Turkish Journal of Computer and Mathematics Education Vol.12 No.9 (2021), 1708 - 1716
Research Article

Dual Encryption based secured data maintenance using Fog Computing

K. S. Mohanasathiya[a], and Dr. S. Prasath[b]

[a]Ph.D. Research Scholar (Part-Time), Department of Computer Science, Nandha Arts and Science College, Erode, Tamil Nadu, India
[b]Assistant Professor & Research Supervisor, Department of Computer Science, Nandha Arts and Science College, Erode, Tamil Nadu, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Many people and organizations are accessing data in the cloud due to the rapid growth of cloud computing .Fog computing interface used between cloud and the end devices to reduce the overhead of the cloud computing and better network services, with secure data transmission requirement. In this paper, Identity Based Broadcast Encryption with Decrypting Time Interval (IBBE-DTI) scheme is proposed for protecting the data securely. This facilitates the data to be encrypted with authentication token which is the combination of private key and identities of users who wants the data. To increasing the security, data owner additionally set decrypting time interval along with the data to be encrypted which leads to additional key namely Time Secret Key (TSK) for decryption. This paper proposed a dual verification process for efficient user authentication based on authorization token, which will be defined by the data owner, and a Unique Signature, which will generate by the fog processor at the time of encryption. This proposed work supports both security of data and verifies the user authentication for efficient data transmission with low computation overhead.

1. Introduction

At a low cost, the cloud offers vast data storage and computing capability. Organizations are migrating their data and computing facilities to it because of its on-demand design and low cost and zero maintenance functionality. People's requirements for mobility, low latency, and unstable network access are not being fulfilled by current cloud infrastructure. More intelligent distributed infrastructure, such as fog, is needed to satisfy these requirements (R. K. Johney, 2019). Fog computing's benefits include the ability to use it in a variety of areas, including interactive information processing, IoT, vehicular networks, video analytics, and big data analytics (S. Chen, 2020).

Fog computing also has a lots of benefits, including location awareness, heterogeneity, real-time access, wireless access, and scalability, which, in addition to the significant benefits, poses a great security and privacy concerns (M. Heydari, 2019). Fog allows aggregation, data filtering, and analysis at the network's edge, resulting in improved quality of service (QoS) (O. Mounnan, 2020). Fog devices are used to capture, store, and transmit data in fog computing, and fog nodes are used to link these devices to cloud servers (Wang, J., 2020).

The fog layer is the middle layer in three-layer architecture, and its security function covers all layers, making it essential to the overall system's security (Y. Miao, 2019). Data encryption and encrypted data search are critical for ensuring the security of sensitive data stored at Fog nodes in the case of an untrustworthy Cloud network (M. Arun, 2020). Anonymous data hides the user's personal information in the communication process, such as network location and user identity, using an encryption technique, etc (Li, F., 2020). As well known, authentication service is the entry point of any security system, which consists of verifying users' identities (B.Amor, 2019). Therefore to ensure a secure communication at fog computing we need a lightweight authentication and key management scheme (M. Wazid, 2019).

Edge devices (sensors, smart phones, etc.), fog devices (gateways, small servers, base stations, and other devices with processing, storage, and network access capabilities), and cloud data centers are also common authentication entities in FC (Wang, L., 2020).

In comparison to symmetric encryption, asymmetric encryption is generally slower and more computationally expensive. As a result, using asymmetric algorithms to encrypt a vast volume of IoT data is impossible. Symmetric encryption uses less resource and has a low computing complexity, and it has a high level of reliability as long as the key is kept secret (Khashan, O. A. 2020). The data must be transmit into cipher text with any encryption mechanism like asymmetric or symmetric before passin-g to the fog server. To provide complete security, authentication must be

provisioned with a secure key exchange (Diro, A 2020). The data are handed over to fog nodes for processing and stored in cloud, the data will be out of control from data owners (Wen, M., 2019).

