*International Journal of Engineering & Technology*, 7 (3.27) (2018) 586-592

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# A Study on Privacy Preservation Techniques and Scope of Applying Deep Learning Concepts in Security: a Survey

**Ravula Arun Kumar[1]*, Dr.Vinuthna Kambalapally[2]***

[1]*Research Scholar, Deparment of Cse,* Koneru Lakshmaiah Education Foundation, Vijayawada, India.
[2] *Associate professor, Deparment of Cse,* Koneru Lakshmaiah Education Foundation, Vijayawada, India
**Corresponding author E-mail: arunravula12@gmail.com*

## Abstract

The Data privacy and security plays a major scientific role in the research industry with a variety of content and with different datasets of cloud –fog – Internet of things. These three domains have been placed a rapid search content in security as well as networking basics. Here, it is found that different survey methods and search techniques that provides secure privacy data when data gets uploaded to the cloud via fog nodes. Thus, we also check those can be any deep learning techniques that can be applied for the purpose of security in cloud source. Infrastructure as the fog computing is named as edge computing which has a disturbed network, so it can't be entirely trusted when we upload the data to the cloud and in fact, cloud also has some concerns about security as it is updated and maintained by third party service providers. To precise, we check various methods that can be applied to secure the data, make comparisons and also checking for the crop where can be deep neural learning along with machine learning can be applied for this survey.

**Keywords***:* Cipher text Attribute based Encryption (CP-ABE); Ciphertext Policy Attribute set based encryption (CP-ASBE); Deep –learning; Efficient Key policy Attribute based Encryption (EKP-ABE); Hierarchical Attribute set based Encryption; Hierarchical Identity based Encryption (HIBE); Key Policy -Attribute Based Encryption.

## 1. Introduction

Fog computing as created an impact on the generalized computing market for resource allocation and for any other network management, as it has limited storage and computing, but the advantage is resource pooling and data is dynamically allocated which could fetch the maximum consistency in breaking the information as per the security standards [1,2]. Fog cloud has provided and bring a scope for the quality of service of data storage and also for resource computation, the resource allocation with the working of np-hard problems gives much scope of data accessing as well as providing security based on access policy and the renew policy [3,4]. Privacy schemes of attribute-based encryption, cipher text-based attribute encryption, Homomorphic encryption gives the much and broad scope of uncertainty in falling the structure of secure-preserving of data [5,6] fine-grained policy along with location-based service which could produce some locations based on Geo positioning system (GPS).

The Big data of cloud has been properly organized at edge node or fog note because it has a rapid source of information which can contain structural data or it may contain unstructured data, as of data mining we predict and classify many things just like we apply encryption and decryption techniques based on cryptographic systems [7,8]. A homomorphic technique that can be applied to set off attributed which match based on a tree-based architecture that projects a board vision structure aspect in providing the mission and vision technique for the set of given values that generate the multiple assets for a key policy of delegator. Here the problem with the internet of things devices might be critical when we apply the content to we able devices of smart things such as watches, shocks and other glasses and smart cool watches etc. they provide with censorable content which sense the information from the human structure and send it to the IoT devices patient monitoring is one of the aspect that which can be modified without security for the Internet of things devices, as the devices play major role in science and engineering and open 2025, the major part of sciences and clinical resources would be done by IOT.

Here the problem arise when the attacker Sense the data and manipulate according to the needs of him, treat it can be done just for the sake of novelty, the information critically would reduce based on the attacker search and manipulation of active data and passive data [8], if the data could passive the information can be just seen through end no modification is done and if the attacker would justify his nature by manipulating the information then it could be a serious threat to the data uploaded via IOT nodes to the edge nodes, the edge nodes of the fog contain the LTE objects that have light transmission of information can be broken by the Daniel of service, where the information can be broken by the people that majorly skipped with the nature of accuracy stating the positioning of the circumstances, distributed Daniel of service could recommend, says security patches have to be updated whenever they asked based on some extra features such as firewall up gradation, network security updates and etc.

IT companies of many scale structures of sales force, Google and AT & T labs focused much on cloud services they offer and also a lot more research is developed to get the cloud into proper infrastructure the mapping between the fog or edge nodes and the cloud infrastructure of private cloud, community cloud and also public cloud provider much sense when compared to the era of slavery cloud services. Deep neural learning and networking plays a vital role in capacity optimization and also for resource allocation, the algorithms like NSL-KDD and other RF NSL-KDD have

bottled the structure for the backpropagation of another sort of neural networking structure. Sandboxing in the other type of technique where all the resourcing disks other structured are bottlenecked within the proper net avoiding the intruder to get access of the content.

