iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3329

Protected Entree Design for Big Data Knowledge in Cloud

L. Sudha[1], M. Divya[2], S. Jothi[3], K. M. Aiswaryaa[4] Aruna K.B[5]
[1]Associate professor, Dept of CSE, SA Engineering college, Chennai, India
[2, 3, 4, 5]Student of B.E, Dept of CSE, SA Engineering college, Chennai, India

Abstract: Nowadays, the access to the data in the cloud is provided with weak authentication, of the user. Besides, as more and organizations are using clouds to store their data, it becomes more challenging to deal with the issue of access policy. Due to this the leakage of critical information are not well handled. Integrity and confidentiality of the personal information are questioned and are not secure. To overcome this, we propose a new NTRU decryption procedure to overcome the decryption failures of the original NTRU without reducing the security strength of NTRU. The scheme can verify 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 cryptosystem stored in clouds without increasing any risk when the access policy is dynamically changed.

Keywords: Access policy, NTRU, decryption failures, cryptosystem update.

I. INTRODUCTION

Cloud computing creates a enormous advantages for any company. The varying benefits including speed, cost efficiency, flexibility there are many business benefits. The cloud environment which is implemented well can help many innovations to come out and also makes the big data analytics more effective than ever. The process that is used when traditional data mining techniques cannot expose the description and meaning of the underlying data is known to be Big data. An unstructured time sensitive data which is very large cannot be processed by relational database engines requires many tedious and challenging techniques to perform the analysis. This type of data requires a different processing methodology called big data, which uses massive parallelism on readily-available hardware. The capacity of the data stored in the cloud increases day by day. Due to this wide increase in capacity and the difficulty in accessing the desired data, the term cryptography to a cloud is considered to be one of the effective attribute for storing and access a large quantity of data which gives rise to Big data. To overcome the failures in cryptography and decryption we propose a secure and access control based on improved NTRU cryptosystem for big data. This process allows the cloud server to efficiently update the cryptography dynamically when a new access policy is identified by the data owner. This update can also be used to authenticate and counter against cheating behaviors of the cloud users using the improved NTRU algorithm. We propose a new improved NTRU decryption procedure to overcome the decryption failures of the original NTRU and the security strength of the original NTRU is maintained. A secure and verifiable access control scheme to protect the big data stored in a cloud is devised based on attribute-based access structure that can be dynamically updated which is more practical. The scheme can verify a user's access legitimacy and validate the information provided by other users for correct plaintext recovery. This model plays a vital role where an efficient and verifiable method is required to update the cryptosystem stored in clouds without increasing any risk when the access policy is dynamically changed.

II. RELATED WORK

[2] Cloud provide some most popular and important cloud service- data storage. It provides security for data. Existing solutions of encrypted data de duplications suffer from security weakness. Proposed scheme de duplicates encrypted data stored in cloud based ownership challenge and proxy re encryption. It achieves high cost savings and reduced up to 90-95storage needed for backup application. Wastage of network resources and consumption of lot of energy is its disadvantage. The scheme uses Elliptic curve cryptography algorithm (ECC).[3] The proposed scheme consist of three solutions, where blind signature provides the user access privacy and a novel use of bloom filter's bit pattern provides the speedup of search task at cloud side. It provides authorization scheme with the guarantee of user access privacy. Highly efficient in terms of incurred storage and computation cost. Data encryption does not allow the cloud to answer the user queries is its disadvantage. Blind signature and bloom filter algorithms are used. [4] In this paper, the print crypto scheme enables end users to encrypt the data under the access policies called cipher-policy attribute based encryption. While the attributes are still protected, it partially hide attribute values. This is an efficient and trained big data access control scheme with privacy preserving policy. The whole attributes are hidden. Security analysis and performance