In proposed system, fog provides effective security for the data by time based decrypting process and dual verification process before transmitting the cipher text to the user. The data owner defined both decrypting time interval and authentication of user.

The contributions of this proposed paper are summarized as follows:

1. Identity Based Broadcast Encryption with Decrypting Time Interval (IBBE-DTI) scheme is used to achieve effective user authentication. Using this, the respective user is predicted so that the data received by unauthorized user shall be avoided.
2. The data owner additionally set the decrypting time interval with the raw data, which will reflect at the time of decryption. Because of the time interval the cipher text need a specific time key for decryption which has a limited time period. This will improves the data security by short decrypting time period.
3. The proposed system uses authenticator for dual verification process which supports high data security. It will checks the user authentication and unique signature respectively at first step and second step of verification process.

The rest of the paper is organized as follow. Section II presents literature survey about security in fog computing and encryption techniques. Section III contains the methodology of the proposed work. Section IV has result and discussion which shows the efficiency of the proposed work. Section V contains conclusion of our proposed work.

2. Literature Review

(D. Wu, 2020) Proposed a cooperative computing strategy for block chain secured fog computing for data security during data transmission. For reducing time delay, fog node clusters are used and the access policy is enhanced and the access control list maintained by the block chain based fog node clusters is implemented.

(G.Kumar, 2020) designed a security framework for fog computing to improve the IoTs security. Single point of aggregation and lattice cryptographic approach is used from fog interface for establishing the security services. For enhancing the efficiency of the framework Level-1,Level-2 cache (L1,L2) were implemented. It still needs to optimize the memory management and resource allocation schemes of the framework for improved results.

(Javed, 2019) proposed a Fog-Assisted Cooperative Protocol (FACP) that transmits downlink and uplimk traffic messages efficiently with the help of fog Road Side Units (RSUs).FACP, which combines IEEE 802.11p and C-V2X wireless systems, reduces the time it takes a vehicle to receive traffic information and improves the efficiency of traffic information by using collaborative transmissions.

(W. Zhang, 2020) introduced a model in fog computing, a device model and key message attack model for Internet of Vehicles, and developed a data transmission system focused on privacy security to increase data transmission efficiency in Internet of Vehicles and secure vehicle users' privacy information. To reduce the time delay and encourage the selfish node to transmit data the Robin Steiner bargaining game model is designed.

(H. Xiong, 2019) proposed an anonymous attribute-based broadcast encryption (A2 B2 E) that has the property of secret access policy and allows the data owner to exchange his or her data with several participants who are within a predefined receiver collection and follow the access policy. The data sharing mechanism is reliable and practical to this encryption approach, which facilitates comprehensive vulnerability monitoring and performance assessment.

(S. Zhang, 2020) suggested a Group Key Management Protocol for sharing files stored in cloud among a group of members. Here mixed encryption scheme is used for group key generation and prevent a shared files from attackers verification schemes. Even the security was obtained by this protocol at the same time it exhibits a computation complexity problem.

(G. Thumbur, 2021) presented a authentication scheme which is an efficient and secure certificate less aggregate signature scheme for vehicular ad hoc networks. Here multiple signatures from various vehicles are combined and aggregated into a single signature for reducing the verification time and computation overhead of a Road Side Units.

(K. Tsai, 2019) proposed AES encryption architecture which is a low power consumed architecture, named Low-Power AES Data Encryption Architecture (LPADA), that decreases the power used by the AES for data encryption by using low power SBox, power management method and power gating technique. To increase the safety of the session-key regeneration a key updating system is also suggested which will evade replay attack and eavesdropping attacks.

(Mustacoglu, 2020) introduced a password-based encryption (PBE) technique to protect sensitive data, examine the performance metrics of the proposed method, and presented the experimental results for the key generation and the encryption/decryption calculations. It also needs to develop different methods for identifying failed login attempts in order to deter attackers from attempting to log into the device.

