International Research Journal of Engineering and Management Studies(IRJEMS)
Volume: 03 Issue: 03 | March -2019 e-ISSN: 2395-0126

# BIG DATA SECURITY BASED ON ACCESS CONTROL SCHEME IN CLOUD

Mr. A. Arulmurugan[1], A. Surya[2], B.P. Shaaruk[3], S. Harishishwaryakumar[4]
*A.V.C College of Engineering & IT& Anna University & Mayiladuthurai, Tamil Nadu*

[1]. Mr. A. Arulmurugan, Professor ,A.V.C College Of Engineering, Mayiladuthurai.
[2]. A. Surya,IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
[3]. B.P. Shaaruk, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
[4]. S. Harishishwaryakumar, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.

## 1. ABSTRACT:

Due to the complexity and volume, outsourcing ciphertexts to a cloud is deemed to be one of the most effective approaches for big data storage and access. Nevertheless, verifying the access legitimacy of a user and securely updating a ciphertext in the cloud based on a new access policy designated by the data owner are two critical challenges to make cloud-based big data storage practical and effective. Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities. In this paper, we propose a secure data sharing using DES cryptosystem for big data storage in clouds. We first propose a new DES decryption algorithm to overcome the decryption failures of the original DES and then detail our scheme and analyze its correctness, security strengths, and computational efficiency. Our scheme allows the cloud server to efficiently update the ciphertext when a new access policy is specified by the data owner, who is also able to validate the update to counter against cheating behaviors of the cloud. It also enables (i) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (ii) a user to validate the information provided by other users for correct plaintext recovery. Rigorous analysis indicates that our scheme can prevent eligible users from cheating and resist various attacks such as the collusion attack.

## 2. EXISTING SYSTEM:

Outsourcing to clouds is one of the most popular approaches to securing the big data storage, in which the data owners encrypt their data based on cryptographic primitives and store the encrypted data to the clouds.
In outsourcing, a secure mechanism should be established between a data owner and a cloud.
In order for the cloud to perform operations over the encrypted data, "Fully Homomorphic Encryption" (FHE) was usually adopted, Homomorphic encryption was also applied to guarantee the security of data storage.
Adequate access control is key to protect the stored data. Access control has traditionally been provided by operating systems or applications restricting access to the information, which typically exposes all the information if the system or application is hacked.

## 3. PROPOSED SYSTEM:

In the proposed system the DES algorithm is used to overcome the problems in the existing system.
We propose a secure data sharing and verifiable access control to protect the big data stored in a cloud storage.

## 4. LITERATURE SURVEY:

**Title**:**Secure and Efficient data communication protocol for Wireless Body Area Networks**

Wireless Body Area Networks (WBANs) are expected to play a major role in the field of patient-health monitoring in the near future, which gains tremendous attention amongst researchers in recent years. One of the challenges is to establish a secure communication architecture between sensors and users, whilst addressing the prevalent security and privacy concerns.In this paper, we propose a communication architecture for BANs, and design a scheme to secure the data communications between implanted /wearable sensors and the data sink/data consumers (doctors or nurse) by employing Ciphertext-Policy Attribute Based Encryption (CP ABE) [1] and signature to store the data in ciphertext format at the data sink, hence ensuring data security. Our scheme achieves a role-based access control by employing an access control tree defined by the attributes of the data. We also design two protocols to securely retrieve the sensitive data from a BAN and instruct the sensors in a BAN. We analyze the proposed scheme, and argue that it provides message authenticity and collusion resistance, and is efficient and feasible. We also evaluate its performance in terms of energy consumption and communication/computation overhead

**Title**:**Cryptography for Big Data Security**

The scheme can verify a user's access legitimacy and validate the information provided by other users for correct plaintext recovery. We devise an efficient and verifiable method to update the ciphertext stored in clouds without increasing any risk when the access policy is dynamically changed by the data owner for various reasons.We prove the correctness of the proposed scheme and investigate its efficiency and security strength.

This chapter focuses on state-of-the-art provably secure cryptographic techniques for protecting big data applications. We do not focus on more established, and commonly available cryptographic solutions. The goal is to inform practitioners of new techniques to consider as they develop new big data solutions rather than to summarize the current best practice for securing data.In this chapter, we have presented a wide variety of cryptographic techniques for securing data in transit, in storage, and in use. We believe that, as security becomes a critical requirement for sensitive big data processing, these techniques will become an integral part of the big data ecosystem. We hope that the exposition in this chapter will raise awareness of the latest types of tools and protections available for securing big data. We believe better understanding and closer collaboration between the data science and cryptography communities will be critical to enabling the future of big data processing.