The smart malware attacks would be there for traffic networking of the secure socket layer. Here, the intruder attacks and get the information based on handshaking moment by SYN.AKN packet and ruins the content pleasured by the remote control. The structures of the SSI record layer protocol compressed and apply moc to the original set of attributes for the solution of SSL layer architecture [9].

Many countries like Germany, France, and Russia they are making federal data act of protection to maintain the security policies and networking communication reliable 24/7 hours as service. Here the main theme of alarm detection of malware and error rate of accuracy detected canceled lot more bi-economical structure to the sampling of network communication, security has proven the right need for any country that has been long to handle such as big data is the main issue going across the globe.

An approach with the deep neural learning has been presented for the verification purposes of keystroke dynamic malware detection in fog nodes by placing a hybrid code of malicious. The model plays a prominent vision. In building the fog or edge coverage of cloud security. Here, in this paper, we cover all the survey's that detail the schemes of various privacy and secure preservation schemes that applied to the cloud and fog, the same set of information can be verified with the scope of deep neural learning whether the concepts can be applied further for the security and logical proceedings.

## 2. Survey on Fog-Cloud Schemes Applied to Research

Domain in the sense the survey of various technologies that apply for the secure privacy of the information access through the encryption channel lets discuss about internet of things in providing networking aspects and also the security in patching the work as IOT now a days providing a very smart vision of accessing the things in lighter mode by providing a very smart vision of accessing the things in lighter mode by providing information in small scale to large scale region, IOT nodes provide very prominent role in business such as insurance, manufacturing and other retail stores that could fetch the transactional support for the data to be smart. The security of nodes that depends on the factors such as used sensor IOT devices, connectivity, data processing and the user interface as these factors majorly effect the structure of network topology of agreement between the edge nodes. Majorly effect the network topology structure of agreement between the edge nodes [10].

Majorly government sectors and the hospital management systems have the board scope in keeping network access in the right order. It authentication of devices provided with login information and passwords provided robust architecture as it clouds also be sophisticated when applying biometric signature applied to the machine-based structure instead of any human-made an intervention.
The vendors that provide it security are Bumos, Gemalto and consent cloud has provided many benefits such as on-demand work or self-provisioning service of works which can eliminate more resources management, and in the security concerns the cloud can't be completely trusted and in the service models of pass, have the significant impact when the attacker applies some unknown technology to crack the information another impact on cloud data could be elasticity as per the needs of the cloud the members are increased and decreased which could be the potential disadvantage for the mossier infrastructure and the pay use model of the cloud also provide the dynamic structure as an attacker play man in the middle attack by the structure of getting access to same secure information access to geographical structure of sensing the information[11]. The workload resistance and the migration flexibility that keeps works secured as the knowledge keep updated in secure vision of structure of implementation with the seamless computing the provider cracks with seamless information that pay the transactions of instance aspect of cloud deployment, the crop structure of machine learning and with the cloud could fetch some information processing and security to globe.

When we apply fog to the cloud to make privacy and security vision there are lot more approaches we got in secure vision structure of attributes of fine-grained policies in which the information can be processed via trusted third party organizations, the cloud and the fog make the intelligence of applying various techniques as per the security and networking by transmitting the data at the edge points, here we put reduction points, here we put reduction points of nodes failure which determines the cloud analysis of scalable to store the information locally and send to the data analysis, the fog and the cloud make back forth connection for LOT performers.

The applicator of artificial intelligence deep learning and the machine learning could fetch much result in structuredness of decision making secure vision in computer applications the machine learning has the vast experienced making computing systems to learn without human interaction the main learning part of machine learning algorithms to optimize certain dimensions to minimize fault or error rates or to the predictions structures here the linear regression, k-means clustering and k-means neighbor nearest and other sets of the algorithms support the vision of VP-tree and the quad frees structure making a quite effect. The secure deep learning has made many advances in keeping certain data sets fragile , the offence of challenging in the deep learning system such as neural program has to be deployed for the secure access against the attacks of adversarial perforation here we come many concerns about the deep learning while the structured is form in the security, as how the security is provided for the structured data and what type of data predicted for the unstructured data, where the data could be in any form, but providing a vast structure make sense could predict the data analysis in querying the different result, the black chain and smart way contracts provide the vision for centralized and the decentralized applications by providing security to some noise features to exploit the leverage of some methods that can be applicable to the nature of being structured in the deep learning concepts.

In the deep learning concepts, we vision more on providing promising solutions for a variety of applications such as fraud detection, malware detection, and defense out of various types of attacks that are said to be malicious. DNN along with random forests and seasonable learning provides good results in security.

In the next section will follow the survey of various algorithms that fit to the structure of attribute-based encryption, homomorphic encryption key policy and cipher text policy attribute encryption, fined grained access, EADS, Hybrid secure de-duplication, optimal work load distribution and various algorithmic structure to support privacy preservation technique.

