Secure Data Access Control with Cipher Text Update and Computation Outsourcing in Fog Computing for Internet of Things

Shaik Jaffer Vali [a], Dr. Jitendra Sheetlani [b]

[a] *Research Scholar, Dept. of Computer Science,*
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India
[b] *Research Guide, Dept. of Computer Science,*
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Fog Computing is a region of Computer Science that is under steady construction and development, and related to data security, the worldview turns out to be more solid and secure for IoT's edge stages. The verification of limited memory devices has serious issues since memory utilization is high when applied with different models that have the motivation behind shared confirmation. In this paper, we propose the Novel cipher text-based encryption model (NCEM) which has an information access control plot dependent on Ciphertext-Policy it give information privacy, fine-grained control, and mysterious validation in a multi-authority fog computing framework. The sign cryption and plan cryption overhead for the client is altogether diminished by redistributing the bothersome calculation tasks to fog hubs. The proposed conspire is demonstrated to be secure in the standard model and can give trait repudiation and public unquestionable status. The security analysis, asymptotic multifaceted nature examination, and implementation results demonstrate that our construction can offset the security objectives with useful effectiveness in calculation.

Introduction

The Internet of Things is an assortment of embedded sensors, software, and actuators present in devices imparting over the Internet to yield Intelligence, by collecting, processing and trading the produced data. In 2008, the US National Intelligence Council recorded IoT as one among six advances with expected effect on US interests towards 2025 [1]. The remote sensors embedded in an IoT device create an exponential measure of Big data; both constant and batch data. Big data is a rich environment, the essential distinction between continuous and batch data is the recurrence at which the data is produced.

The meaning of Big data is portrayed in a boundless number of ways, Gartner characterized Big data as a "high-volume, high-speed as well as high-assortment data resource that request financially savvy, inventive types of data processing that empower improved knowledge, dynamic, and process automation" [2].

Volume, Variety, and Velocity essentially portrays Big data as the size, type, and the rate at which data is created separately, named as the 3 V's of Big Data. The work of Cloud Computing administrations has significantly helped the processing and storage of this Big data produced by IoT devices.

The conveyance of administration in Cloud Computing includes three assistance models used by an end client; Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). A portion of the upsides of the utilization of Cloud Computing administrations are Auto-provisioning, Elasticity, Cost-viability, Quality of Service (QoS)/Service Level Agreement (SLA) and Scalability. The device is remotely associated with the cloud and naturally gets home to the huge amounts of data created, organizations like Amazon Web Services (AWS), GoGrid, Google, Microsoft and Salesforce.com offer these Cloud Computing administrations. Along these lines, Cloud Computing can be considered essentially as the conveyance of computing as an assistance. Dropbox and OneDrive are instances of individual distributed storage administrations, being utilized all around the globe, our data is put away for nothing, ensured and client access in numerous areas.

Notwithstanding, with the touchy ascent of new and distinctive brilliant IoT devices being conveyed every day, the cloud isn't sufficient. Move of this gigantic data to the cloud actually represents a high dormancy issue, security, dependability, and protection issues, which has prompted the move to the Fog Computing worldview. Fog Computing doesn't wipe out the utilization of Cloud Computing administrations, rather stretches out the cloud to the edge of the organization, in this manner improving the organization and starting vicinity to end clients. [3] characterized Fog Computing as a profoundly virtualized stage that gives process, storage, and systems administration administrations between end devices and conventional Cloud Computing Data Centers. Low inertness, high productivity and ensured QoS are significant favorable circumstances of Fog Computing. Likewise, capacity to process or use Big data continuously is a solid favorable position, writing study on this procedure extensively investigates this point.

Internet of Things (IoT)

The Internet of Things is an assortment of physical devices that have been built with embedded sensors and actuators in them, joined into an organization and collaborates with the Internet. The IoT stage offered ascend to the improvement of keen devices, savvy home automation frameworks, and shrewd vehicles and essentially anything brilliant. Sensor hubs embedded in them do all the shrewd stirs that wind up producing huge amount of data.

