Smart Intelligent Computing and Communication Technology
V.D. Ambeth Kumar et al. (Eds.)

doi:10.3233/APC210045

Attaining Cloud Security Solution Over Machine Learning Techniques

K.Muthulakshmi[a,1] and Dr.K.Valarmathi[b]
[a]*Research scholar, Anna University, Chennai, India*
[b]*Associate Professor, Panimalar Engineering College, Chennai, India*
[c]*Professor, Dept of CSE, Panimalar Engineering College, Chennai, India*

Abstract. Cloud computing provides physical and logical computation resource on demand for the set of service. Cloud environment reduce the infrastructure cost and easy to use without any extra burden. Cloud storage an access raised the several security issues like data privacy, access control, authentication, virtual machine security, web security etc., In one side hackers, breaches, cloud security issues and threats get expanded. But in another side many technologies are keep increased to secure cloud data. Technology may be cryptographic technique, anonymization technique, machine learning technique etc., In this paper we analyse cloud computing basics, models, machine learning technique and some security solution through machine learning technique such as support vector machine (SVM), K-Nearest Neighbour (KNN), Decision tree and Naïve Bayes classifier technique.

Keyword. Cloud, security, machine learning, SVM, KNN, Naïve Bayes.

1. Introduction

Cloud computing is one of the most influential and relatively new technologies in our lives. With this technology, you can access computer resources and facilities at any time [1]. The healthcare industry is constantly evolving and can provide information on future healthcare models. Businesses can use cloud technology to manage changes and issues. This healthy technology facilitates communication, cooperation and coordination with various health care providers [2][3].This is a new digital technology model that is often used in the healthcare sector. It not only processes medical information, but also facilitates the sharing or exchange of medical information between different partners [4]. In the age of big data, comprehensive health information improves the performance of cloud networks, which improves not only infinite data but also their internet. In the field of health care, electronic health records (EHRs) face many challenges related to privacy and unauthorized access, but information security and security are one of the most important of these challenges [5][6].

[1]K.Muthulakshmi, Research Scholar, Dept of CSE, Anna University, Chennai, India. Email:muthulakshmi@gmail.com[1]

There are risks ranging from warehouse recovery attacks that affect the security and confidentiality of medical data to effective attacks on distributed denial of service (DDOS) [7]. A cyber-attack activated through a recovery plan has far more consequences than financial loss and violation of personal life. Current privacy policy is not sufficient to ensure proper e-health cloud computing. The greatest danger to medical records provided in the cloud is the internal attacks of individuals with company evidence, which is far worse and more dangerous than external attacks [8][9]. This study aims to provide an in-depth review of the strengths and weaknesses of health care in EHR attacks. EHR contains a lot of confidential and sensitive information that is different from patient information and financial information, which not only displays the patient's tactical information in the event of a leak, but also causes financial loss. [10].

2. Background study

2.1 Cloud Computing

Cloud computing is a technology which provide access to the shared resources like CPU, Hard disk, Network devices those resource automatically assigned with minimum administrative task. It delivers many computing services like Servers, Databases, Storage, Analytics Networking etc., cloud security is protect cloud data, application & infrastructure from threats.

2.2 Cloud Service Model

Cloud provide3 types of services.

IAAS – Fundamental resources, physical M/C, Virtual storage are access though infrastructure as a service. It provides all services via server visualization. Customer can access resource of computing via administrature access to VM.PAAS – It provide deployment and development tool to develop runtime application administration task is taken care by cloud providers depending upon function of platform. The types may be application, stand alone, open platform and addon development.SAAS – It consider application as a service to the end users. It requires low deployment cost, less vendor, it provide more robust solution.

2.3 Cloud Security

Cloud security contains set of contols, technologies, procedures and policies will work together to protect cloud based storage system. Cloud provider take care of cloud security delivery. Cloud data security is more important when we move our sensitive data towards cloud storage. Selecting right cloud security solution depending upon application is a major task.