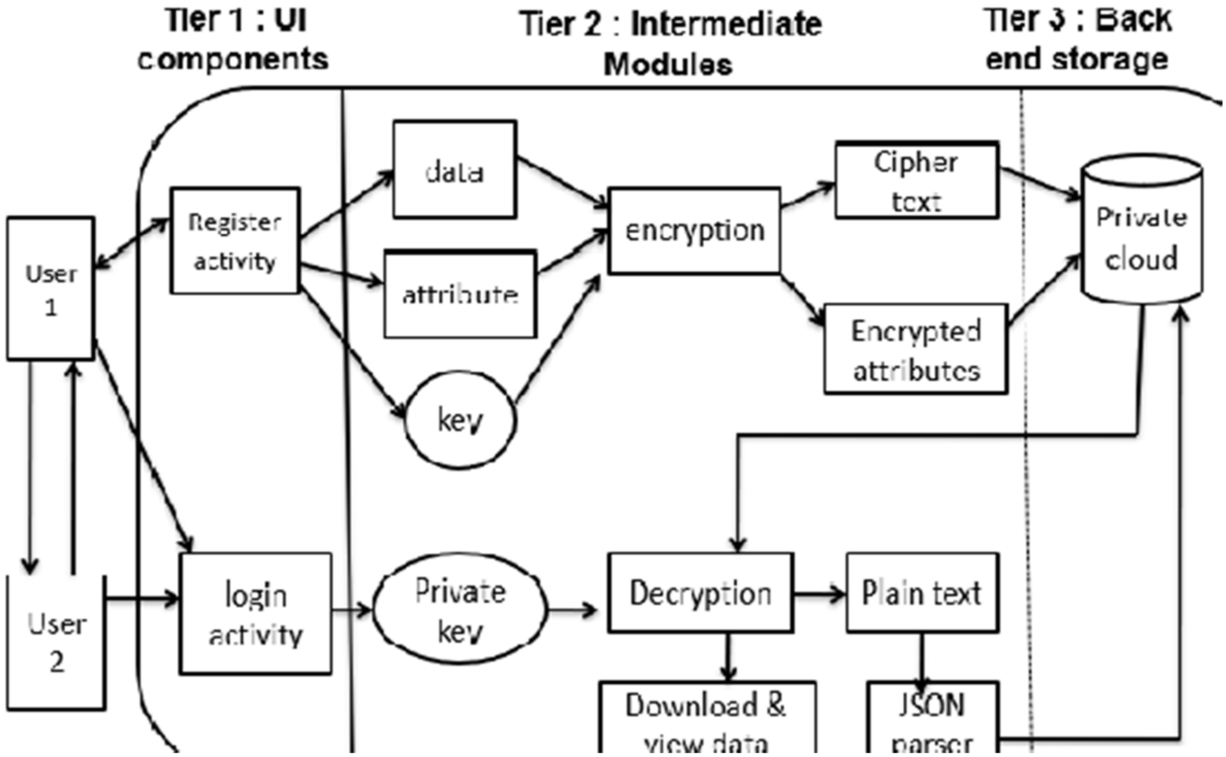
evaluation can preserve the privacy from any LSS access policy without much overhead. Access policy leakage is its disadvantage. ABF build algorithm is used. [7] The user can search keyword using the search query and attribute values in a framework using KSAC (keyword search with access control) over encrypted data in cloud computing. Hierarchical predicate Encryption is the cryptography technology behind KSAC which achieves access policy and keyword update with reducing the data privacy. Since KSAC includes the noise it is proven to enhance the security and privacy level. The scheme every time before search requires the data owners to handle search capability derivation which is considered to be a disadvantage. The scheme uses hierarchical predicate encryption algorithm. [10] In this paper secure authentication protocol for cloud big data in authorization structure. Client obtain their own data from the cloud. CSP Cloud services provider manager by cloud which is not trusted by user entity. Access policy defined by data owners and user attribute and distribute by authority. It is efficient by improving the security management. Multiple authority designed big data access control. CSP is not fully trusted, not flexible, data process is very critical are some of the disadvantages. Key Gen algorithm is used to generate public key and secret key. [12] In this paper introducing software defined network framework. It is an end to end security assessment framework to ignore the security issues by integrating the cloud IOT. It is flexible to manage the network security issues become more important to adopt the cloud IOT as well as reducing business security task. Business security risk can be reduced and is also scalable and flexible to manage the network. Security open issue and complexity of the cloud are disadvantages. Ada rank algorithm is used in the scheme. **[16]** In order to overcome the threats of user location privacy due to location based services the system presents an efficient and privacy-preserving location-based query solution, called EPLQ and also to achieve privacy preserving spatial range query, the first predicate-only encryption scheme is proposed for inner product range (IPRE). The design was developed with efficient, accurate, and secure solution for privacy-preserving spatial range query. The solution for situation like two potential usages are privacy-preserving similarity query and long spatial range query are not given. Setup algorithm, Encryption algorithm, Generate token algorithm, Check algorithm. **[17]** In this paper the flaws of traditional CP-ABE like revealing the confidential information have been overcome using PASH a privacy aware s-health access control system. In PASH the attribute values which are more sensitive are kept hidden in encrypted SHR and only attribute names are revealed through which it attains security in standard model. The scheme provides attribute privacy, decryption test efficiency, expressiveness, full security. The decryption test is supported but it is inefficient because the expensive pairing operation in the test linearly grows in number. Cipher text policy attribute based encryption algorithm is used**. [19]** This paper is based to overcome the difficulties faced by user due to semi-trusted cloud servers using CP-ABE(cipher text policy attribute based encryption). CP-ABE