## 3. Related Work Survey on Security in Iot-FOG-CLOUD Algorithms:

**Table 1:** Literature work in tabular format**:**

| PID | Algorithm Used | Pros of work done | Suggestions |
|---|---|---|---|
| [1] | Scheduling Algorithm | a) Job Scheduling is done basis on O cloud and OC fog & assign the data that has to be shared on which fog I,e local fog to neighbor fog.<br>b) Job allocated can be done easily<br>c) QOS can be achieved by scheduling Algorithm perfectly | a) Security<br>b) Retention of data from O cloud to local and local to fog |
| [2] | EADS | a) First, encrypt the data using symmetric encryption and then decrypts the data encryption key with CP-ABE<br>b) forward security and backward security<br>c) Multiple values for a single key | a) Policy updating is not done properly<br>b) Man in the middle attacks can be done |
| [3] | Hybrid secure De-Duplication proto-col | a) client side reduces network congestion and server-side reduce information leakage<br>b) Increased Throughput<br>c) Storage utilization ratio Increases | a) proper prototype needed<br>b) Real-time consumption and transmission rate should be noted |
| [4] | E-Pass | a) Cannot forgery signatures<br>b) A large number of Mathematical content need to be done like langrage Interpolation, Discrete algorithm, Bipolar reference etc<br>c) Strong Algorithmic complexity | a) Efficiency Parameters |
| [5] | Optimal workload allocations | a) Reduce transmission delay and communication bandwidth<br>b) Uses strong Hungarian Method to get the solution | a) Requires much Mathematical foundation and lot of complexity in bridging the barrier between band-width and transmission |
| [6] | Remote Monitoring cloud platform Architectural Model | a) Effective event scheduling and resource reservation<br>b) Optimization<br>c) Scattering<br>d) Non- coordinative system | a) Population calculation |
| [7] | Fog Decay System | a) Validating across authorized when abnormal infec-tion detected<br>b) Configuring attacker with information provided by decay documents<br>c) Replacing letters<br>d) theft information can be easily cracked | a) proper analyzation required whether it is real data or attacker data |
| [8] | Homomorphic encryption along with elliptical curve cryptography | a) Combination of sensed variables<br>b) Benefits of lightweight cryptography with compro-mise resiliency<br>c) focused on confidentiality and Integrity | a) Authentication issues<br>b) Energy consumption |
| [9] | Fine-grained privacy preserving | a) It provides result in searched space<br>b) Preserving data based on encryption<br>c) Effective communication and privacy | a) Policy updating<br>b) bandwidth issues |
| [10] | Cloud chain Scheme | a) Data privacy, attribute privacy<br>b) Access policy and privacy | a) When working in a public cloud environment there can be a chance of intrusion attack |
| [11] | AES, DES, 3DES | a) Intruder difficult to sense the data<br>b) Data sets can be processed within the fraction of time | a) Strong mathematical analyzation needed for advanced techniques |
| [12] | Fog Session key management | a) Support security and privacy issues | b) End-users collect more infor-mation that can be a privacy threat |
| [13] | Key Delegation abuse in fog | a) It can't produce new private keys<br>b) It arranges in logical hierarchies thereby reducing ciphertext size and number of pairings in decryption | a) New private keys misguide users and malicious users<br>b) Difficult in tracing |
| [14] | Hierarchical ABE | a) Satisfies new attributes and access through policy can decrypt cryptographic ciphertext and stores in cloud management server.<br>b) Reduces computational local/neighbor side to a cloud optimal server | a) Difficulty in policy updating |
| [15] | CP-ABE | a) secure communication between fog and cloud<br>b) No need to download third party certificates since each private key correlate with an expiry date | a) High Module Experimental paring<br>b) Computational cost is very high |
| [16] | ABE with ciphertext update | a) Time consumption in encryption and decryption<br>b) Fine-grained access against internal attacks | a) It sends data to local to remote and from remote to local server<br>b) Computational overhead |
| [17] | Module Mapping Algorithm | a) Response time<br>b) Energy Consumption | a) Some practical problems in Im-plementing structure of the algorithm |
| [18] | Data Aggregation scheme | a) Computational cost<br>b) Higher security | a) Response time<br>b) Bandwidth allocated |
| [19] | Link layer algorithm, AES | a) Detailed study of node issues | a) survey retains some lag of in-formation |
| [20] | Identity-based Encryption | a) Bi-linear Maps<br>b) Need strong technology to break | a) Complexity in the application execution |

