NETWORK SECURITY USING FOG COMPUTING IS A DECENTRALIZED NETWORK COMPUTING

V. Suresh Kumar
Department of Computer Science
PG & Research Department,
Gobi Arts & Science College,
Gobichettipalayam, Tamil Nādu, India

Dr. P. E. Elango
Department of Computer Science
PG & Research Department,
Gobi Arts & Science College,
Gobichettipalayam, Tamil Nādu, India

Abstract- Fog computing is a gifted computing paradigm that spreads cloud computing to the advantage of networks. Fog computing is considered as an extension of cloud computing to the edge of the network, which is a highly virtualized platform of resource pool that provides computation, storage, and networking services to nearby end users. In cloud computing deployment, data centers are usually owned by cloud service providers. However, fog service providers can be different parties due to different deployment choices: 1) Network access suppliers or remote transporters, who have control of home doors or cell base stations, may fabricate haze with their current foundations; 2) Cloud specialist co-ops, who need to grow their cloud administrations to the edge of the organization, may likewise fabricate mist frameworks; 3) End clients, who own a neighborhood private cloud and need to diminish the expense of possession, might want to transform the nearby confidential cloud into mist and rent spare assets on the nearby confidential cloud.

In this paper, a novel cryptographic solution is proposed to secure data in fog computing. The solution combines the AES-GMAC operation mode with information dispersal over GF(2 w) to provide data confidentiality, integrity, and availability along with source authentication. The proposed cryptographic solution is based on the dynamic key-dependent approach, which allows for a good compromise between the security level and computational complexity. In the proposed solution, the collected data at one fog node is encrypted, authenticated, and dispersed in a pseudorandom manner to its n neighbor fog nodes. Additionally, attackers should seek the dynamic key, which is different for each input data. On the other hand, redundant fragments protect the stored data against up to (n − k) fog nodes' failure or unavailability.

KEYWORDS: Fog, Untrusted servers, Secret sharing, fog nodes

1. INTRODUCTION

Furthermore, multiple apps will be running on top of these devices, consuming and producing various data types with varying sizes, semantics, frequencies, and privacy levels. By delivering the data to the network edge, fog computing has been developed to get around these restrictions. In order to support time-critical applications, it entails placing data processing, administration, and storage "close" to the users' devices. Be

aware that fog computing is a supplement to cloud computing rather than a replacement. Therefore, a link between the cloud and the fog nodes is necessary. The gathered data is examined and sent to the cloud for backup, while the short-term data is held momentarily at fog nodes. This short-term data may contain important information, such as user passwords. The fog node can be a small data center, a user device (such as a laptop or mobile phone), or a network device (such as a gateway or router).

This study presents a unique data protection mechanism for fog computing. To accomplish data protection and availability, it combines secret sharing across GF(2w) with the usage of a dynamic key-dependent technique, where w is adjustable and may be adjusted to 8, 16, 32, or 64. The suggested approach entails distributing the gathered data into n encrypted pieces with a dynamic key that alternates on a regular basis. Any k of the n fragments and the matching dynamic key is needed for data recovery. Then the fog nodes' surrounding nodes are given the encrypted fragments. As a result, in order to access the usefully analyzed information, an attacker must compromise at least k fog nodes. Contrarily, redundant pieces shield the data against failure or unavailability up to (nk) fog nodes.

2. SECRET SHARING

A distributed secret protection system is called Secret Sharing. Getting over centralized system drawbacks such as single point of failure, secret key leakage, etc., it entails spreading a secret among several entities. Revealing a secret involves breaking it up into smaller pieces, or shares. By using the inverse method on a subset of the dispersed shares, the secret may be obtained. As a result, even if part of the shares are lost, the secret can still be obtained.

A distributed secret protection system is called Secret Sharing. Getting over centralized system drawbacks such as single point of failure, secret key leakage, etc., entails spreading a secret among several entities. Revealing a secret involves breaking it up into smaller pieces, or shares. By using the inverse method on a subset of the dispersed shares, the secret may be obtained. As a result, even if part of the shares is lost, the secret can still be obtained.