Fog Computing:

Cisco's Ginny Nicolas initially instituted Fog Computing; it tends to be just portrayed as an expansion of the Cloud Computing worldview to the edge of the organization, consequently fog is a type of cloud nearer to the ground. Applications and processing of data are performed at the edge of the organization instead of existing exclusively in the cloud. Along these lines, brilliant edge devices can process data as opposed to being deeply engendered (cloud) for processing which saves the cloud assets and limits the idleness engaged with getting to data. In the IoT situation, shrewd edge devices can fundamentally produce gigantic measures of data; communicating such traffic profoundly and retransmitting the reaction back to the edge puts extraordinary interest on the assets. Thus, in the fog computing condition, a great part of the processing is done by the IoT devices advanced for this capacity.

This method is known to limit dormancy and effectively use network transfer speed by diminishing the measure of data that should be sent to the cloud. Figure 1 depicts an outline of what Fog computing involves and the collaborations or connections between the cloud and fog, fog to the edge devices and delineates the capacity of Fog Computing.

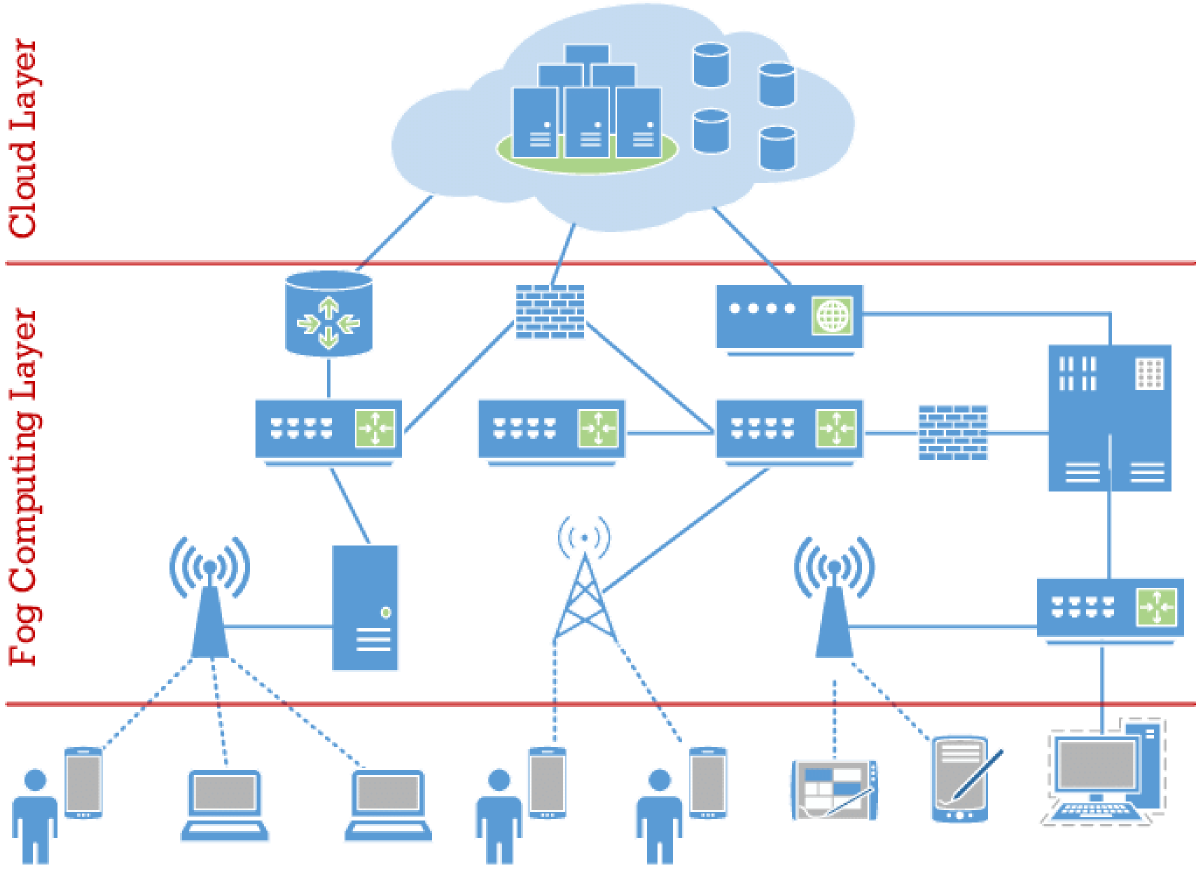

Figure 1: Architecture of Fog computing

Fog computing fuses the utilization of a fog hub; switches, switches or a security camera can be viewed as a fog hub, contingent upon the IoT device been conveyed. An IoT stage should manage the six areas expressed in [13], specifically;

- the domain of the "things", containing both fixed and cell phones, sensors, and so on.,
- the network domain covering the edge, the total, and the center,
- the Cloud domain,
- the service and application domains,
- the user’s domain, and
- the Fog node

Each domain presents various prerequisites to the IoT platform, and will request explicit activities and treatment from the control and the board layers.

Methodology

System Model

In this proposed model, the trait authority is a completely confided in party which is accountable for creating framework boundaries just as mystery key for every client. The CSP is a semi-confided in party which gives high-limit and online data storage administration. It is likewise answerable for confirming the mark before tolerating the refreshed cipher text. The fog hubs are likewise semi-confided in parties which are sent at the network edge and offer an assortment of administrations. They are responsible for producing part of the cipher text and transferring the entire cipher text to the CSP, and furthermore helping clients to unscramble the cipher text from the CSP. Also, they help end clients to sign the cipher text update demand. Data proprietor. The data proprietor has a lot of data from the IoT devices to be transferred to cloud. It is intended to characterize access and update strategies to create the entire cipher text with the fog hubs. The client is connected to fog hubs and outfitted with IoT devices, for example, keen cameras, clinical sensors and savvy meters.

