A Managed Access System Provider for Safe and Confirmable Fog-Cloud Computing

Jhansi Bharathi Madavarapu[1*],Giribabu Sinnapolu[2], Shailaja Salagrama[3], Prasad Kalapala[4], K.Reddy Madhavi[5]

[1]Department of Information Technology, University of the Cumberland's, Williamsburg, Kentucky, USA,40769
jhansimadavarapu@gmail.com
[2]Department of Electrical Engineering, Oakland University, Rochester, MI 48309
girisinnapolu@gmail.com
[3]Department of Information Technology, University of the Cumberland's, Williamsburg, Kentucky, USA,40769
Shailajasalagramass@gmail.com
[4]Department of Mechanical Engineering, JNTUK Kakinada, Andhra Pradesh, India
prasadkalapala567@gmail.com
[5]Professor, AI&ML, School of Computing, Mohan Babu University, Tirupati
kreddymadhavi@gmail.com

Abstract. This research introduces HPCS, a model for a clinical decision support system that makes use of private and public cloud computing. In order to reliably and safely track a patient's vitals, a fog server inside the HPCS architecture uses a basic data mining method. It is possible to securely send aberrant symptom reports to a cloud server for accurate prediction the moment they are detected. To safely build a one-layer neural network on fog servers, we present a novel and secure outsourced inner-product protocol. An approach to piecewise polynomial computing allows for the implementation of any activation function in a multilayer neural network on a cloud server while ensuring user privacy is preserved. The problem of computational overload is the focus of our novel protocol, the "privacy-preserving fraction approximation protocol." We show in simulations that HPCS satisfies the goal of health monitoring without exposing patients' privacy to third parties by striking the ideal balance between real-time processing and very precise prediction.
.

Keywords: Cloud Computing, Security, Internet of Things" (IoT), Encryption, and Access Control.

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_112

1 Introduction

Mobile devices with smart sensors must sense, gather, and process data in order for the edge network to achieve intelligent control. Having said that, storage and compute capability on mobile devices are typically somewhat limited. Mobile cloud storage is clearly a good choice due to the large amount of space available, the user-friendliness, and the cheap pricing. The potential exposure of private information is a drawback. Encrypting sensitive data is an important first step in keeping it safe. Making the necessary privacy protection method, meanwhile, will be no easy task. If complex encryption and decryption algorithms are used on mobile devices, the cost of terminal operation will be greatly increased.

Edge networks rely on data felt, gathered, and analyzed by mobile devices with Paste Smart sensors to offer intelligent control, but these devices typically lack the storage and processing power needed for the job. The cheap cost, convenient accessibility, and ample storage capacity offered by mobile cloud storage make it a good substitute. The first layer of protection is to encrypt sensitive information. The extensive use of privacy protection algorithms with high levels of complexity across mobile platforms will put a strain on terminal resources, and they are not easy to build.

An encrypted search architecture that is optimized for speed and security in mobile cloud storage is introduced in this study. It is called ENSURE. The impact of edge computing on ENSURE is substantial. So that mobile devices can concentrate on other tasks, the computation-intensive process can be handled by the edge server. Furthermore, it safeguards data by reducing data gathered from unreliable clouds and by hiding the link between a user's search phrase and the results returned by the cloud.

2 Related Work

Data, zone/location, and deployment security are all factors that end users think about when implementing services like the Internet of Things (IoT), WSN, and cloud computing. In contrast to the faraway cloud in the "middle framework/network," fog nodes are physically closer to the end users, making them potentially more vulnerable while in flight. The cloud, "online social networks," wireless networks, and smart grids are only a few examples of the numerous situations where privacy-preserving techniques have proven indispensable. Fog networks allow privacy-preserving techniques to function, even while end-device computations are frequently denied resources.

Edge devices, such as sensors, transmit private information to a fog node for aggregation. By utilizing homomorphic encryption, which does away with the need for unscrambling, it is feasible to provide privacy-preserving aggregation at the entrances of the region [5]. Differential confidentiality or privacy protections [6] can be employed to prevent a subjective subset of a dataset from being made public in reaction to quantitative queries. The client's work context when utilizing fog services is another possible security hole.