(Li, 2020) presented a concept of proxy re-encryption with equality test (PRE-ET) which combined the methods of proxy re-encryption (PRE) and public key encryption with equality test (PKE-ET) to efficiently share the searched healthcare data on cloud server. The main problem of the proposed system is computation cost of "test" is very high.

3. Methodology

In this paper, the proposed model consist of three entities namely Data Owner, Fog Processor and User as shown in Figure 1.

3.1 Data owner

Data owner generates authentication token of the user and transmit to fog processor with the data to be encrypted, which was associated with the decrypting time interval.

3.2 User

Valid user can get the data after double time verification process and decrypting it with private key and valid TSK.

3.3 Fog Processor

Fog processor plays a vital role in maintaining authenticator and time server for valid user verification and maintains the encrypted data securely. The working process of proposed system model is discussed in following three phases:

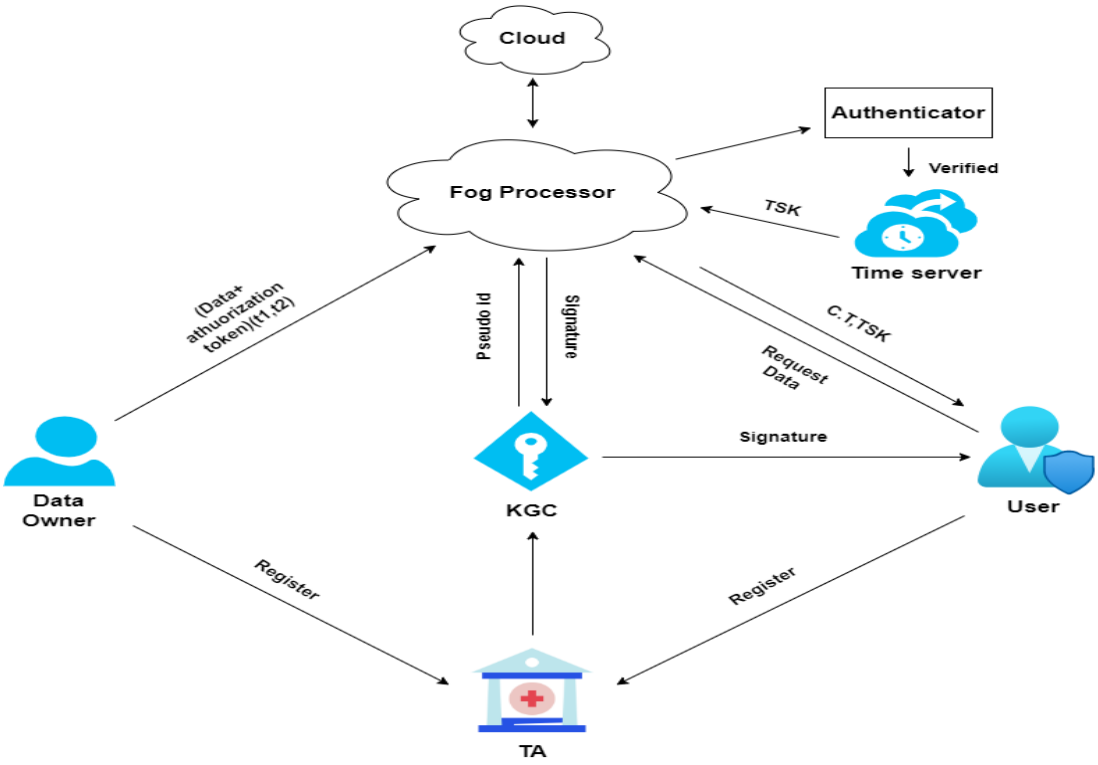

Figure 1. Proposed system model

3.4 Phase 1

In phase 1, the first step of processing is to register them for joining into the system. Here Trusted Authority is maintained for registering by the data owner and user. After registration completed the data owner outsource the data

to fog processor with corresponding authorization tokens. The authorization token consists of secret key and identities of the user who wants data. Authorization token maintains the information about the respective user identities to avoid transmitting the data to wrong user. Additionally the data owner adds decrypting time interval (t1,t2) condition with original data. Data owner outsource original data, authorization token and associated time interval to the fog processor.