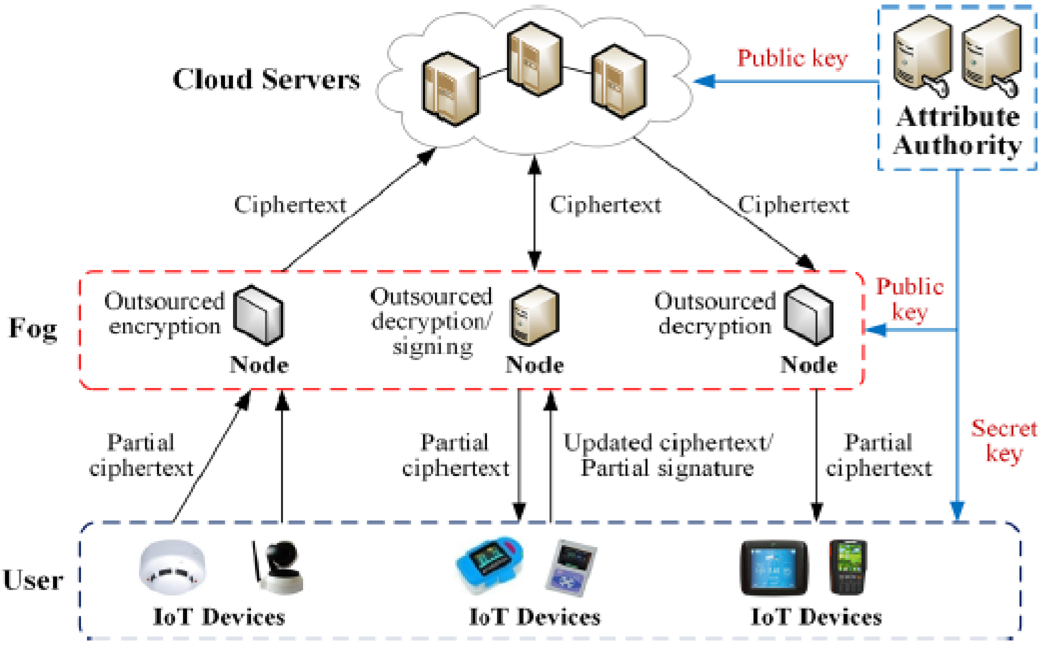

Figure 2: Architecture diagram of proposed NCEM model

Stage 1: System setup

Setup 1: The attribute authority takes as input security Parameter k, and outputs the system public key (PK) and master secret key (MK).

Stage 2: Key generation

Key Gen (PK, MK, S). The attribute authority takes as input PK, MK, a set of attributes S, outputs the secret key SK for the user. And the outsourcing key SK' is sent to fog nodes.

Stage 3: Data symmetric encryption

Fog. Encrypt (PK, T). The fog node takes as input PK, an access policy T, outputs a partial cipher text CT'. Owner. Encrypt (PK, M, Tu, CT). The data owner takes as input PK, a data M, an update policy Tu, a partial cipher text CT', and outputs the cipher text CT.

Stage 4: Data decryption

Fog. Decrypt (PK, CT, SK'). The fog node takes as input PK, a cipher text CT and a user's SK', and outputs a partial decrypted cipher text T if the attributes satisfy access policy T.

In the cipher text CT.

User. Decrypt (T, SK). The user takes as input a partial decrypted cipher text T and SK, then recovers the MK and outputs the plaintext M.

Stage 5: Cipher text update

Fog. Sign (PK, U, Tu, SK'). The fog hub takes as information PK, a client's cipher text update demand U and SK', update strategy Tu. It yields an incomplete mark ST' and the worldwide key GK. Client. Sign (PK, ST', SK). The client takes as info PK, an incomplete mark ST' and SK, yields the mark ST. Confirm (Public key, ST, GK). The CSP takes as info PK, a mark ST and a worldwide key GK. It yields valid if ST is a legitimate mark by the underwriter whose credits fulfilling Tu.

The work process of our plan is appeared in the figure. In the introduction stage, the trait authority utilizes the design calculation to produce the framework boundary. Producing keys with the calculation, the power quality creates mystery keys for proprietors and clients of the data. To accomplish high encryption effectiveness, the proprietor enters the data gathered first with an arbitrary DK applying a symmetric encryption calculation and characterizes an entrance strategy and an approach update, the hub utilizes the fog calculation Encryption to scramble mostly data access strategy, and afterward the data proprietor utilizes an exclusive .Encrypt calculation to end the encryption with admittance to the arrangement and strategy update and put away in the CSP. While getting to data, the fog hub first uses the fog calculation. Decryption to decipher incompletely scrambled text, the client can utilize the client. Decryption calculation to recoup data. In the wake of changing the data, the client likewise utilizes stage encryption calculations to scramble the refreshed data. Prior to making the last adjustment, the client utilizes the client. Join calculation to produce the mark with the arrival of fractional mark of fog hub. Calculation of the sign. At that point, the CSP utilizes the Verify calculation to check the mark lastly acknowledges the refreshed encoded text if the mark is valid. At long last, different clients can get the refreshed data with the decryption calculations. In this manner, clients with Think Internet devices can get to and proficiently update touchy data in fog computing.

In our plan, cloud workers and fog hubs are interested, they execute the undertakings and may conspire to get the unapproved data. In particular, the security model covers the accompanying angles.

1) Data privacy: The unapproved clients which are not the planned recipients characterized by data proprietor ought to be kept from getting to the data.