For instance, the smart grid totally invades customers' privacy because a comprehensive inspection of the smart meter will reveal a plethora of information about the household, like when no one is home and when the TV is on. Fog computing and the privacy-protecting procedures instrument for smart meters [7] do not get along without a third party, trustworthy individual, or auxiliary device, such as a battery. It might be easy for the fog node to collect data on user actions or use estimations. False assignments sent to different fog nodes by the fog client could help it conceal its real efforts from the fake ones. This approach will squander the fog client's time, energy, and money, which is unfortunate.

Setting up a cautious way of separating the program's components is another option to ensure that personal data is protected during resource offloading. When talking about fog computing, the term "territorial security" describes the level of protection offered to fog users inside a specific geographic region. For the most part, fog clients will assign tasks to the fog node that is geographically closest to them, thus the receiving fog node can figure out how far away other nodes are and how close they are. Also, if fog services are used extensively throughout a big area, fog nodes might be able to follow a client's path. The global community will be privy to the whereabouts of any person or object that a fog client establishes a connection with. If the fog client consistently

chooses the fog server that is geographically close to it, every fog node will be able to use its computational resources based on how close the fog client is. While fog nodes are aware of the proximity of a fog client, they are unable to determine the client's identity due to character/identity tangling.

One approach to identity jumbling proposed by the authors of [8] is to have a reliable third party supply phony identification documents to each end user. Typically, a fog client will not pick the closest fog node; instead, it will pick one of the fog nodes it is able to reach depending on factors like its activity[11][13], the load balance status, and other similar considerations. Fog nodes can only observe avoidance zones, not modify them, for fog clients. The fog nodes' coverage or ranges may intersect, but the fog client's region might be rather small. The approach outlined in [9][14] can be used to keep the peace in the region.

Access control has been a useful instrument in ensuring the safety of the building and the customers' comfort. Within the same trust zone, we handle the default access control. Encryption is a standard practice before sending data to a third party or the cloud for security purposes. The degree of key management flexibility in an asymmetric key-based technique is low. Possible approaches to provide fine-grained access control include a number of open-key-based solutions. The granular DAC method described in references [9, 10] relies on attributes-based estimation (ABE). In fog computing, RAC is presented in [8] using a policy-based approach, which allows for dependable collaboration and resource interoperability. When using fog computing for access control across client fog clouds, it could be difficult to satisfy organizational goals with limited resources.

3 Implementation

Fog computing is a solution to the problem of potential need for additional security measures in "Internet of Things" (IoT) "new applications and services" that deal with potentially sensitive data. The data-gathering nodes, the cloud, and the gateways that connect the two are the three primary components of an Internet of Things (IoT) fog computing system. "Internet of Things" gateways, which are commonly assumed to have low computational capabilities, will have their security examined in this article. Nonetheless, they might outsource part of their job to the cloud in order to improve reaction times for IoT devices. Deploying nodes and gateways over vast territories, powered by renewable energy sources like solar or wind and stored in batteries, is essential for mission-critical Internet of Things applications like environmental monitoring or disaster assistance. Aiming to minimize power consumption, this planned endeavor investigates the most effective methods of encrypting communications at the "Internet of Things" gateways.