3.5 Phase 2

In phase 2, the data send by the user can be protected by the fog processor with the help of encryption as following:

Generally all data are outsourced to cloud which is a centralized system. Fog computing is a cloud computing extension, but it is a decentralized computing structure located between the cloud and devices which produce data. Here fog processor is used in fog environment to provide effective interface for data processing between the users and cloud. Now the fog processor receives a data with authentication token and decrypting time interval. After that, the fog processor starts two major works namely encrypting the data and generates a unique signature for the corresponding user for the verification process.

3.5.1 IBBE-DTI Encryption

For enhancing security, fog processor would store the data in encrypting form by using some encrypting algorithm. In our proposed model Identity Based Broadcast Encryption with Decrypting Time interval (IBBE-DTI) techniques was used which is the combinations of IBBE and decrypting time interval set by the data owner. In IBBE-DTI, data owner used secret key for encrypting the plain text. But that secret key does not directly associate with the data because in this encryption technique, data owner creates an identification key source namely authorization token. The authorization token provides information about the person who has the ability to decode plain text. In other words, only the data users whose names are specified in the authorization token may decode encrypted data. Fog processor receives plaintext and key sources for encrypting and performs IBBE and the cipher text has condition namely decrypting time interval.

3.5.2 Decrypting Time Interval

Decrypting time interval is nothing but, data owner of a data can specify any time interval during the encryption process; the user can decrypt to recover the original plain text only if it has a TSK (Time Secret Key) that corresponds to a time in that interval. For obtaining the Time Secret Key here Trusted Time Server (TTS) was used. With the use of Time Secret Key the decrypting process can be done only in the limited time period which improves the data security. For example the data owner may specify time interval (t1, t2), that means the user can decrypt the cipher text as soon as it is received and a TSK has been obtained, but only up to time t2. After this time, TSK provided by the Trusted Time Server will not help in decryption process.

IBBE-DTI technique supports user benefits from accessing the plain text in a timely manner and where the utility of a TSK becomes limited shortly after its broadcast time. The user can get the Time Secret Key from the Trusted Time Server through Fog Processor at the time of receiving the cipher text. The user cannot decrypt the cipher text with the private key; he/she must need an additional key called Time Secret Key which is associated with the encrypted text. So it extends the security of data by providing dual key for decrypting, if the user has a private key only he/she does not decrypt the information so they need an additional time key for the time depended cryptography process.

3.5.3 Unique Signature Generation

After encrypting the cipher text then fog processor increases security for data by generating Unique Signature. Unique Signature generation is the addition security process which can be done by fog processor with the help of Key Generation Center (KGC). If the user wants a particular data he/she must register themselves with the Trusted Authority. At the time of registering the Trusted Authority sends the user registration to the Key Generation Center. KGC gather the information about the user individual identity which is used for creating a pseudo-identity. Pseudo-identity is one of the key factors for Unique Signature Generation process.

KGC generates the pseudo-id with minimum key size which will increase the efficient signature generation process. Unique Signature can be created by combining the data, secret key, and pseudo-id. Here the unique signature can be generated by fog processor that has the sources such as plain text, and secret key. It will ensure authentication and data integrity. After creating Unique Signature the fog processor transmit it to the KGC and it will send to the

responding user. Finally the fog processor maps the unique signature into the cipher text with associated time interval then outsource into the cloud for secure storage.