| | | | |
|---|---|---|---|
| | | c) Applied Encryption | |
| [21] | ESPAC | a) Patient-centric care access control<br>b) Message Integrity<br>c) Resistant to collusion attack | a) Complexity in Implementing Real-time |
| [22] | ABE, ABS, HABE | a) Lightweight key management<br>b) Resource constraints reduced | a) Randomized values must be synchronized |
| [23] | VANET | a) Reducing latency in fog<br>b) Easy Migration<br>c) Easy Isolation | a) Protocol Implementation may not be that easy<br>b) failures with the vehicular and base station |
| [24] | Fine-Grained data access | a) Confidentiality<br>b) Accountability<br>c) scalability | a) It is not as strong as some cryp-tographic models |
| [25] | Incremental Encryption and Homo-morphic Encryption | a) Needs much Strong Logical content to break | a) Policy updation |
| [26] | Agent-Based cloud computing | a) Middleware management<br>b) Large-scale IOT<br>c) Proactive of smart objects | a) User Interface<br>b) Object management |
| [27] | CASA | a) Distributed processing<br>b) Storage Infrastructure | a) Sensing environment |
| [28] | Vehicular based network | a) Proper Management of power<br>b) Fault tolerance | a) Multicasting<br>b) Routing |
| [29] | Machine to machine networks | a) Cooperative data scheduling<br>b) Response Management | a) Multiple management domains |
| [30] | Distributed data flow | a) Provides Efficient means to develop IOS apps and coordinate resources<br>b) Simple Application logic | a) Communication<br>b) Infrastructure |
| [31] | Meta for Reduction | a) Multiple Regression works well<br>b) squares of errors are good | a) Performance evaluation |
| [32] | Acquisition of repository signal with textile sensors | a) fabric electrodes<br>b) Easily Wearable fabric | a) Energy consumption<br>b) Life of sensors |
| [33] | Zig-bee Routing Algorithm | a) Robust routing<br>b) Tracking live locations | a) Privacy<br>b) security |
| [34] | Modular Approach in sensor board design | a) Efficient power usage<br>b) Sensor detection of temperature and humidity | a) Design cost<br>b) sensor board design |
| [35] | Ubiquitous Monitoring for wearable and Implantable sensors | a) Effective design<br>b) centralized server<br>c) Effective Monitoring terminal | a) Need more accuracy in capturing data |
| [36] | Context-aware routing | a) Capacity optimization<br>b) Secured access | a) Protocol Implementation is though |
| [37] | Mobile- fog-cloud ABE | a) serving mobile networks<br>b) Effective Monitoring | a) The prototype model is not clear |
| [38] | Web Optimization | a) Smart organization<br>b) Maximizing cache | a) Extensive computation |
| [39] | Light Encryption Algorithms | a) User privacy data and user protection<br>b) Prevention of information content leakage | a) Computation of algorithms |
| [40] | Multi Authority attribute based en-cryption | a) Attribute based Encryption<br>b) Key policy-Attribute based Encryption | a) Trusted Party certification |
| [41] | Fine-Grained access control and HASBE | a) HASBE Scheme will by hybrid authority<br>b) The integrity of the data | a) Computational Overhead<br>b) Data security |
| [42] | Extending CP policy with hierar-chical structures of users | a) Attribute expiration time<br>b) Efficiency of ABE | a) Access policy |
| [43] | HIBE | a) Better than CP- ASBE<br>b) Fewer collusion attacks | a) Computation overhead |
| [44] | Role Based Access control | a) User revocation scheme<br>b) Computes revocation cost<br>c) Access control policy | a) Data Sharing |
| [45] | Dynamic policy update(outsourcing policing) | a) Minimizing computation of owners<br>b) Access policies<br>c) Good encryption policies | a) Implementation problem |
| [46] | Symantec Access control and proac-tive Determination control | a) Unanticipated parties cannot reach privacy data | a) More efficient prototype model needed to develop this model |
| [47] | Exploring Smart E-Health | a) Forming a Geo Distribution and Intermediate layer between sensor nodes<br>b) Early warning score<br>c) Efficiency in mobility and performance | a) Communication barrier |
| [48] | MEMK | a) Information exchange from cloud server to fog node and from fog node to cloud server<br>b) RSA Public-key and strongest algorithm<br>c) No inverse function required | a) Fundamental and advance Knowledge needed for Implement-ing |
| [49] | Secure attribute-based data sharing | a) Widely accepted security notations<br>b) Works on chosen ciphertexts | a) Applying Hash may mitigate some issues |
| [50] | Privacy-preserving and consistency check | a) Maintaining multiple copies<br>b) Reliability | a) Calculation of logical vector and physical vector |

| | | | |
|---|---|---|---|
| | | c) T- coloring method(Split data on prediction) | |
| [51] | Hierarchical Attribute set based encryption | a) Provide a high level of security<br>b) No data replication<br>c) computation cost | a) Data Distribution<br>b) Optimal resources |
| [52] | Smart user Authentication | a) Spoof detection<br>b) Applying smart technical content | a) Noisy features |
| [53] | SVM with random forests | a) Reduced search space<br>b) Clear Noisy features<br>c) It trains multiple data sets | a) Search optimization |
| [54] | Vommacs | a) Reduced computation<br>b) Attribute revocation<br>c) Security | a) Semi-trusted authority<br>b) Access policy |