The employment of the dynamic key method, the (AES) block cipher with (GCM) mode, and the usage of dynamic key-dependent secret invertible coding matrices are the three primary elements that guarantee the resilience of the proposed system. In actuality, the backward and forward secrecy is guaranteed by the employment of the dynamic key technique. In other words, if the attacker exposes the data from one session by compromising the key, he is not permitted to expose the data from the preceding or subsequent sessions.

The security evaluations demonstrate the proposed scheme's resistance to various security assaults and its ability to guarantee the integrity, authenticity, and secrecy of security services. Though typically at the expense of computational complexity, execution time overhead, and resource constraints, high levels of security are frequently provided.

3. SECURITY ISSUES IN FOG COMPUTING

Data centers used for cloud computing deployment are often owned by cloud service

providers. However, due to various deployment options, fog service providers might be distinct parties: 1) Internet service providers or wireless carriers that manage home gateways or cellular base stations may construct fog using their current infrastructures; 2) Cloud service providers who wish to extend their cloud services to the edge of the network may also construct fog infrastructures; 3) To lower the cost of ownership, end users who own local private clouds would like to convert them to fog and rent out unused resources on the local private clouds. The fog's issue of trust is complicated by its flexibility.

3.1 TRUST MODEL

Damiani et al. suggested employing a distributed polling technique to evaluate the dependability of a resource before downloading as part of a strong reputation system for resource selection in P2P networks. We may need to address problems such in developing a reputation system based on fog computing

- how to achieve persistent, unique, and distinct identity,
- how to treat intentional and accidental misbehavior,
- how to conduct punishment and redemption of reputation.

3.1.1 Rogue Fog Node

In order to evaluate the dependability of a resource before downloading it, Damiani et al. presented a comprehensive reputation system for resource selection in P2P networks. We may need to address problems in order to create a reputation-based fog computing system.

3.1.2 Authentication

Since front fog nodes provide services to extremely large end users, authentication is a crucial challenge for the security of fog computing. The primary security concern with fog computing, according to Stojmenovic et al., is authentication at various levels of fog nodes. Traditional PKI-based authentication has limited scalability and is inefficient.

3.1.3 Network Security

Since wireless is so prevalent in fog networking, wireless network security is a major challenge. Jamming assaults, sniffer attacks, and other examples of attacks. These threats can be dealt with in the wireless network research area, which is outside the purview of this survey. In a network, we often have to rely on manually created configurations from a network administrator and separate network management traffic from ordinary data traffic. When enormous-scale cloud servers are spread out throughout the network edge without simple access for maintenance, fog nodes installed at the Internet's edge will undoubtedly place a tremendous load on network administration. Many elements of fog computing can benefit from the use of SDN, including easier deployment and maintenance, increased network scalability, and lower costs. Additionally, we contend that using SDN in fog computing will present both new issues and possibilities for fog networking security.

4. SECURITY IN DATA STORAGE

Fog computing involves the outsourcing of user data and the transfer of user control over data to a fog node, which has the same security risks as cloud computing. First of all, it is challenging to guarantee data integrity since the outsourced data may be deleted or

erroneously manipulated. Second, unauthorized parties could exploit the submitted data for their own purposes. In the context of cloud computing, an auditable data storage service has been suggested to counter these dangers and safeguard data. In order to offer integrity, secrecy, and verifiability for cloud storage systems so that a client may verify its data stored on untrusted servers, techniques like homomorphic encryption and searchable encryption are coupled.

4.1 Secure and Private Data Computation

Getting safe and privacy-preserving processing outsourced to fog nodes is a key concern in fog computing. Computer Verifiability Verifiable computing allows computer equipment to delegate a function's processing to other, perhaps unreliable servers while still keeping verifiable results. The function is evaluated by the other servers, who also provide evidence that the calculation of the function was done correctly along with the result.

The protocol can give the client input and output privacy (at no extra expense), preventing the server from learning anything about the input and output. Pinocchio is a system created by Parno and Gentry that enables clients to validate generic computations performed by servers using just cryptographic presumptions.