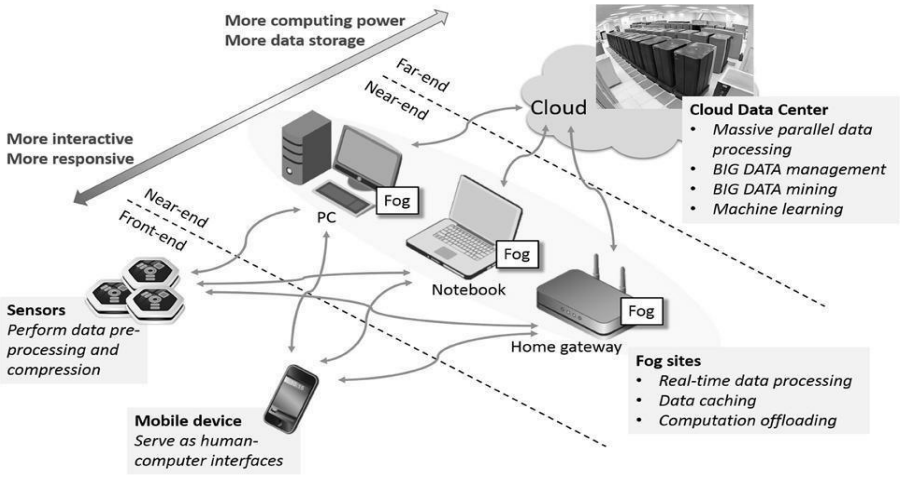


Fig:1 FogComputingOverview

Although there hasn't been a comprehensive assessment of the performance and energy efficiency of popular algorithms like "Rivest-Shamir-Adleman" (or "RSA") and "Elliptic Curve Cryptography" (or "ECC") in IoT scenarios, they are still being investigated. In addition, the most widely used "Transport Layer Security" ("TLS") cypher suites rely on RSA, a basic public key-exchange technique, which necessitates key sizes that are excessively large and cannot be scaled to adequately secure the majority of IoT devices. The alternative, "ECC," is both scalable and lightweight.

To ensure that the two cryptographic algorithms, "RSA" and "ECC," are comparable in terms of security, power consumption, and data throughput, we test them on an Internet of Things gateway test bed. In the proposed fog computing scenario, "ECC" clearly outperforms "RSA"

due to its up to 50% energy savings and twice the data throughput in most cases. These results are corroborated by a frame-by-frame analysis of Ethernet packets.Furthermore, when it comes to the small payloads common in IoT applications, we evaluate the effectiveness of current data compression technologies and discover that they do not considerably enhance real-world data throughput or energy consumption.

The combination of big data with the Internet of Things is partly responsible for the fast expansion of IoT devices and the incredible amount of fresh data. Data transmission and storage constraints can be eliminated by utilizing fog computing to move cloud computing closer to the network's peripheral. Even so, there are fresh privacy and security issues in the fog-cloud computing setting.It is possible to employ "cipher text-policy attribute-based encryption" ("CP-ABE") to establish RBAC in fog-cloud computing instances. Our study presents VO-MAACS, a verifiable outsourced multi-authority access control system. Fog devices can have their cryptographic computations validated using our verification approach. To address the revocation issue, we simultaneously create a user and attribute revocation system that is highly effective. Lastly, our method is effective and cost-effective, as shown by simulation and analytical findings.

4 Results and Discussion

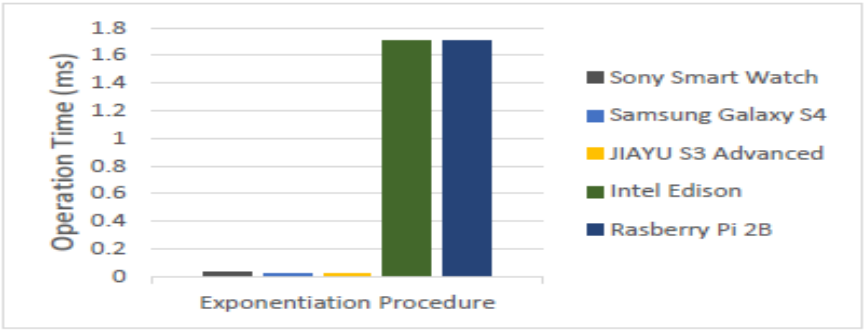
Since this use case involves a vehicular network, we will begin by evaluating the computational overheads on both the server and a variety of general-purpose IoT devices. We simulated the server-side PROUD operations (CSP and STES) on a laptop and tested how well the basic cryptographic procedures (pairing and exponentiation operations) worked. Technical details of the pre-owned PC. We examine Fig. 3 to see how three different levels of security impact our proposal's performance while dealing with bilinear maps and mathematical operations in a multiplicative group.

"Fig: 2 Pairing Function Computation Costs at the Server Side"

Cloud support in an IoT environment may withstand communication overhead, as seen in Fig. 3. Because PROUD allows access policy updating, the CSP must store more ciphertext components, which is different from other state-of-the-art ABSC schemes. Users and CSP can

communicate at low cost due to the ciphertext's constant size.In order to measure the system's performance, we compute the cost of the multiplication operation, which is a rather easy process. The average duration for exponentiation operations increases as the security level grows, as seen in Figure 4. The selection of the type A pairing function and the configuration of three security settings were crucial in achieving these outcomes.

