A Secure and Verifiable Outsourced Access management in Fog-Cloud Computing

Komala G [1], Assistant Professor
Christu Jyothi Institute of Technology & Science, Jangaon
A.Poorna Chandra Reddy [2], Assistant Professor
Christu Jyothi Institute of Technology & Science, Jangaon

ABSTRACT:

Abstract

In this paper, we propose a framework for hybrid privacy-preserving clinical decision support system in fog–cloud computing, called HPCS. In HPCS, a fog server uses a lightweight data mining method to securely monitor patients' health condition in real-time. The newly detected abnormal symptoms can be further sent to the cloud server for high-accuracy prediction in a privacy-preserving way. Specifically, for the fog servers, we design a new secure outsourced inner-product protocol for achieving secure lightweight single-layer neural network. Also, a privacy-preserving piecewise polynomial calculation protocol allows cloud server to securely perform any activation functions in multiple-layer neural network. Moreover, to solve the computation overflow problem, a new protocol called privacy-preserving fraction approximation protocol is designed. We then prove that the HPCS achieves the goal of patient health status monitoring without privacy leakage to unauthorized parties by balancing real-time and high-accurate prediction using simulations.

I.Introduction

Smart sensor-equipped mobile devices sense, collect, and process data generated by the edge network to achieve intelligent control, but such mobile devices usually have limited storage and computing resources. Mobile cloud storage provides a promising solution owing to its rich storage resources, great accessibility, and low cost. But it also brings a risk of information leakage. The encryption of sensitive data is the basic step to resist the risk. However, deploying a high complexity encryption and decryption algorithm on mobile devices will greatly increase the burden of terminal operation and the difficulty to implement the necessary privacy protection algorithm. PasteSmart sensor-equipped mobile devices sense, collect, and process data generated by the edge network to achieve intelligent control, but such mobile devices usually have limited storage and computing resources. Mobile cloud storage provides a promising solution owing to its rich storage resources, great accessibility, and low cost. The encryption of sensitive data is the basic step to resist the risk. However, deploying a high complexity encryption and decryption algorithm on mobile devices will greatly increase the burden of terminal operation and the difficulty to implement the necessary privacy protection algorithm. In this paper, we propose

ENSURE, an efficient and secure encrypted search architecture over mobile cloud storage. ENSURE is inspired by edge computing. It allows mobile devices to offload the computation intensive task onto the edge server to achieve a high efficiency. Besides, to protect data security, it reduces the information acquisition of untrusted cloud by hiding the relevance between query keyword and search results from the cloud.

Fog computing extends cloud computing to the edge of a network enabling new Internet of Things (IoT) applications and services, which may involve critical data that require privacy and security. In an IoT fog computing system, three elements can be distinguished: IoT nodes that collect data, the cloud, and interconnected IoT gateways that exchange messages with the IoT nodes and with the cloud. This article focuses on securing IoT gateways, which are assumed to be constrained in terms of computational resources, but that are able to offload some processing from the cloud and to reduce the latency in the responses to the IoT nodes. However, it is usually taken for granted that IoT gateways have direct access to the electrical grid, which is not always the case: in mission-critical applications like natural disaster relief or environmental monitoring, it is common to deploy IoT nodes and gateways in large areas where electricity comes from solar or wind energy that charge the batteries that power every device. In this praposed work, how to secure IoT gateway communications while minimizing power consumption is analyzed.

The throughput and power consumption of Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are considered, since they are really popular, but have not been thoroughly analyzed when applied to IoT scenarios. Moreover, the most widespread Transport Layer Security (TLS) cipher suites use RSA as the main public key-exchange algorithm, but the key sizes needed are not practical for most IoT devices and cannot be scaled to high security levels. In contrast, ECC represents a much lighter and scalable alternative. Thus, RSA and ECC are compared for equivalent security levels, and power consumption and data throughput are measured using a testbed of IoT gateways. The measurements obtained indicate that, in the specific fog computing scenario proposed, ECC is clearly a much better alternative than RSA, obtaining energy consumption reductions of up to 50% and a data throughput that doubles RSA in most scenarios. These conclusions are then corroborated by a frame temporal analysis of Ethernet packets.

In addition, current data compression algorithms are evaluated, concluding that, when dealing with the small payloads related to IoT applications, they do not pay off in terms of real data throughput and power consumption.With the rapid development of big data and Internet of things (IOT), the number of networking devices and data volume are increasing dramatically. Fog computing, which extends cloud computing to the edge of the network can effectively solve the bottleneck problems of data transmission and data storage. However, security and privacy challenges are also arising in the fog-cloud computing environment.

Ciphertext-policy attribute-based encryption (CP-ABE) can be adopted to realize data access control in fog-cloud computing systems. In this paper, we propose a verifiable outsourced multi-authority access control scheme, named VO-MAACS. In our construction, most encryption and decryption computations are outsourced to fog devices and the computation results can be verified by using our verification method. Meanwhile, to address the revocation issue, we design an efficient user and attribute revocation method for it. Finally, analysis and simulation results show that our scheme is both secure and highly efficient.