provides a system where there is no central authority and the secret keys are issued by the attribute based authorities independently. The scheme proved to be secure in random oracle model. It is proved to provide additional features like revocation of user and update the cipher text. The scheme faces lack in security because of not combining CP-ABE with two factor authentication. Global setup algorithm, secret key generation algorithm, encryption and decryption are some of the algorithms used. **[22]** one of the vital part of IOT is wireless sensor networks (WSN) which is used in fields like monitoring. Due to this peculiarity, it is highly susceptible to many attacks. Most of the systems focused on only detection methods, thereby it lacked detailed performance analysis. WSN is used by many IOT applications to monitor the environmental conditions like smart healthcare. There is anomalies in network, that reflects in the data collected from the network. [26] This paper introduces time releases proxy condition re encryption scheme which enables file owner but cloud storage does not work with traditional encryption so this indicates that the privacy of encrypted data is not protected in cloud. It provides re encryption scheme for storing and sharing data in designated time arrives to decrypt. It provides storage space in cloud and no fear of losing data handled by exception. But when specific time arrives it decrypt the cipher text and does not support designated cipher text.[27] This paper implemented implantable bio sensor. It collects personal or tiny data and health record of the patient in a front end integration. This works with add on security mechanism which provides more flexible and efficient for security protection of sensitive data. It is flexible, efficient and harder to attack by attacker and also offers security protection. Security risk may arise by storing the data in the public cloud and space complexity are some cons of this scheme.[28] In this paper, a centrally controlled light weight cloud trusted authorities based integrated is used to provide distributed mutual authentication for energy provider, gateways etc. the scheme is efficient and provide semantic security using a certificate less cryptosystem. The main advantage with the system is, it is resistant against man in the middle attack, redirection, denial of service attacks . This protocol cannot be directly integrated with the cloud computing entities. [29] In this paper we introduce CASTRA (Context Aware Security Technology for Responsive and Adaptive Protection) which is used to authenticate and access control with the multifaceted biometric authentication that implemented in the amazon cloud computing platform. It provide more secured performance in CASTRA like mobile application. It provides friendly authentication, confidentiality, user security and also reduces bandwidth consumption. Supervised Learning algorithm is used. [30] This paper provides (AABBE) anonymous attribute based broadcast encryption for which enables the data owner to share a file only to the authorized user of the cloud provider and hidden access policy. It provides high efficiency and decryption techniques. It is very secured by sharing personal data. Unauthorized user cannot access others personal data. Cipher text can be identified easily and malicious users can decrypt the user's personal data are some cons of this model.