3.6 Phase 3

In this phase, the user receives data from the fog processor. Fog processor get a request from the user, then it will checks the requested user is valid or not with the help of authenticator. Here dual verification process was proposed which is the major part of our proposed system model. Authenticator get a cipher text as input from the fog processor, then it will verifies the user by the authentication token which is declare by the data owner. The user verified by the authentication token is the first step of verification process. If the user was correct then the second step of verification can be processed otherwise the user request could be denied at this step. After the successful first step verification process the authenticator moves for second step of verification in which the Unique Signature of the user was verified. The fog processor get unique signature for verification from the user. Hence the authenticator check the signature gets from the user and signature mapped with the cipher text was match or not. If the signature was not valid then the user request denied at the second step verification or it can be moved to next step. After dual verification process the valid user gets the Time Secret Key which is generated by the Trusted Time Server. The Trusted Time Server produces the TSK from the time interval (t1, t2) after dual verification process successes otherwise it does not produce TSK.

Finally fog processor produces the cipher text and TSK to corresponding user who has private key and authorized by the data owner. Then the user decrypts the data immediately before the time limit set by the data owner. Here TSK is only valid up to the time t2; after time t2 the TSK provided by Trusted Time Server does not valid and the cipher text cannot be decrypted. It will improves the data security by this time depended cryptography mechanism. The proposed system supports efficient user authentication by providing dual verification process. Compared with other cryptography process, the time limited decryption process provides much more security for data.

4. Result and discussion

The performance of the proposed model can be analyzed by comparing the parameters such as key size, security and time consumption for encryption and decryption are compared with existing works GKMP [6] and PBE [9].

4.1 Key Size

In cryptography encryption and decryption process requires a key which may be public or private key. The key size will be one of the factors to decide the process security level. Table 1 contains the key size for proposed method, existing works GKMP &BPE.

Security Bit Level	Key Size		
	GKMP	PBE	Proposed method
80	180	176	160
112	234	228	224
128	282	274	256
192	402	396	384
256	534	526	512

Table 1: Key Size of different methods

Figure 2 shows the key size comparison between the GKMP, PBE and Proposed method. It shows that the proposed work achieve high security with minimum key size. To achieve 112 bits of security level, GKMP method needs a key size of 234 bits and PBE needs a key size of 228 bits while proposed work needs a key size of 224 bits as shown in Table 1 and Figure 2.

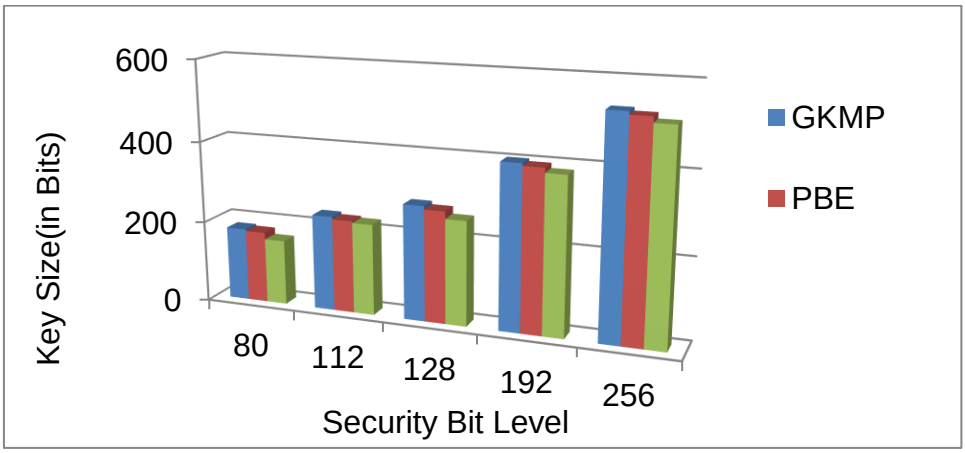

Figure 2: Security Bit Level of proposed work

4.2 Encryption time

The encryption time of the proposed work is compared with the existing GKMP and BPE and it is shown in Table 2.