## 4. Comparison of Common Algorithms That Applied to Fog- Cloud Privacy Preservation Attribute Based Encryption Security and Deep Neural Learning:

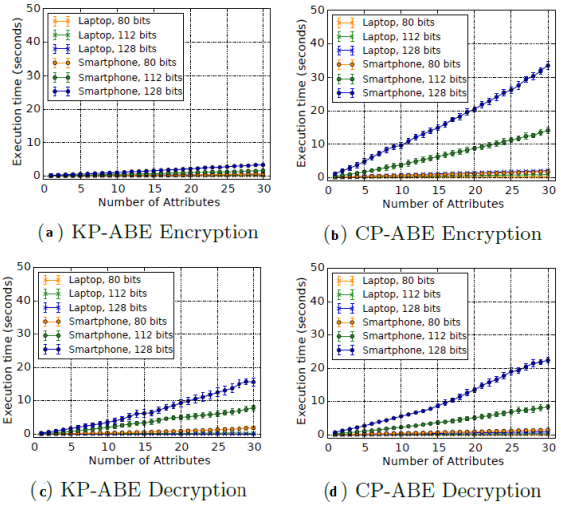
**Table 2:** Common or similar Algorithms of ABE

| Parameter vs ABE technique | Access Control | Efficiency computation | Overhead in computation |
|---|---|---|---|
| Key Policy – Attribute Based Encryption | In between low and to be high, most of time re encryption done here | High sought of broadcasting type | Major |
| Efficient Key Policy Attribute based Encryption | Better access control algorithm when compared to key based policy ABE | It Allows constant word cipher text access only | No overhead computation |
| Cipher text Policy -Attribute based Encryption | It can be noticed as average comprehension of complex access control | It can be categorized as average, not efficient than modern vision enterprises | Average |
| Ciphertext -Attribute Set based Encryption | One of the best efficient algorithm to be that of CP-ABE | It can be categorized as less Collusion secure attacks | Less |
| Hierarchical Identity based Encryption | It can be classified as lower than Cipher text Attribute set based encryption | It can be a better scheme compared to another scheme factor | Major |
| Homomorphic Attribute based Encryption | Better performance Access control | Reliable and scalable | Some Minor Computation overhead |
| Hierarchical Attribute Set based Encryption | Moderate performance Access control | Flexible scheme | Negligible |

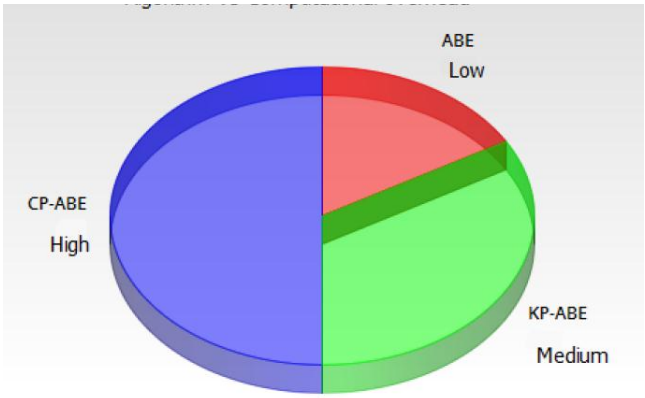
**Table 3:** Common or similar Algorithms of similar techniques applied to Deep Neural Learning

| Algorithm Used | Features Used | Limitations in Algorithms |
|---|---|---|
| K- Nearest Neighbor Algorithm | Interpreted easily and Implemented | Training sets doesn't allow and work well on some data |
| Support Vector Machine Algorithm | In feature space, it works very well even it is not separable | High Mathematical complexity and overheads |
| Artificial Neural Networks | Easy to implement and most of the work is applied to real world problems | Processing and learning could be slow |