4.2 Privacy

When end users utilize services like cloud computing, wireless networks, and IoT, the leaking of private information like date, location, or use is getting attention. Fog computing presents additional difficulties for maintaining such privacy since fog nodes are closer to end users and have access to more sensitive data than faraway clouds that are part of the core network.

4.2.1 Data Privacy

While often resource-prohibited at the end devices, privacy-preserving algorithms can operate in the fog network between the fog and the cloud. Sensitive data generated by sensors and end devices are typically collected by fog nodes at the edge. It is possible to provide privacy-preserving aggregation at the local gateways without decryption by using methods like homomorphic encryption.

4.2.2 Usage Privacy

The way a fog client makes use of the fog services is another privacy concern. For instance, with a smart grid, the reading of the smart meter would reveal a lot of information about a family, such as when no one is home and when the TV is on, which blatantly violates the privacy of the user. Despite the fact that smart metering has been proposed with privacy-preserving techniques.

5. ACCESS CONTROL IN FOG COMPUTING

Access control has shown to be a dependable solution for maintaining user privacy while ensuring system security. In a similar trust domain, traditional access control is often addressed. While access control in cloud computing is typically performed cryptographically for outsourced data because of the outsourcing nature of the technology. In terms of key management, symmetric key-based solutions are not scalable. In an effort to establish fine-grained access control, many public key-based techniques are presented.

5.1 INTRUSION DETECTION TECHNIQUES

Intrusion detection techniques are widely deployed in a cloud system to mitigate attacks such as insider attacks, flooding attacks, port scanning, and attacks on VM and hypervisor or in a smart grid system to monitor power meter measurements and detect abnormal measurements that could have been compromised by attackers. In fog computing, IDS can be deployed on the fog node system side to detect intrusive behavior by monitoring and analyzing log files, access control policies, and user login information. They can also be deployed at the fog network side to detect malicious attacks such as denial-of-service (DoS), port scanning, etc. In fog computing, it provides new opportunities to investigate how fog computing can help with intrusion detection on both the client side and the centralized cloud side.

This paper examines a number of security and privacy challenges related to fog computing, a cutting-edge computing paradigm that gives nearby end users access to elastic resources at the network's edge. In this article, we talk about network security, safe data storage, and other security-related topics. We also draw attention to privacy concerns related to data privacy, user privacy, and location privacy that may require fresh thinking to address new difficulties and developments.

6. CONCLUSION

For fog systems, a cryptographic technique that simultaneously encrypts authenticates, and fragments input data is presented. This is the first study in this direction that we are aware of. The suggested strategy is new in that it makes use of the dynamic key-dependent cryptographic technique to increase the security of fog systems, in which a dynamic key is created by combining a random nonce with a secret key that is shared by all participants in the system (a dynamic key).

REFERENCES

1. Damiani, E., et al.: A reputation-based approach for choosing reliable resources in peer-to-peer networks. In: CCS. ACM (2002).

2. Cao, N., Yu, S., Yang, Z., Lou, W., Hou, Y.T.: Lt codes-based secure and reliable cloud storage service. In: INFOCOM. IEEE (2012).

3. Cash, D., et al.: Dynamic searchable encryption in very-large databases: Data structures and implementation. In: NDSS. vol. 14 (2014).

4. Novak, E., Li, Q.: Near-pri: Private, proximity-based location sharing. In: INFOCOM. IEEE (2014).

5. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: Nearly practical verifiable computation. In: Security and Privacy. IEEE (2013).

6. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A measurement-based rogue ap detection scheme. In: INFOCOM. IEEE (2009).

7. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A timing-based scheme for rogue ap detection. TPDS 22 (2011).

8. 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).

9. Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets authentication in NFC-based mobile computing. In: MobileCloud. IEEE (2014).

10. Gil Press: Idc: Top 10 technology predictions for 2015. http://goo.gl/zFujnE

11. Ha, K., Chen, Z., Hu, W., Richter, W., Pillai, P., Satyanarayanan, M.: Towards wearable cognitive assistance. In: Mobisys. ACM (2014).