2.4 Cloud Security Threats

1. Data loss / Leakage

Data loss is the serious cloud security count nearly 69% organisation points. This issue data gets shared using public link.
2. Data Breaches
This threats is still number one ranking in the survey. It cause financial and reputational damage.
3. Misconfiguration and inadequate change control.
Accidently business data gets exposed via the cloud.
4. Lack of cloud security architecture and strategy
5. Insufficient identity, credit access and key management – Lack of credential and key management
6.Account Hijacking-The account may be hacked and data get steeled.

2.5 Machine Learning

Machine learning is a technique which progressively improve the model or set of task given.Some task are assigned to machine. The machine will learn from its experience by getting more experiment. The machine takes decision, prediction or forecasting based on set of input is given. Supervised learning is a machine learning method which trains the machine towards labelled data i.e known output. It has two categories.
Classification – a classification is used to classify depends on input parameter into one category
Regression – a regression is used to classify the input into output variable as real values.
Types of Supervised learning
1) Regression – It is a supervised learning technique which is used to find correlation between variables and continuous output variable. This technique is mainly used to predict whether using temperature or other factors and also predict market trends. Linear regression, Logistic regression, polynomial regression is different kind of regression technique.
2) Classification – It is a supervised learning technique which categorized the training input data. The out put category may be classes or group. Binary classifier, multi class classifier are types of classification.
3) KNN (K-Nearest-Neighbour) – It is a supervised learning technique which shows the available data. New data points are classified based on the nearest similar value. It is the most effective technique for larger dataset.
4) SVM (Support Vector Machine) – It is a popular supervised learning technique. SVM creates decision boundary best line called a hyper plane which is used to segregate categories of input variable into output category. SVM mainly used for text categorisation, face detection, image classification. There are two type of SVM. Linear SVM and Non-Linear SVM.
5) Naïve bayes classifier – It is a supervised learning technique based on Bayes theorem. It use probability to classify the object. Sentimental analysis, spam filter is popular example of naïve bayes classifier. There are three types of naïve bayes models, Gaussian, multinomial and bernoulicalssifer. Unsupervised learning is a type of machine learning technique. It find the hidden pattern from the input data set. It is a model which trained using unlabelled dataset. It makes machine to think like a human. There is no training for the machine.
Clustering is the method used to group similar object. Analysis can be done for the clustered object.

Association – It is used to find similarity between two objects. Market basket analysis is the popular example of association.

3. Machine Learning Algorithm in Cloud Security

3.1. SVM(Support Vector Machine)

Personal health care information and medical record are stored in cloud. The above field must give more concentration to protect and give security in the cloud. Support vector machine is a efficient method for data protection and image segmentation of medical record.

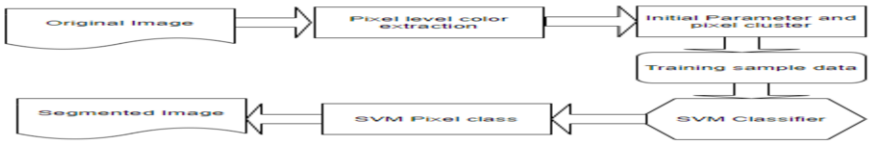

Figure 1: Support Vector Machine using pixel color extraction

The medical record original image gets extracted by using pixel color level. This extracted output is given to input of SVM for classification. It maximises prediction accuracy. SAAS –is a efficient model to give solution for health information technology. Medical data gets divided into pixel color. Cloud provider could not access medical data without owner knowledge[12].

3.2 KNN- K-Nearest Neighbour

Data classification is the important procedure for giving cloud data security. Data classification must do proper information filtering with specific data sensitivity and requirements of security level. The data may be public, sensitive, non-sensitive, highly confidential etc., Traditional KNN has low proficiency in data filtration.

