Engineering from Karpagam University, Tamil Nadu in 2013. His research interest includes Wireless Sensor Network, Body Area Network and Network Security. He is served as a reviewer for various International Journals.