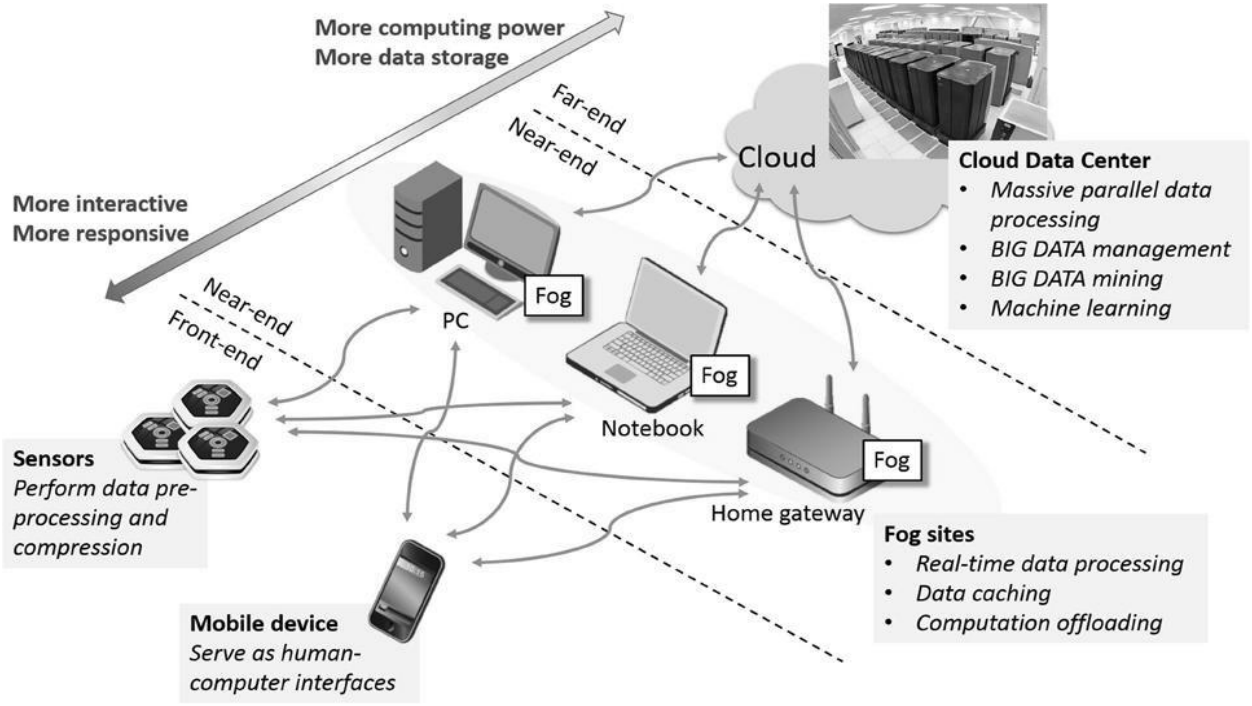

Fig: Fog Computing Overview

II.Implementation

The spillage of confidential information, for instance, data, zone/location or deployment, are getting contemplations when end customers are putting into practice services such as IoT, WSN, cloud computing. There are also defies for ensuring such security in fog computing, in light of the fact that fog nodes are in of end customers locality and can assemble more fragile in-plan than the remote cloud lying in the middle framework/network. Privacy-preserving methodologies have been planned in various circumstances together with cloud [Cao et al, 2014], online social networks [Novak et al, 2014], wireless network [Qin et al, 2014] and smart grid [Rial et al, 2011]. In the fog network, Privacy-preserving methodologies can be running amidst the fog and cloud while those computations are normally resource denied toward the end contraptions or devices. Fog node at the edge generally assembles sensitive data delivered by sensors and end contraptions/devices. Methods, for instance, homomorphic encryption can be exploited to allocate privacy-preserving aggregation at the area doors devoid of unscrambling [Lu et al, 2012]. Differential confidentiality or privacy [Dwork,

2011] can be brought into play to ensure non-disclosure of confidentiality of a subjective single section in the data set if there ought to emerge an event of quantifiable queries. One more security concern is the employment outline with which a fog client makes use of the fog services. Case in point in smart grid, the scrutinizing of the smart meter will reveal piles of information of a family unit, for instance, at what time there is no person at home, and at what time the TV is turned on, which entirely breaks customer's privacy. Regardless of the way that privacy-preserving methodologies instrument have been projected in smart metering [McLaughlin et al, Rial et al, 2011,], they can't be joined in fog computing particularly, as a result of the nonattendance of a trusted pariah or third party or no accomplice contraption/device like a battery. The fog node which can devoid of quite a bit of a stretch accumulate estimations of end customer practice or usage. One possible gullible course of action is that the fog client makes sham assignments and offloads them to diverse fog nodes, disguising its bona fide endeavors among the fake ones. Then again, this game plan will extend the fog client's cost and waste resources and imperativeness or energy. Another course of action would be arranging a sharp strategy for separating the application to guarantee the offloaded resource utilizations don't divulge confidential information. In fog computing, the territory security mainly implies the zone assurance of the fog clients. As a fog client generally speaking offloads its endeavors to the nearest fog node, the fog node, to which the errands are offloaded, can derive that the fog client is contiguous and more far off from distinctive nodes. In addition, if a fog client makes use of different fog services at diverse ranges, it may reveal its path heading to the fog nodes, tolerating the fog nodes interest. For whatever period of time that such a fog client is attached on an object or whatever it to, the location privacy of the individual or the thing is at threat. In case a fog client constantly altogether picks its nearest fog server, the fog node can unquestionably understand that the fog client that is exercising its preparing resources is adjoining. The most ideal approach to ensure the region