III. PERFORMANCE ANALYSIS

Reference paper	Author Name	Advantages	Disadvantages
[19]	Jianghong Wei, Wenfen Liu and Xuexian Hu	Revocation of user and update cipher text.	Lack in security and not outsourcing decryption.
[18]	Sergio Salinas, Xuhui Chen, Jinlong Ji.	Secure outsourcing, large scale data analytics.	Vulnerable to malicious attacks.
[3]	Chia-Mu Yu,Chi-Yuan Chen.	Guaranteed privacy using blind signature.	Cloud doesn't answer the user queries.
[5]	Mazhar Ali, Revathi Dhamotharan, Eraj Khan	Provides confidentiality with access control without compute intensive re-encryption.	Trust Level arises insider threats.
[4]	Kan Yang, Qi Han, Hui Li	Preserves privacy without much over head.	Access policy may leak privacy.

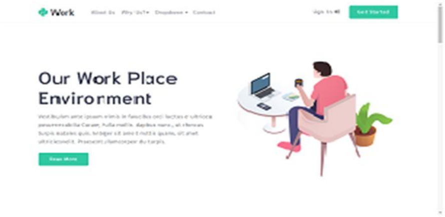
A. *Proposed System*

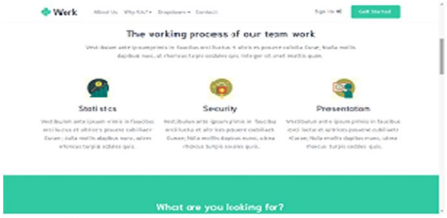
Protected design for big data knowledge in cloud will be developed with cloud and big data as domain in eclipse software. Data owner, data user and cloud admin are the provisions available in the system. Data owner will upload the data onto the cloud. The private key is generated automatically for every data entry in cloud. The data are encrypted and the cipher text and cipher attributes are generated and stored in the cloud. Data user, i.e., whoever wants to access data can give data request to the data owner. On accepting the request, the private key will be shared with data user through email. Now for decryption using private key the improved NTRU cryptosystem will be used overcome the decryption failures. The plain text is parsed by JSON parser and stored in cloud.

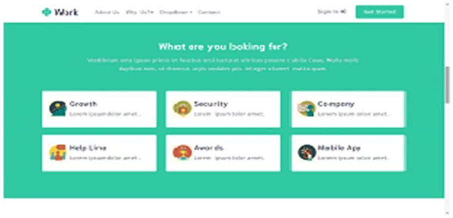


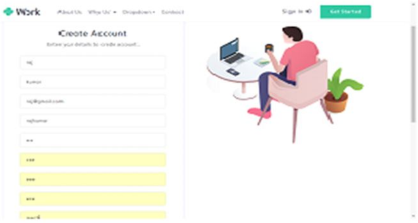
IV. PROPOSED IMPROVED NTRU CRYPTOSYSTEM

A. Home Page

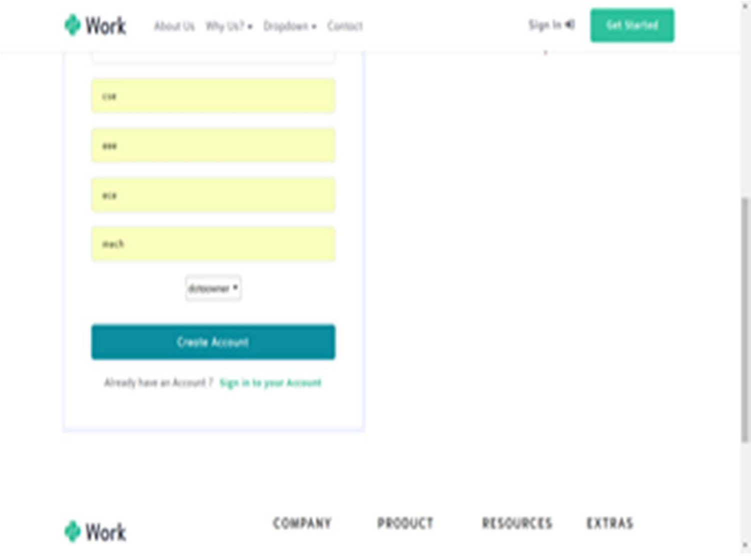




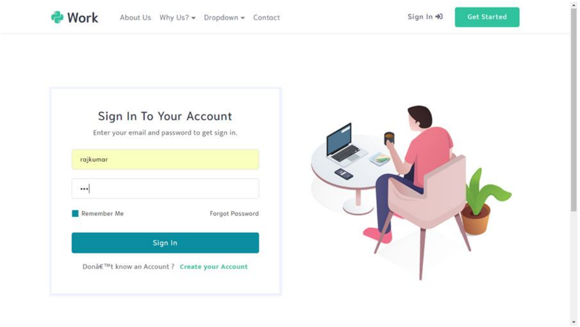




B. Registration Page For Data Owner



C. Login Page For Data Owner



Sign In To Your Account

Enter your email and password to get sign in.