TSF – KNN (Training Set Filtration Key Nearest Neighbour) – Algorithm is integrating with KNN for data secured management procedure classification. TSF KNN is used to secure mobile cloud computing model and classify the data as public data or non-confidential data, highly confidential or top classified data. [13]

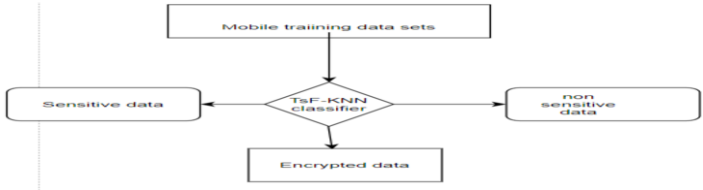

Figure 2: TsF-KNN

3.3 Decision tree

Decision tree machine learning classifier technique are widely used in text classification, health care, remote diagnostic etc., Cloud service provider host decision

tree model to the cloud server. C4.5 algorithm mainly deal with noise and produce different decision tree. DT-TSVM (Decision Tree Twin Support Vector Machine) – Using this model encrypted training data set gets classified in secure manner.

3.4 Naive Bayes Classifier

Medical data are stored in cloud. The data are trained by using Naïve Bayes classifier technique without leaking any patient record. Patient details should not leaked out during the disease diagnosis phase. The trained data from Naïve Bayes classifier is sent to cloud provider for storage. Some homomorphic cryptographic tools are used for secure aggregation of medical record[24].

4. Conclusion

In this paper we analyse and review the cloud security basic, threats, machine learning technique and cloud security solution through machine learning technique. Finally we conclude machine learning technique attract the academic scholar and play a important role in sensing threats and occurrences.

References

[1] Chadwick, D.W. and Fatema, K., A privacy preserving authorisation system for the cloud. Journal of Computer and System Sciences, 78(5), pp.1359-1373, 2012

[2] Karadsheh, L., Applying security policies and service level agreement to IaaS service model to enhance security and transition. computers & security, 31(3), pp.315-326, 2012.

[3] Suthar, K. and Patel, J., Encryscation: An secure approach for data security using encryption and obfuscation techniques for iaas and daas services in cloud environment. In Proceedings of International Conference on Communication and Networks (pp. 323-331). Springer, Singapore, 2017.

[4] Liu, X., Zhang, Y., Wang, B. and Yan, J., Mona: Secure multi-owner data sharing for dynamic groups in the cloud. IEEE transactions on parallel and distributed systems, 24(6), pp.1182-1191, 2012.

[5] Xu, H., Guo, S. and Chen, K., Building confidential and efficient query services in the cloud with rasp data perturbation. IEEE transactions on knowledge and data engineering, 26(2), pp.322-335, 2012.

[6] Shen, Q., Liang, X., Shen, X., Lin, X. and Luo, H.Y., Exploiting geo-distributed clouds for a e-health monitoring system with minimum service delay and privacy preservation. IEEE journal of biomedical and health informatics, 18(2), pp.430-439, 2013.

[7] Liu, H., Ning, H., Xiong, Q. and Yang, L.T., Shared authority based privacy-preserving authentication protocol in cloud computing. IEEE Transactions on parallel and distributed systems, 26(1), pp.241-251, 2014.

[8] Zhou, J., Cao, Z., Dong, X. and Lin, X., PPDM: Privacy-preserving protocol for dynamic medical text mining and image feature extraction from secure data aggregation in cloud-assisted e-healthcare systems. IEEE journal of selected topics in signal processing, 9(7), pp.1332-1344, 2015.

[9] Zhang, K., Liang, X., Baura, M., Lu, R. and Shen, X.S., PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs. Information Sciences, 284, pp.130-141, 2014.

[10] Bahtiyar, Ş. and Çağlayan, M.U., Trust assessment of security for e-health systems. Electronic Commerce Research and Applications, 13(3), pp.164-177, 2014.

[11] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Security enhancement in healthcare cloud using machine learning." Procedia Computer Science , pp 388-397, 2018.

[12] Inani, Anunaya, Chakradhar Verma, and Suvrat Jain. A machine learning algorithm TSF k-Nn based on automated data classification for securing mobile cloud computing model. IEEE 4th International Conference on Computer and Communication Systems (ICCCS). IEEE, 2019.

[13] Liu, Ximeng, et al. Privacy-preserving patient-centric clinical decision support system on naive Bayesian classification. IEEE journal of biomedical and health informatics pp. 655-668, 2018.