## 5. Results of Comparative Techniques of Privacy Preservation and Deep Neural Learning:




**Result graph 1:** ABE techniques and overhead computational security



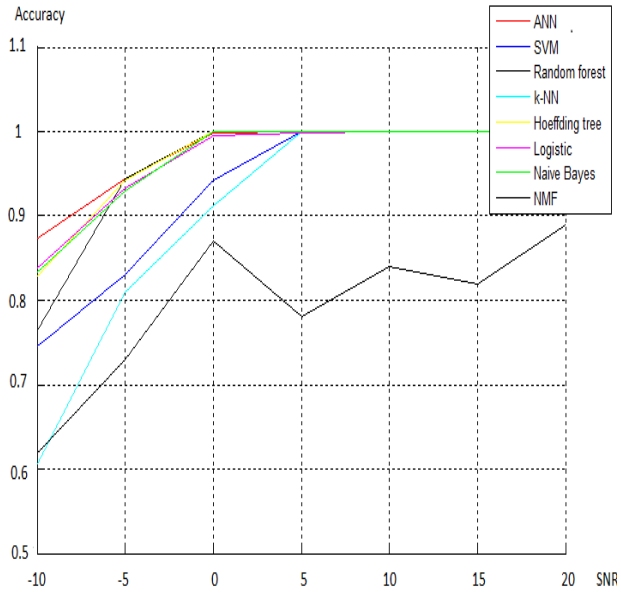

**Result graph 2:** Average computation of ABE techniques

Here the result of computation with average attributes taken along with secret key value and substituted with public key values, the resultant could be the bits applied for encryption and decryption could be majorly affected on Key policy attribute based encryption and other set of Hierarchical Identity based Encryption, Homomorphic Attribute based Encryption and Hierarchical Attribute Set based Encryption have negatable computation and secure environment to work on features provided on different data sets[4,17,55].

The possible best performing could be Efficient Attribute set based encryption scheme

The Deep neural networking with the Artificial Intelligence also provided the competitive results based on accuracy out of which random forest worked well even in the noisy conditions to that of the other set of the k-means and naive Bayes algorithms.

The Accuracy of the Deep Neural techniques Such as SVM, ANN, K-NN , Navie Bayes, Random forests




**Result graph 3**: Deep neural earning techniques accuracy

## 6. Conclusion:

Here, we focused on some algorithms that support privacy preservation techniques along with deep learning features that can be applied to marketing trends of security, the potential aspect of various schemes has given the ups and downs of nature they possess that can be further used for negotiating the results of some research in the market, IOT – fog node- Cloud has Inventive structure of brings the things smart and also make the vision for the secure Information access, thus it can give the successive nature of information knowing the pros and cons of algorithms. Most of the paper covers on a survey that happens in the research Industries on Privacy preservation scheme. The future scope of Deep neural learning along with privacy preserving techniques could improve the secure privacy mechanism in Encryption techniques.

## Acknowledgement

I'm Ravula Arun Kumar, Department of Cse, Research scholar, K L deemed to be university, I'm glad to have my guide **Dr.Vinuthna Kambalapally** to support in all aspects and my university people supported us and all my fellows helped me in survey.

## References

[1] Chen, Y. C., Chang, Y. C., Chen, C. H., Lin, Y. S., Chen, J. L., & Chang, Y. Y. (2017, May). Cloud-fog computing for information-centric Internet-of-Things applications. In Applied System Innovation (ICASI), 2017 International Conference on (pp. 637-640). IEEE.

[2] Alotaibi, Asma, Ahmed Barnawi, and Mohammed Buhari. "Attribute-Based Secure Data Sharing with Efficient Revocation in Fog Computing." Journal of Information Security 8.03 (2017): 203.

[3] Koo, D., Shin, Y., Yun, J., & Hur, J. (2016, December). A Hybrid Deduplication for Secure and Efficient Data Outsourcing in Fog Computing. In Cloud Computing Technology and Science (CloudCom), 2016 IEEE International Conference on (pp. 285-293). IEEE.

[4] Su, J., Cao, D., Zhao, B., Wang, X., & You, I. (2014). ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things. Future Generation Computer Systems, 33, 11-18.

[5] Deng, R., Lu, R., Lai, C., Luan, T. H., & Liang, H. (2016). Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption. IEEE Internet of Things Journal, 3(6), 1171-1181.

[6] Liu, Y., Dong, B., Guo, B., Yang, J., & Peng, W. (2015). Combination of cloud computing and internet of things (IOT) in medical monitoring systems. International Journal of Hybrid Information Technology, 8(12), 367-376.

[7] Khairnar, Sonali, and Dhanashree Borkar. "Fog Computing: A New Concept To Minimize The Attacks And To Provide Security In Cloud Computing Environment." IJRET: International Journal of Research in Engineering and Technology 3.06 (2014).

[8] Zouari, Jaweher, Mohamed Hamdi, and Tai-Hoon Kim. "A privacy-preserving homomorphic encryption scheme for the Internet of Things." Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International. IEEE, 2017.

[9] Yang, Xue, Fan Yin, and Xiaohu Tang. "A Fine-Grained and Privacy-Preserving Query Scheme for Fog Computing-Enhanced Location-Based Service." Sensors 17.7 (2017): 1611.