rajkumar

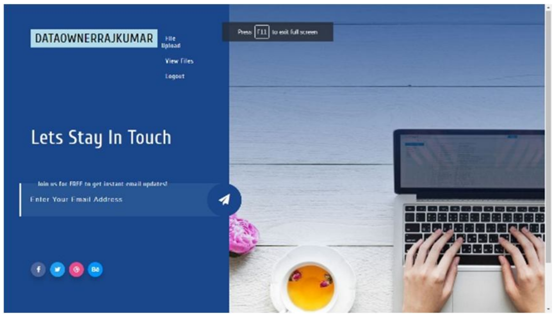
•••

■ Remember Me   Forgot Password

Sign In

Donâ€™t know an Account ? Create your Account

D. Data Owner Page

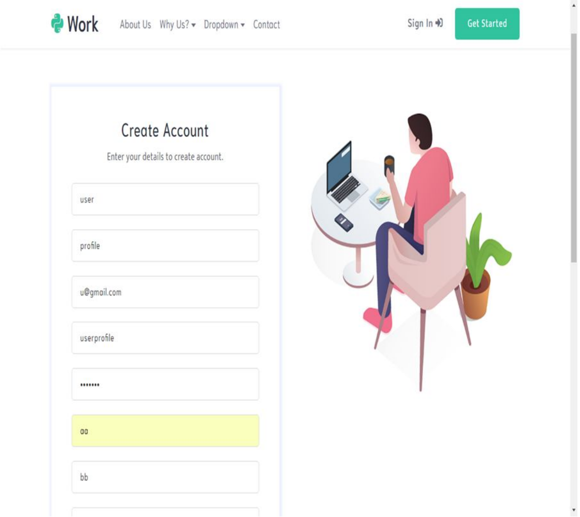


Lets Stay In Touch

Join us for FREE to get instant email updates!

Enter Your Email Address

E. Registration Page For Data User



Create Account

Enter your details to create account.

user

profile

u@gmail.com

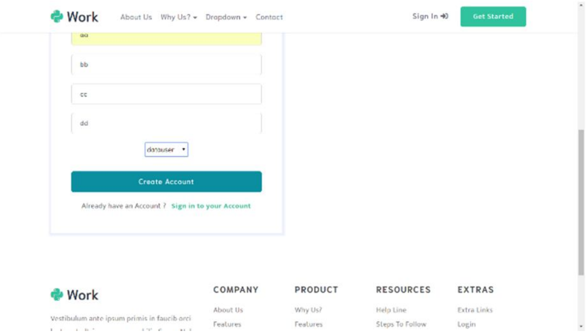
userprofile

•••••••

aa

bb

F. Login Page For Data User



aa

bb

cc

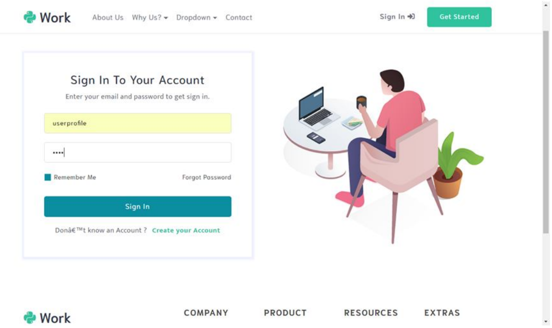
dd

datauser

Create Account

Already have an Account ? Sign in to your Account

Vestibulum ante ipsum primis in faucib orci



Sign In To Your Account

Enter your email and password to get sign in.