Table 2: Encryption time Vs Number of authorities

No.of Authorities	Encryption Time		
	GKMP	PBE	Proposed method
4	1350	1260	1000
8	1800	1600	1400
12	2400	1950	1800
16	3700	2600	2400
20	6000	4200	3500

When the number of authorities gets increased, the encryption time is low for the proposed method because the data owner sends data to fog processor for encryption. The fog processor encrypts the data quickly when the authentication of data user defined correctly. Compared with GKMP and BPE, the encryption time is low for the proposed method and it is shown in Figure 3.

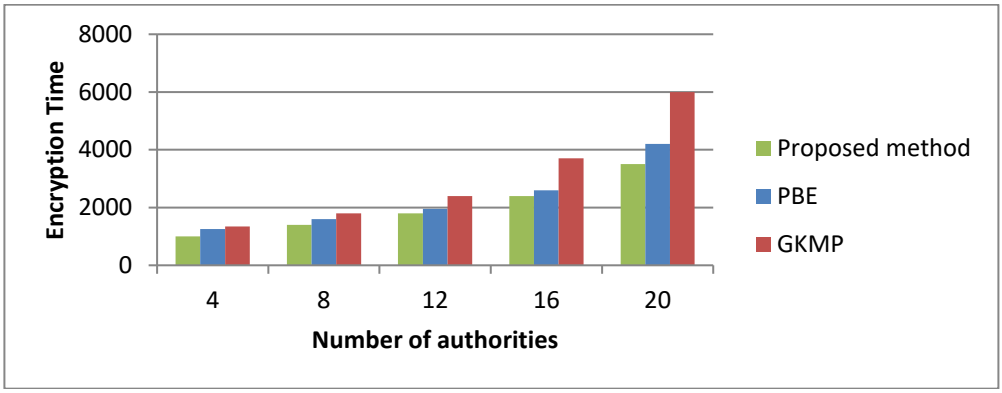

Figure 3: Encryption time Vs Number of authorities

4.3 Computational Overhead

The following table shows the comparison of total computation overhead with total no. of users for different methods. In the below figure, the total computation overhead has get reduced in the proposed system when compared to the existing methods and it is shown in Table 3.

Table 3: Computational overhead Vs Total No. Of users

Total no. of users	Total Computation overhead		
	GKMP	BPE	Proposed method
10	15	12	8
20	28	24	10
30	40	34	22
40	80	73	30
50	92	78	36

The proposed method minimizes the computation overhead while compared with existing methods like GKMP and BPE. In proposed method, a group of users can share a data which requires a single authentication token. This will reduce the computation overhead and it is shown in Figure 4.