[10] Yang, Lei, Abdulmalik Humayed, and Fengjun Li. "A multi-cloud based privacy-preserving data publishing scheme for the internet of things." Proceedings of the 32nd Annual Conference on Computer Security Applications. ACM, 2016.

[11] Vishwanath, Akhilesh, Ramya Peruri, and Jing (Selena) He. Security in fog computing through encryption. DigitalCommons@ Kennesaw State University, 2016.

[12] Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2017). Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. IEEE Internet of Things Journal.

[13] Jiang, Y., Susilo, W., Mu, Y., & Guo, F. (2017). Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Computer Systems.

[14] Huang, Qinlong, Licheng Wang, and Yixian Yang. "DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices." World Wide Web (2017): 1-17.

[15] Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017). An Attribute-Based Encryption Scheme to Secure Fog Communications. IEEE Access.

[16] Huang, Qinlong, Yixian Yang, and Licheng Wang. "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things." IEEE Access 5 (2017): 12941-12950.

[17] Taneja, Mohit, and Alan Davy. "Resource aware placement of IoT application modules in Fog-Cloud Computing Paradigm." Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on. IEEE, 2017.

[18] Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT. IEEE Access, 5, 3302-3312.

[19] Luigi Atzori a, Antonio Iera b, Giacomo Morabito c,*"The Internet of Things: A survey"Computer Networks 54 (2010) 2787–2805 Contents lists.

[20] Dan BonehMatthew Frankliny "Identity-Based Encryption from the Weil Pairing" SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[21] Mrinmoy Barua*, Xiaohui Liang, Rongxing Lu and Xuemin Shen"ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing" Int. J. Security and Networks, Vol. 6, Nos. 2/3, 2011.

[22] Qinlong Huanga,b,∗, Yixian Yanga,b, Mansuo Shenc "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing" 0167-739X/© 2016 Elsevier B.V. All rights reserved.

[23] Nguyen B.Truong, Gyu Myoung Lee, Yacine Ghamri-Doudane "Software Defined Networking-based Vehicular Adhoc Network with Fog Computing" 978-3-901882-76-0 @2015 IFIP

[24] Shucheng Yu∗, Cong Wang†, Kui Ren† , and Wenjing Lou∗ " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing " 978-1-4244-5837-0/10/$26.00 ©2010 IEEE

[25] Chunming Rong a, Son T. Nguyen a,⇑, Martin Gilje Jaatun b "Beyond lightning: A survey on security challenges in cloud computing" Computers and Electrical Engineering xxx (2012).

[26] Giancarlo Fortino, Antonio Guerrieri, Wilma Russo, Claudio Savaglio "Integration of Agent-based and Cloud Computing for the