2) Fine-grained admittance control: The data proprietor can custom expressive and adaptable arrangements so the data just can be gotten to and refreshed by the clients whose ascribes fulfill these strategies.

3) Authentication: If clients couldn't fulfill the update strategy in cipher texts, it ought to likewise be kept from refreshing the cipher texts.

4) Collusion opposition: at least two clients can't consolidate their mystery and redistributing keys and gain admittance to the data they can't get to separately.

Experimental result

In Figure 3 (a) we just think about the cost season of encryption on fog hub among our own and the plans in [16,17,19] since the plans in [18,20] don't uphold encryption redistributing. It is shown in Figure 3 (b) that the calculation season of encryption calculation on data proprietor in our plan is fundamentally equivalent to that in [17], and is littler than that in [18,20] in light of the encryption redistributing. Contrasted and [16,19], the encryption calculation in our plan acquires somewhat more calculation overhead since our plan requires the data proprietor to test n,

$$\{C''_{2,i}, D''_i\}_{i\in[\ell_e]}$$

what's more, perform one Hash work □ = H1(C1) (we don't consider the Hash capacities H2 and H3 here since they are associated with marking convention). In any case, the encryption time is roughly 0.14–0.8 s, which is adequate to the end clients.

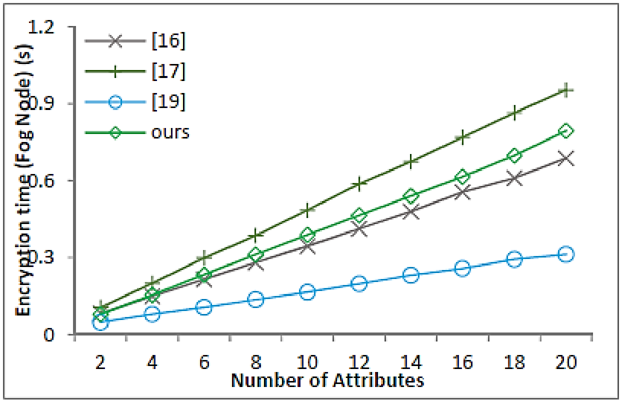

Figure 3(a): Encryption for Fog node side

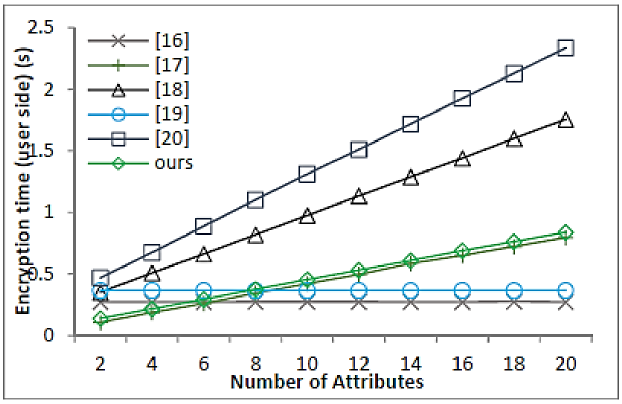

Figure 3(b): Encryption for user side

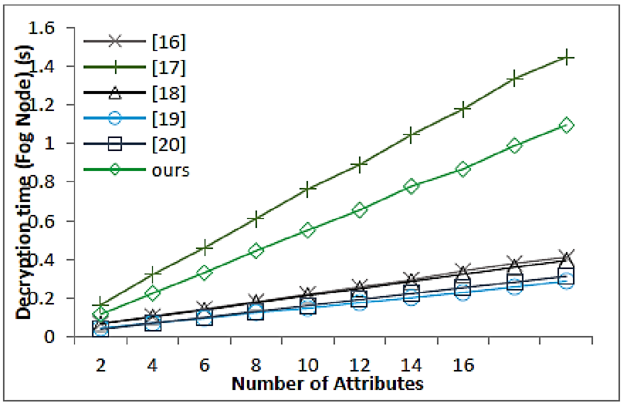

Figure 4(a): Decryption of Fog node side

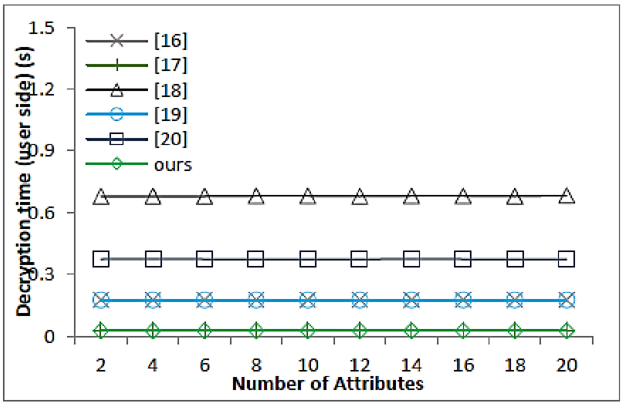

Figure 4(b): Decryption of user side

Figure 4 (a) shows that on the fog hub side, the decryption calculation of our plan acquires more calculation overhead than the plans in [16,18–20]. In any case, Figure 4 (b) shows that our plan performs better than different plans aside from [17] in productivity of decryption time on the client side. This is on the grounds that our plan re-appropriates the most calculation devouring position of decryption to the fog hub and just brings about the expense of one exponentiation and one augmentation in $\mathbb{G}T$ on the client side. In Figure 4 (a), the decryption season of our plan one the fog hub is roughly 0.1 1 s, which increments straightly with the quantity of characteristics. Anyway it is appeared in Figure 4 (b) that the running season of $FullDecryption$ calculation is almost 0.03 s, which is satisfactory for the end client. Since our plan is public evident, the confirmation can be performed on any confided in outsider and doesn't expand the calculation weight of the client. Furthermore, Huang et al. [16] and Zhang et al. [19] just help limit access strategy, while our plan bolsters any droning Boolean capacity. By and large, our plan performs well in encryption and decryption on the client side and supports extra helpful properties, for example, multi specialists, mysterious confirmation, and public certainty.