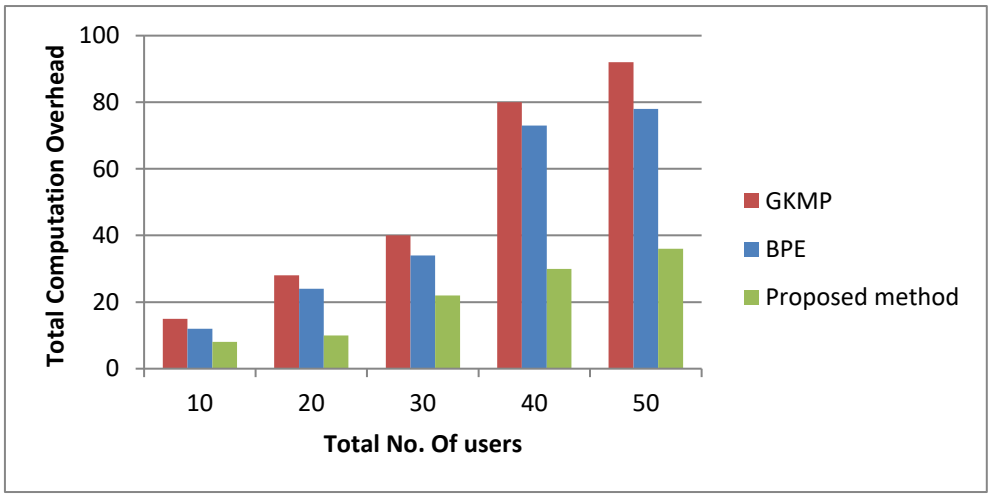

Figure 4: Computational overhead Vs Total No. Of users

5. Conclusion

In this paper, the proposed Identity Based Broadcast Encryption with Decrypting Time Interval (IBBE-DTI) provides efficient security for the user data. This approach can help data owners to encrypt outsourced data using identity-based access control, which eliminates the need for complex cryptographic techniques. Decrypting Time Interval adds advantage by providing a limited time for decrypting and it makes use of Time Secret Key along with Private Key at the time of decryption. Dual verification process ensure, the data to be accessed only by the authorized user who defined by the data owner. Compared with existing works, the proposed method transmits data securely to only authorized user with low computation overhead.

References

Aroulanandam, V.V., Latchoumi, T.P., Balamurugan, K., Yookesh, T.L. (2020). Improving the energy efficiency in mobile Ad-Hoc network using learning-based routing. Revue d'Intelligence Artificielle, Vol. 34, No. 3, pp. 337-343. https://doi.org/10.18280/ria.340312

Arun .M, S. Balamurali, B. S. Rawal, Q. Duan, R. L. Kumar and B. Balamurugan, (2020) *"Mutual Authentication and Authorized Data Access Between Fog and User Based on Blockchain Technology," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, pp. 37-42.*

AMOR .A. B, M. ABID and A. MEDDEB, (2019) *"SAMAFog: Service-Aware Mutual Authentication Fog-based Protocol," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, pp. 1049-1054.*

Balamurugan, K., Uthayakumar, M., Gowthaman, S. and Pandurangan, R., 2018. A study on the compressive residual stress due to waterjet cavitation peening. Engineering Failure Analysis, 92, pp.268-277.

Balamurugan, K., 2020. Metrological changes in surface profile, chip, and temperature on end milling of M2HSS die steel. International Journal of Machining and Machinability of Materials, 22(6), pp.443-453.

Chen .S, X. Zhu, H. Zhang, C. Zhao, G. Yang and K. Wang, (2020) *"Efficient Privacy Preserving Data Collection and Computation Offloading for Fog-Assisted IoT," in IEEE Transactions on Sustainable Computing, vol. 5, no. 4, pp. 526-540.*

Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020*). Lightweight authenticated-encryption scheme for Internet of things based on publish-subscribe communication. IEEE Access, 8, 60539-60551.*

Deng .H et al., (2020) *"Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3168-3180.*

Heydari .M, A. Mylonas, V. Katos, E. Balaguer-Ballester, V. H. F. Tafreshi and E. Benkhelifa, (2019) *"Uncertainty-Aware Authentication Model for Fog Computing in IoT," 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, pp. 52-59.*

Javed, M. A., Nafi, N. S., Basheer, S., AyshaBivi, M., & Bashir, A. K. (2019). *Fog-Assisted Cooperative Protocol for Traffic Message Transmission in Vehicular Networks. IEEE Access, 7, 166148–166156.*

Johney .R. K, E. Shelry and K. R. RemeshBabu, *"Enhanced Security through Cloud-Fog Integration," (2019) International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 1530-1535.*

Khashan, O. A. (2020). *Hybrid lightweight proxy re-encryption scheme for secure fog-to-Things environment. IEEEAccess, 8, 66878 66887.*

Kumar .G et al., (2020) *"A Novel Framework for Fog Computing: Lattice-Based Secured Framework for Cloud Interface," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7783-7794,*

Latchoumi, T.P., Ezhilarasi, T.P. and Balamurugan, K., 2019. Bio-inspired weighed quantum particle swarm optimization and smooth support vector machine ensembles for identification of abnormalities in medical data. SN Applied Sciences, 1(10), pp.1-10.