security or privacy is through character/identity tangling such that in spite of the way that the fog nodes knows a fog client is adjoining it can't recognize the fog client. There are various systems for identity jumbling; for example, authors of [Wei et al, 2012] bring into play a trusted outcast to create fake ID for each end customer. In reality, a fog client does not as per usual pick the nearest fog node yet rather picks openly one of the fog nodes it can get to concurring some criteria, for instance, idleness, load balance standing, etc. For this circumstance, the fog node can simply know the repulsive territory of the fog client yet can't do all things considered specifically. Regardless, once the fog client brings into play computing resources from various fog nodes in an extent, its region can come down to a little region, since its region must be in the intersection purpose of the different fog nodes coverage’s or ranges. By bringing into play procedure of [Gao et al, 2013] we can preserve the region security in such circumstances.

As far as Access control is concern so it has been a tried and true gadget to ensure the security of the structure and securing of assurance of customer. Standard access control is ordinarily tended to in a same trust region. While due to the outsource method for cloud computing, the access control in cloud computing is by and large cryptographically realized for outsourced data. Symmetric key based course of action is not versatile in key management. A couple open key based courses of action are proposed endeavoring to fulfill fine- grained access control. Authors of [Yu et al, 2010] have planned a fine-grained data access control arrangement created on attribute-based encryption (ABE). Authors of [Dsouza et al, 2014] put forward a

policy-based resource access control in fog computing, to support secure joint exertion and interoperability between heterogeneous resources. In fog computing, how to arrange access control crossing client fog cloud, meanwhile meet the arranging goals and resource constrictions will be frustrating.

III. CONCULSION

Fog computing, a worldview that stretches out cloud computing and services to the edge of the network, meets improved prerequisites by finding information, calculation control or computation power, and systems administration capacities closer to end hubs. Fog computing is recognized by its openness to end clients, especially its backing for versatility. Fog nodes are geographically disseminated, and are employed near wireless access points in regions with a noteworthy use. Fog devices may take the type of stand-alone servers or system gadgets with on-board processing capacities. Services are facilitated at the system or network edge or even inside of end-client gadgets/tools, for example, set-top boxes or access points. This decreases services idleness/latency, enhances QoS and gives a better affair than the client. Fog computing holds up developing Internet of Things (IoT) applications that request ongoing or unsurprising inertness, for example, industrial automation, transportation, and systems of sensors and actuators. Because of the capacity to bolster a wide land dispersion, fog computing is all around situated for continuous or real-time huge information examination. Fog underpins thickly distributed data or information collecting points, adding a fourth hub to the regularly said Big data measurements 3V (volume, variety, and velocity). Issues of security and protection are in fog computing, however this remains understudied especially in the outline and execution of fog computing. Security elucidations exist for cloud computing, yet because of the hidden contrasts between cloud computing and fog computing, such arrangements may not suit fog computing gadgets/tools that are at the edges of systems/networks. In such situations, fog computing gadgets or devices face dangers that don't emerge in a very much oversaw cloud

IV.References

1. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to strangers: authentication in ad-hoc wireless networks. In: NDSS (2002)
2. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Workshop on Mobile Cloud Computing. ACM (2012)
3. Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets authentication in nfc-based mobile computing. In: MobileCloud. IEEE (2014)

4. Cao, N., Yu, S., Yang, Z., Lou, W., Hou, Y.T.: Lt codes-based secure and reliable cloud storage service. In: INFOCOM. IEEE (2012)
5. Cash, D., et al.: Dynamic searchable encryption in very-large databases: data structures and implementation. In: NDSS, vol. 14 (2014) Damiani, E., et al.: A reputation-based approach for choosing reliable resources in peer-to-peer networks. In: CCS. ACM (2002)
6. Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. WCMC **13**(18), 1587–1611 (2013)
7. Dsouza, C., Ahn, G.J., Taguinod, M.: Policy-driven security management for fog computing: preliminary framework and a case study. In: IRI. IEEE (2014)
8. mDwork, C.: Differential privacy. In: van Tilborg, H.C.A., Jajodia, S. (eds.) Encyclopedia of Cryptography and Security. LNCS, vol. 2011. Springer, Heidelberg (2011)
9. ETSI: Mobile-edge computing (2014
10. Gao, Z., Zhu, H., Liu, Y., Li, M., Cao, Z.: Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In: INFOCOM. IEEE (2013)

.