"Fig: 3 Exponentiation Computation Costs at the Server Side"



"Fig:4 Exponentiation Computation Costs"

5 Conclusion and Future Works

Due to the proximity of data, control over computations, and system management tools to end hubs, fog computing is able to meet more rigorous standards. The fact that fog computing is user-friendly and open to new ideas is a key differentiator, particularly when it comes to promoting change. In heavily populated regions, wireless access points and distributed fog nodes work together. There are two types of computing systems that can be considered fog: dedicated servers and networked devices. All the action when it comes to providing services takes place at the periphery of a system or network, or even within end-user hardware and software. The result is less downtime and better quality of service (QoS). Fog computing hinders "Internet of Things" (IoT) applications that rely on consistent or predictable inactivity, such as transportation networks, sensor/actuator systems, and factory automation. Due to its support for a broad geographical dispersion, fog computing is ideal for big data analysis in real-time or continuous mode. The often-mentioned "3V" of Big Data—"volume," "variety," and "velocity"—are shrouded in mystery due to the distributed nature of the data or information collection sites. From a privacy and security standpoint, numerous research have investigated fog computing's architecture and deployment. Fog computing relies on auxiliary devices and tools, therefore the security reasons that support cloud computing might not apply. Fog computing devices are vulnerable to threats that wouldn't exist in a highly monitored cloud system.

References

1. "BalfanzD.," "Smetters K.," "StewartP.," "Wong,H.C.":"Talkingtostrangers: authenticationinad-hocwireless networks."In: "NDSS(2002)"
2. "BonomiF.," "MilitoR.," "ZhuJ.," "Addepalli S.":"Fogcomputinganditsroleinthe"Internet of Things." "In Workshopon Mobile CloudComputing." "ACM (2012)"
3. "BouzefraneS.," "MostefaA.F.B.," "HouacineF.," "CagnonH.:" "Cloudletsauthenticationinnfc-basedmobile computing."In: "Mobile Cloud." "IEEE(2014)"
4. "Cao N.," "Yu S.," "Yang Z.," "Lou W.," "Hou Y.T.": "Lt codes-based secure and reliable cloudstorageservice."In:"INFOCOM." "IEEE (2012)"
5. "Cash D., et al.": "Dynamic searchable encryption in very-large databases: data structuresand implementation." In: “NDSS, vol. 14 (2014)”
6. "Damiani, E.," et al.: "A reputation-basedapproach forchoosingreliableresourcesinpeer-to-peernetworks."In:"CCS." "ACM(2002)"
7. Madavarapu, Jhansi Bharathi, "Payroll Management System" (2014). All Capstone Projects. 82.https://opus.govst.edu/capstones/82
8. J. B. Madavarapu, R. K. Yalamanchili and V. N. Mandhala, "An Ensemble Data Security on Cloud Healthcare Systems," 2023 4th International Conference on Smart Electronics

and Communication (ICOSEC), Trichy, India, 2023, pp. 680-686, doi: 10.1109/ICOSEC58147.2023.10276231.
9. "Gao Z.," "ZhuH.," "LiuY.," "LiM.," "Cao Z.":"Locationprivacyindatabase-drivencognitiveradionetworks:Attacksandcountermeasures."In:"INFOCOM." "IEEE(2013)."
10. Yalamanchili, Radha Krishna, "International Student Portal" (2014). All Capstone Projects. 85.https://opus.govst.edu/capstones/85
11. Madavarapu, J. (2023). Electronic Data Interchange Analysts Strategies to Improve Information Security While Using EDI in Healthcare Organizations. Available from ProQuest Dissertations & Theses Global. (2832638159). https://www.proquest.com/dissertations-theses/electronic-data-interchange-analysts-strategies/docview/2832638159/se-2
12. "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)"
13. "Dsouza C.," "Ahn GJ," "Taguinod M.": "Policy-driven security management for fog computing: preliminary framework and a case study." In: "IRI. IEEE (2014)"
14. "Encyclopedia of Cryptography and Security." "LNCS," "vol. 2011." "Springer, Heidelberg (2011)" ETSI: "Mobile-edge computing" (2014).