Li, F., Cui, C., Wang, D., Liu, Z., Elmrabit, N., Wang, Y., & Zhou, H. (2020). *Privacy-aware secure Anonymous communication protocol in CPSS cloud computing. IEEE Access, 8, 62660-62669.*

Li, W., Jin, C., Kumari, S., Xiong, H., &Kumar, S. (2020). *Proxy re-encryption with equality test for secure data sharing in internet of things-based healthcare systems. Transactions on Emerging TelecommunicationsTechnologies.*

Loganathan, J., Janakiraman, S. and Latchoumi, T.P., 2017. A Novel Architecture for Next Generation Cellular Network Using Opportunistic Spectrum Access Scheme. Journal of Advanced Research in Dynamical and Control Systems,(12), pp.1388-1400.

Miao .Y, J. Ma, X. Liu, J. Weng, H. Li and H. Li, (2020) *"Lightweight Fine-Grained Search Over Encrypted Data in Fog Computing," in IEEE Transactions on Services Computing, vol. 12, no. 5, pp. 772-785.*

Mounnan O, A. E. Mouatasim, O. Manad, T. Hidar, A. A. El Kalam and N. Idboufker, (2020) *"Privacy-Aware and Authentication based on Blockchain with Fault Tolerance for IoT enabled Fog Computing," 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, pp. 347-352.*

Mustacoglu, A. F, Catak, F. O., & Fox, G. C. (2020). *Password-based encryption approach for securing sensitive data. Security and Privacy, 3(5).*

Ranjeeth, S., Latchoumi, T.P. and Victer Paul, P., 2019. Optimal stochastic gradient descent with multilayer perceptron based student's academic performance prediction model. Recent Advances in Computer Science and Communications. https://doi. org/10.2174/2666255813666191116150319.

Thumbur .G, G. S. Rao, P. V. Reddy, N. B. Gayathri, D. V. R. K. Reddy and M. Padmavathamma, (2021) *"Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1908-1920.*

Tsai .K, F. Leu, I. You, S. Chang, S. Hu and H. Park, (2019) *"Low-Power AES Data Encryption Architecture for a LoRaWAN," in IEEE Access, vol. 7, pp. 146348-146357.*

Wazid .M, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues and Y. Park, (2019*) "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8804-8817.*

Wang, J., Wang, F., Shi, S., & Yang, W. (2020). *Lattice-based incremental signature scheme for the authenticated data update in fog computing. IEEE Access, 8, 89595-89602.*

Wang, L., An, H., & Chang, Z. (2020). *Security enhancement on a lightweight authentication scheme with anonymity fog computing architecture. IEEE Access, 8, 97267-97278.*

Wen, M., Chen, S., Lu, R., Li, B., & Chen, S. (2019). *Security and efficiency enhanced revocable access control for fog-based smart grid system. IEEE Access, 7, 137968-137981.*

Wu .D and N. Ansari, (2020*) "A Cooperative Computing Strategy for Blockchain-Secured Fog Computing," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6603-6609.*

Xiong .H, H. Zhang and J. Sun, (2020) *"Attribute-Based Privacy-Preserving Data Sharing for Dynamic Groups in Cloud Computing," in IEEE Systems Journal, vol. 13, no. 3, pp. 2739-2750.*

Zhang .W and G. Li, (2020) *"An Efficient and Secure Data Transmission Mechanism for Internet of Vehicles Considering Privacy Protection in Fog Computing Environment," in IEEE Access, vol. 8, pp. 64461-64474.*

Zhang .S, S. Han, B. Zheng, K. Han and E. Pang, (2020) *"Group Key Management Protocol for File Sharing on Cloud Storage," in IEEE Access, vol. 8, pp. 123614-123622.*