userprofile

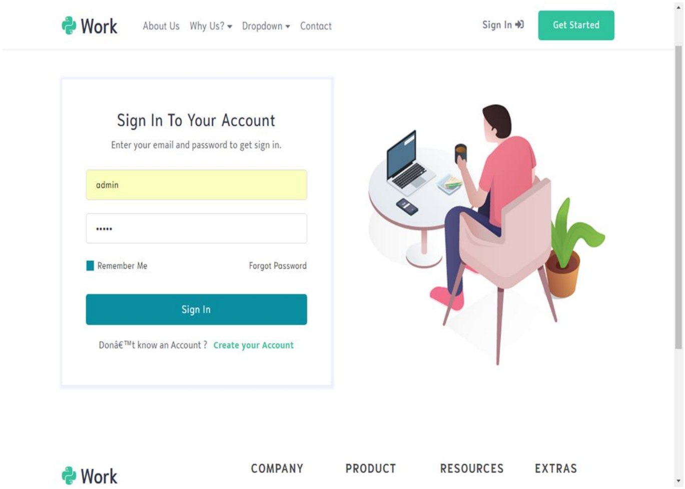
••••

■ Remember Me   Forgot Password

Sign In

Donâ€™t know an Account ? Create your Account

G. Login Page For Admin



Sign In To Your Account

Enter your email and password to get sign in.

admin

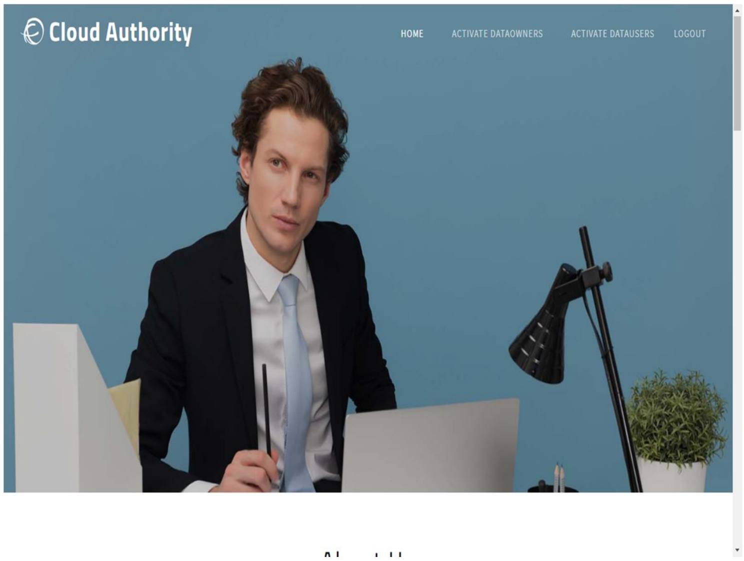
•••••

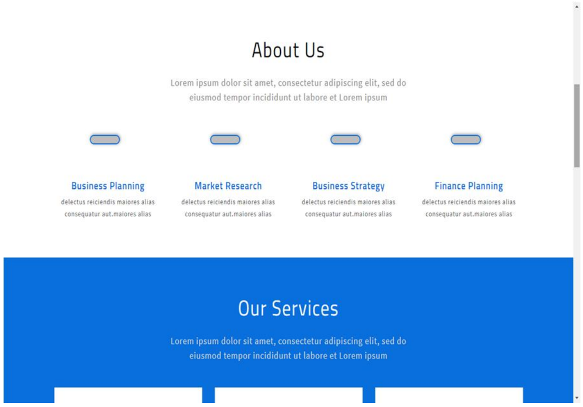
Remember Me

Forgot Password

Donâ€™t know an Account ? Create your Account

H. Admin Page





About Us

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et Lorem ipsum

Business Planning

delectus reiciendis maiores alias consequatur aut.maiores alias

Market Research

delectus reiciendis maiores alias consequatur aut.maiores alias

Business Strategy

delectus reiciendis maiores alias consequatur aut.maiores alias

Finance Planning

delectus reiciendis maiores alias consequatur aut.maiores alias

Our Services

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et Lorem ipsum

V. CONCLUSION

For the past decades a user can access cloud for saving the data. In this project, user can secure their data stored in the cloud by using the NTRU Cryptosystem with the encryption and decryption process. While request for the data download the user will sent the secure id to user who needs to download with the access of the mail.

REFERENCES

[1] Karthick Elangovan, Dr. Sethukarasi.T." Knowledge enrichment of Prediction using Machine Learning algorithms for Data Mining and big Data as a Survey", International Journal of Advances in natural and applied science 10(15). October 2016 Pages 20-30.