**Title**:**Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges**

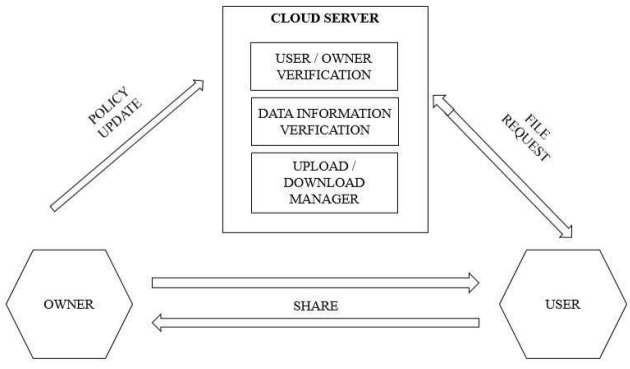
Recent research in the field of quantum computing and quantum information theory has brought about a credible threat to the current state-of-the-art for information protection. The current data protection mechanisms that typically comprise cryptographic systems rely on computational hardness as a means to protect sensitive data. This is to say that there are cryptographic problems that are difficult or impossible to solve using conventional computing. Because of recent advances in quantum computing and quantum information theory, the quantum computer presents a serious challenge to widely used current cryptographic techniques.

This is because some of the same cryptographic problems, which are difficult or impossible to solve using conventional computing, become fairly trivial for the quantum computer.

**Title**:**A secure cloud computing based framework for big data information management of smart grid**

Smart grid is a technological innovation that improves efficiency, reliability, economics, and sustainability of electricity services. It plays a crucial role in modern energy infrastructure. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently; and how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability and flexibility. In this paper, we propose a secure cloud computing based framework for big data information management in smart grids, which we call "Smart-Frame." The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, we present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

**5. ARCHITECTURE:**




**6. IMPLEMENTATION:**

**6.1. MODULE:**
Registration
Login
Data Owner
Data User
Cloud Server

**6.1.1. REGISTRATION:**

The registration module allow the user and data owner to create login username and the password by submitting their information like mail id, phone number, name, etc.
By registering the network or cloud the user can gain access to the resources stored in the cloud.

**6.1.2. LOGIN:**

In this module the user can login by using their unique username and password.
The login module verify the user given username and password with the stored username and password in the cloud.
If the username and password is matched the user can access the resources.
If it does not match the user does not allowed to access the resource.

**6.1.3. DATA OWNER:**

The data provider are allowed to upload the file to the cloud server. The data provider have the private key. This key is used to perform

the encryption operation and also the decryption operation.
If the user need to view the uploaded file the data provider need to share their key to the users.

**6.1.4. DATA USER:**

The user can gain access to the cloud to use the cloud resource by registering on the cloud.
If the user want to view and download the file uploaded by the owner. The user need to gain the two different key decryption key and the policy key to download the file.

**6.1.5. CLOUD SERVER:**

The cloud server are responsible for the encryption and also the decryption operation.
They are responsible for updating the data owner policy key.

**7. CONCLUSION:**

In this paper, we first propose an improved DES cryptosystem to overcome the decryption failures of the existing system and then present a secure and verifiable access control scheme based on the improved DES to protect the outsourced big data stored in a cloud. Our scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding outsourced ciphertext to enable efficient access control over the big data in the cloud. It also provides a verification process for a user to validate its legitimacy of accessing the data to both the data owner and t-1 other legitimate users and the correctness of the information provided by the t-1 other users for plaintext recovery. The security of our proposed scheme is guaranteed by those of the DES cryptosystem and the (t; n)-threshold secret sharing. We have rigorously analyzed.

**8. REFERENCES:**

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.
[2] V. Marx, "Biology: The big challenges of big data," Nature, vol. 498, no. 7453, pp. 255–260, 2013.
[3] G. P. Consortium et al., "A map of human genome variation from population-scale sequencing," Nature, vol. 467, no. 7319, pp. 1061–1073, 2010.
[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.
[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

[6] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94– 107, 2016.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp- tion for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 89–98.
[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography– PKC 2011, pp. 53–70, 2011.
[9] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 37–46, 2013.
[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT 2011, pp. 568– 588, 2011