Conclusion

In this paper, we proposed NCEM plot for data partaking in fog computing framework. The proposed conspire understands the security in the standard model and supports numerous pragmatic properties, for example, secrecy, fine-grained admittance control, mysterious validation, property repudiation, and public obviousness. The substantial calculation activities of the encryption and cipher encryption calculations are moved operations to the fog hubs making our plan more proficient and more reasonable for fog computing than the current plans. The security analysis, asymptotic intricacy, and execution correlations show that our construction hits a decent harmony between the security and overhead productivity.

REFERENCES

1. Rong, C.M.; Nguyen, S.T.; Jaatun, M.G. Beyond lightning: A survey on security challenges in cloudcomputing. *Comput. Electr. Eng*. **2013**, *39*, 47–54.
2. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 13–17 August 2012.
3. Stojmenovic, I.; Wen, S.; Huang, X.Y.; Luan, H. An overview of fog computing and its security issues. *Concurr. Comput. Pract. Exp*. **2016**, *28*, 2991–3005.
4. Ahmad, M.; Amin, M.B.; Hussain, S.; Kang, B.H.; Cheong, T.; Lee, S.Y. Health fog: A novel framework for health and wellness applications. *J. Supercomput.* **2016**, *72*, 3677–3695.
5. Yang, Y.J.; Liu, J.K.; Liang, K.T.; Choo, K.K.; Zhou, J.Y. Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data. In Proceedings of the Computer Security-ESORICS 2015, LNCS 9327, Vienna, Austria, 21–25 September 2015; Springer: Heidelberg, Germany, 2015.
6. Vengatesan, K. et al. "An approach of sales prediction system of customers using data analytics techniques". Advances in Mathematics: Scientific Journal 9. 7(2020): 5049-5056.
7. Yi, S.H.; Qin, Z.R.; Li, Q. Security and privacy issues of fog computing: A survey. In Proceedings of theInternational Conference on Wireless Algorithms, Systems, and Applications, Qufu, China, 10–12 August 2015.
8. Ren, K.; Wang, C.; Wang, Q. Security challenges for the public cloud. *IEEE Internet Comput*. **2012**, *16*, 69–73.
9. Gia, T.N.; Jiang, M.Z.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fog computing in healthcare Internet of things: A case study on ECG feature extraction. In Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and

Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, UK, 26–28 October 2015.