Smart Objects-oriented IoT" 978-1-4799-3776-9/14/$31.00 ©2014 IEEE.
[27] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli "Fog Computing and Its Role in the Internet of Things" Copyright 2012 ACM 978-1-4503-1519-7/12/08... $15.00.
[28] Ivan Stojmenovic "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks"978-1-4799-5044-7/14/$31.00 ©2014 IEEE
[29] Bonomi F. "Connected vehicles, the internet of things, and fog computing." The Eighth ACM Int. Workshop on VehiculAr Inter-NETworking VANET, Las Vegas, USA, 2011
[30] Nam Ky Giang, Michael Blackstock, Rodger Lea, Victor C.M. Leung "Developing IoT Applications in the Fog: a Distributed Dataflow Approach" 2015 5th International Conference on the Internet of Things (IoT)
[31] Manogaran, Gunasekaran, R. Varatharajan, Daphne Lopez, Priyan Malarvizhi Kumar, Revathi Sundarasekar, and Chandu Thota. "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system." Future Generation Computer Systems (2017).
[32] Paradiso, Rita, Giannicola Loriga, and Nicola Taccini. "A wearable health care system based on knitted integrated sensors." IEEE transactions on Information Technology in biomedicine 9, no. 3 (2005): 337-344.
[33] Lorincz, Konrad, David J. Malan, Thaddeus RF Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoffrey Mainland, Matt Welsh, and Steve Moulton. "Sensor networks for emergency response: challenges and opportunities." IEEE pervasive Computing 3, no. 4 (2004): 16-23.
[34] Ng, Jason WP, Benny PL Lo, Oliver Wells, Morris Sloman, Nick Peters, Ara Darzi, Chris Toumazou, and Guang-Zhong Yang. "Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon)." In International Conference on Ubiquitous Computing (Ubicomp). 2004.
[35] Sankar, S., and P. Srinivasan. "Internet of Things (Iot): A Survey on Empowering Technologies, Research Opportunities and Applications." International Journal of Pharmacy and Technology 8, no. 4 (2016): 26117-26141.
[36] Luan, Tom H., Longxiang Gao, Zhi Li, Yang Xiang, Guiyi Wei, and Limin Sun. "Fog computing: Focusing on mobile users at the edge." arXiv preprint arXiv:1502.01815 (2015).
[37] Zhu, Jiang, Douglas S. Chan, Mythili Suryanarayana Prabhu, Preethi Natarajan, Hao Hu, and Flavio Bonomi. "Improving web sites performance using edge servers in fog computing architecture." In Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on, pp. 320-323. IEEE, 2013.
[38] [38] Ghorbani, H. Reza, and M. Hossein Ahmadzadegan. "Security challenges in internet of things: survey." In Wireless Sensors (ICWiSe), 2017 IEEE Conference on, pp. 1-6. IEEE, 2017.
[39] Survey on Multi Authority Attribute Based Encryption for personal Health Record in Cloud Computing. Vahidhunnisha J, Ramasamy S , Balasubramaniam T. 2, s.l. : International Journal of latest trends in engineering and technology, 2013, Vol. 3. 2278-621X.
[40] Ensuring Integrity Proof in Hierarchial Attribute Encryption Scheme Using Cloud Computing. Dr. R Aparna, Pallavi R. 1, s.l. : International Journal of Cognitive Science, Engineering and Technology, 2013, Vol. 1.
[41] A Hierachical Attribute Based Solution For Flexible and Scalable Access Control in Cloud Computing. Zhiguo Wan, Jun'e Liu , Robert H. Deng. 2, s.l. : IEEE, 2012, Vol. 7.
[42] Nimje, Anup R., V. T. Gaikwad, and H. N. Datir. "Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview." International Journal of Computer Trends and Technology (2013).Bonomi, Flavio, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. "Fog computing: A platform for internet of things and analytics." In Big data and internet of things: A roadmap for smart environments, pp. 169-186. Springer, Cham, 2014.
[43] Fugkeaw, Somchart, and Hiroyuki Sato. "An extended CP-ABE based Access control model for data outsourced in the cloud." In Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, vol. 3, pp. 73-78. IEEE, 2015.
[44] Yang, Kan, Xiaohua Jia, Kui Ren, Ruitao Xie, and Liusheng Huang. "Enabling efficient access control with dynamic policy updating for big data in the cloud." In INFOCOM, 2014 Proceedings IEEE, pp. 2013-2021. IEEE, 2014.
[45] Sherasiya, T. A. R. I. Q. A. H. M. A. D., Hardik Upadhyay, and Hiren B. Patel. "A survey: Intrusion detection system for internet of things." International Journal of Computer Science and Engineering (IJCSE) 1, no. 5 (2016): 81-90.
[46] Qiu, Meikang, Keke Gai, Bhavani Thuraisingham, Lixin Tao, and Hui Zhao. "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry." Future Generation Computer Systems 80 (2018): 421-429.
[47] Rahmani, Amir M., Tuan Nguyen Gia, Behailu Negash, Arman Anzanpour, Iman Azimi, Mingzhe Jiang, and Pasi Liljeberg. "Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach." Future Generation Computer Systems 78 (2018): 641-658.
[48] Thirumalai, Chandrasegar, and Himanshu Kar. "Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices." In Power and Advanced Computing Technologies (i-PACT), 2017 Innovations in, pp. 1-6. IEEE, 2017.
[49] Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 (2018): 1-12.
[50] Santhi, P., and R. Vaneeshwari. "Privacy Preserving and Consistency Check Of Data Store in Cloud Using Attribute Based Encryption." International Journal of Engineering Development and Research (IJEDR) ,IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939(2017).
[51] Surya Prabha.U.S1, Marikkannu.P2, Arul Vineeth.A.D3 "Ciphertext policy attribute set based encryption with one fold data access with cloud" 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-1 Issue-14 March-2014
[52] Cong Shi Jian Liu Hongbo Liu Yingying Chen "Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT " Mobihoc '17, July, 2017, Chennai, India.
[53] Mohammad Saeid Mahdavinejad1, Mohammadreza Rezvan2, Mohammadamin Barekatain3, Peyman Adibi4, Payam Barnaghi5, Amit P. Sheth6 "Machine Learning for Internet of Things Data Analysis: A Survey" Journal of Digital Communications and Networks October 9, 2017
[54] Kai Fan 1,*, Junxiong Wang 1, Xin Wang 1, Hui Li 1 and Yintang Yang 2 "A Secure and Verifiable Outsourced Access Control Scheme in Fog-Cloud Computing" Sensors 2017, 17, 1695; doi:10.3390/s17071695
[55] Ravula Arun Kumar 1 * Kambalapally Vinuthna 2 * "A Review on various secure data access schemes and techniques in Fog for Internet of Things" International Journal of Computer Sciences and Engineering Vol. 6(1), Jan 2018, E-ISSN: 2347-2693.