[2] Zheng Yang, Wenxiu Ding, Xixun Yu, Haigi Zhu, Robert H.Deng Volume: 2 Issue: 2, June 2016, Volume: 2 , Issue:2,June 2016," Deduplication on Encrypted Big Data in Cloud", IEEE System Journal, DOI:10.1109/TBDATA.2016.2587659.

[3] Chia-Mu Yu, Chi-Yuan Chen,and Han-ChiehChoa, Volume: 11, Issue:2,June 2017,"Privacy-Preserving Multikeyword Similarity Search Over Outsourced Cloud Data ", IEEE System Journal, DOI: 10.1109/JSYST.2015.2402437.

[4] Kan Yang, Qi Han, Hui Li, Kan Zheng, Senior, Zhou Su, Xuemin,"An Efficient and Fine-Grained Big Data Access Control Scheme With Privacy-Preserving Policy", Volume: 4 , Issue:2 , April 2017 ,DOI:10.1109/JIOT.2016.2571718

[5] Mazhar Ali, Student Member, IEEE, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. "SeDaSC:Secure Data Sharing in Clouds" IEEE systems journal ,Volume: 11 , issue 2 , June 2017, DOI: 10.1109/JSYST.2014.2379646

[6] Wei Li, Bonnie M. Liu, Dongxi Liu, Ren Ping Liu, Peishun Wang, Shoushan Luo, and Wei Ni, "Unified Fine-grained Access Control for Personal Health Records in Cloud Computing "Volume: 26, Issue:2 , Dec 2015 DOI: 10.1109/TPDS.2014.2380373

[7] Zhirong Shen, Jiwu Shu, and Wei Xei "Keyword Search With Access Control Over Encrypted Cloud Data ",IEEE Sensors Journal , Volume: 17 , Issue: 3 , Feb.1, 1 2017 ,DOI: 10.1109/JSEN.2016.2634018

[8] Xili Dai, Xiaomin Wang, Nianbo Liu,"Optimal Scheduling of Data-Intensive Applications in Cloud-Based Video Distribution Services" IEEE Transactions on Circuits and Systems for Video Technology, Volume: 27, Issue: 1 , Jan. 2017 DOI:10.1109/TCSVT.2016.2565918

[9] Kan Yang, Xiaohua Jia, and Kui Ren," Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud" IEEE Transactions on Parallel and Distributed Systems Volume: 26 , Issue: 12 , Dec 2012 DOI: 10.1109/TPDS.2014.2380373

[10] dan yang1, 2, yu-chi chen2, 3, (Member, IEEE), SHAOZHEN YE 1 , and RAYLIN TSO4, Volume: 6 ,22 October 2018," Privacy-Preserving Outsourced Similarity Test for Access Over Encrypted Data in the Cloud", IEEE Access, DOI: 10.1109/ACCESS.2018.2877036

[11] Zhuobing Han, Xiaohong Li, Keman Huang and Zhiyong Feng, Volume: 5 , Issue: 3, June 2018 ,"A Software Defined Network based Security Assessment Framework for CloudIoT "IEEE INTERNET OF THINGS JOURNAL,DOI: 10.1109/JIOT.2018.2801944

[12] JianShen, Dengzhi Liu, Qi Liu, Xingming Sun and Yan Zhang,Volume: 11 , Issue: 4 , Dec. 2017,"Secure Authentication in Cloud Big Data with Hierarchical Attribute Authorization Structure", IEEE Transactions on Big Data, DOI: 10.1109/TBDATA.2017.2705048

[13] Prosanta Gopeand Ashok Kumar Das, Volume: 4 , Issue: 5 , Oct. 2017,"Robust Anonymous Mutual Authentication Scheme for n-times Ubiquitous Mobile Cloud Computing Services", IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2017.2723915

[14] Ying-Hao Hung, Sen-Shan Huang, Yuh-Min Tseng, and Tung-Tso Tsai, Volume: 11 , Issue: 4 , Dec. 2017,"Efficient Anonymous Multi receiver Certificateless Encryption",IEEE Systems Journal, DOI: 10.1109/JSYST.2015.2451193s