10. Sahai, A.; Waters, B. Fuzzy identity based encryption. *Lect. Notes Comput. Sci.* **2004**, *3494*, 457–473.
11. Gagné, M.; Narayan, S.; Naini, R.S. Threshold attribute based signcryption. In Proceedings of the Security and Cryptography for Networks, LNCS 6280, Amalfi, Italy, 13–15 September 2010; Springer: Berlin/Heidelberg, Germany, 2010.
12. Rao, Y.S.; Dutta, R. Expressive attribute-based signcryption with constant-size ciphertext. In Proceedings of the Progress in Cryptology-AFRICACYPT 2014, LNCS 8469, Marrakesh, Morocco, 28–30 May 2014; Springer: Cham, Switzerland, 2014.
13. Chen, C.; Chen, J.; Lim, H.W.; Zhang, Z.F.; Feng, D.G. Combined public-key schemes: The case of ABE and ABS. In Proceedings of the Provable Secure, LNCS 7496, Chengdu, China, 26–28 September 2012; Springer: Berlin/Heidelberg, Germany, 2012.
14. Liu, J.H.; Huang, X.Y.; Liu, J.K. Secure sharing of personal health records in cloud computing: Ciphertextpolicy attribute based signcryption. *Futur. Gener. Comput. Syst*. **2015**, *52*, 67–76.
15. Rao, Y.S. A secure and efficient ciphertext policy attribute-based signcryption for personal health records sharing in cloud computing. *Futur. Gener. Comput. Syst*. **2017**, *67*, 133–151.
16. Yu, G.; Cao, Z.F. Attribute-based signcryption with hybrid access policy. *Peer PeerNetw. Appl*. **2015**, *20*, 1–9.
17. Huang, Q.L.; Yang, Y.X.; Wang, L.C. Secure data access control with ciphertext update and computationoutsourcing in fog computing for Internet of Things. *IEEE Access* **2017**, *5*, 12941–12950.
18. Fan, K.; Wang, J.X.; Wang, X.; Li, H.; Yang, Y.T. A secure and verifiable outsourced access control scheme in fog-cloud computing. *Sensors* **2017**, *17*, 1695, doi:10.3390/s17071695.
19. Zuo, C.; Shao, J.; Wei, G.Y.; Xie, M.D.; Ji, M. CCA-secure ABE with outsourced decryption for fog computing. *Futur. Gener. Comput. Syst*. **2018**, *78*, 730–738.
20. Zhang, P.; Chen, Z.H.; Liu, J.K.; Liang, K.T.; Liu, H.W. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Futur. Gener. Comput. Syst*. **2018**, *78*, 753–762.
21. Mao, X.P.; Lai, J.Z.; Mei, Q.X.; Chen, K.F.; Weng, J. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption. *IEEE Trans. Dependable Secur.* **2016**, *13*, 533–546.
22. Han, J.G.; Susilo, W.; Mu, Y.; Zhou, J.Y.; Au, M.H.A. Improving privacy and security in decentralized CP-ABE. *IEEE Trans. Inf. Forensics Secur*. **2015**, *10*, 665–678.
23. Jiang, R.; Wu, X.; Bhargava, B. SDSS-MAC: Secure data sharing scheme in multi-authority cloud storage systems. *Comput. Secur.* **2016**, *62*, 193–212.