[15] Khalid Alharbi ,Xiaod,ong Lin and Jun Shao , Volume: 4 , Issue: 2, April 2017 ," A Privacy-Preserving Data-Sharing Framework for Smart Grid ", IEEE Internet of Things Journal,DOI:10.1109/JIOT.2016.2561908

[16] Lichun Li, Rongxing Lu and Cheng Huang,Volume 3 , Issue: 2, April 2016," EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data", IEEE Internet of Things Journal,DOI: 10.1109/JIOT.2015.2469605IEEE

[17] Yinghui Zhang, Dong Zheng, Robert H. Deng, Fellow, Volume: 5 , Issue: 3 , June 2018," Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control", IEEE Internet of Things Journal,DOI: 10.1109/JIOT.2018.2825289

[18] Sergio Salinas, Xuhui Chen, Jinlong Ji, PanLi"A tutorial on secure outsourcing of large-scale computations for big data" IEEE AccessYear: 2016 , Volume: 4, DOI: 10.1109/ACCESS.2016.2549982.

[19] Jianghong Wei, Wenfen Liu and Xuexian Hu, Volume: 12 , Issue: 2, June 2018 , "Secure and efficient Attribute-Based Access control for Multiauthority cloud storage", IEEE Systems Journal, DOI : 10.1109/JSYST.2016.2633559

[20] Chyan Yang and Chien-Chao Tsai,''Managing Secure Communications With Multilevel Security and Restricted Character Set Translation'',IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 1 I. NO. 5, JUNE 1993.

[21] Steven M. Bellovin, Randy Bush "Configuration management and security "IEEE Journal on Selected Areas in Communications ,Volume: 27 , Issue: 3 , April 2009 ,DOI: 10.1109/JSAC.2009.090403.

[22] HaomengXie ; Zheng Yan ; Zhen Yao ; Mohammed Atiquzzaman "Data Collection for Security Measurement in Wireless Sensor Networks: A Survey" IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2018.2883403

[23] Battista Biggio, Giorgio Fumera, Fabio Rol" Security Evaluation of Pattern Classifiers under Attack"IEEE Transactions on Knowledge and Data Engineering,Year: 2014 , Volume: 26 , Issue: 4 , DOI:10.1109/TKDE.2013.57

[24] s. sciancalepore, G.piro, D.caldarola, G.boggia, and G.Bianchi, "On the design of a decentralized and multiauthority access control scheme in federated and cloud assisted cyber-physical systems" IEEE transaction on internet of things, DOI: 10.1109/JIOT.2018.2864300

[25] Xu Yuan, Xingliang Yuan, Baochun Li and Cong Wang, Early Access ," Toward Secure and Scalable Computation in Internet of Things Data Applications " , IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2018.2890728

[26] Chun-I Fan, Jun-Cheng Chen, Shi-Yuan Huang, Jheng-Jia Huang, and Wen-Tsuen Chen, Volume: 11 , Issue: 4 , Dec. 2017 ," Provably Secure Timed-Release Proxy Conditional Reencryption", IEEE Systems Journal, DOI: 10.1109/JSYST.2014.2385778

[27] Shu-Di Bao, Meng Chen and Guang-Zhong Yang, Volume: 21 , Issue: 6 , Nov. 2017 , "A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications", IEEE Journal of Biomedical and Health Informatics, DOI: 10.1109/JBHI.2017.2679979

[28] Neetesh Saxena and Bong Jun Choi, Volume: 12 , Issue: 3 , Sept. 2018," Integrated Distributed Authentication Protocol for Smart Grid Communications", IEEE Systems Journal, DOI: 10.1109/JSYST.2016.2574699

[29] Devu Manikantan Shila and Kunal Srivastava, Volume: 5 , Issue: 5, Oct. 2018," CASTRA: Seamless and Unobtrusive Authentication of Users to Diverse Mobile Services", IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2018.285150

[30] Hu xiong, Hao zhang and Jianfei sun, 03 September 2018, pages: 1-22," Attribute based privacy preserving data sharing for dynamic groups in cloud computing", IEEE systems Journal, DOI: 10.1109/JSYST.2018.2865221