International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Secured Access and Security Issues of Maintenance for Cloud Database

Swati Vithal Khidse, Santosh S. Lomte

Abstract*: Users are using the cloud database services for storing there important data in order to utilized cloud services. Data confidentiality remains one of the main concerns and the major barrier to the development of cloud services. But at the same time users also think about "whether there data is in secured hands and how it is protected from the outside world?" In order to make sure users that there data is in safe hands, cloud database are using more secured mechanism for accessing the cloud database. In order to achieve the goal of security we are using AES and honey encryption (HE) algorithm for strong authorization. Before authorization we need to have authentication of the users. We are using keystroke dynamics as a biometrics authentication and second one as color code authentication. Cloud databases should also be properly maintained from security point of view. For the different levels of the cloud database we have find out the security issues which provide help in maintenance of cloud database. By implementing these issues the security of the cloud database will be more increased.

Keywords* : *Honey Encryption, AES, Cloud Database

I. INTRODUCTION

Cloud computing provides users to access their data whenever they required using cloud computing services. The user data is stored in the cloud database. User needs to use internet for accessing services provided by cloud in Fiig.1 we have shown how this is performed by user.

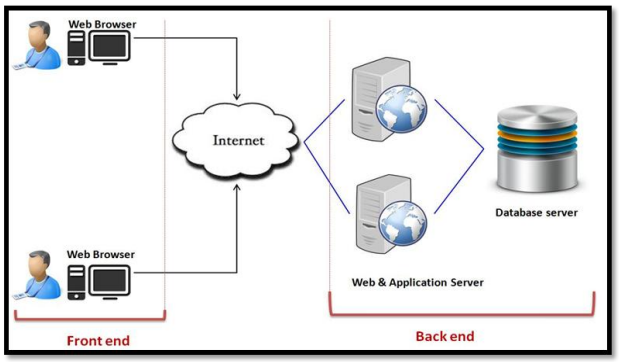

Fig. 1.User accessing cloud database

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Swati Vithal Khidse*, Department of Computer Science & Engg, Dr. BAMU, Aurangabad, India. Email: swatikhidse@gmail.com
Dr. Santosh S. Lomte, Radhai Mahavidhyalaya, Aurangabad, India. Email: drsantoshlomte@gmail.com

Database is the core of nearly every application. Whenever an application performance or availability problem arises, there's a good possibility it's related to the underlying database's performance. Database performance impacts their users. The cloud developers and other moves in technology are making entire IT department more application-focused. But at the end, applications are what matters to the business organization and to end users.

In our method for implementing proposed model, keystroke features of a user are collected during registration process. With the use of the application, along the time for log in, the features got gradually change. For classification we are using Support Vector Machine. When the numbers of users are increasing and thus the number of classes, in order to provide precise classification we are using incremental algorithm of SVM. The next step for user verification is using visual color code authentication. The data while storing in the cloud database is encrypted using honey encryption algorithm.

II. LITERATURE SURVEY

For accessing any cloud database services authentication is the first primary step. If we are taking more care at this step, it becomes easy to handle security. Access security measures are generally considered in three steps: Identification & Authentication, Authorization, and Encryption.

For providing strong authentication we can use keystroke dynamics which is based on behavioral biometric authentications. The way user types vary from user to user; this feature can be used to identify and verify him [1]. Human minds are more proficient in recognizing previously learned pictures in comparison to alphanumeric codes or PIN. Also, users need to carry devices for receiving code or he needs to login to the account for getting code, this method does not require the user to depend on others for verification. A user study has been performed comparing several implementations of the graphical approach with PINs [2].

A literature survey shows that a text-based password suffers from security. In order to improve security while login in comparison with text password, pictographic passwords may be used which are resistant to shoulder surfing. One such approach is color code authentication which provides two-step authentications for the verifying user [3].

An authorization process ensures that a person has the right to assess a certain resources and limits of the access unknowing of other user's information. It is a standard approach to apply encryption techniques into sensitive data to secure it and achieve data confidentiality.

Encryption has always observed as the ultimate security measure. It can be of two types; symmetric and asymmetric algorithms. Symmetric encryption algorithm uses only one key to encrypt and decrypt the data.

These algorithms have been compared based on its performance. Honey encryption algorithm (HE), is used for encrypting messages with low min-entropy keys like passwords or PIN [4].

HE generated ciphertext when decrypted with invalid keys, yields plausible-looking but bogus plaintexts called honey messages, making offline decryption attempts insufficient to search the correct plaintext. HE provides security beyond conventional brute-force bounds [5].

While performing all these functions the cloud service provider for protecting user data in cloud database. There are various issues which need to take care while performing maintenance for cloud database.

Among them some issues belongs to security like Protection against attacks, Encryption and Key management, trust and etc [6].

III. PERFORMANCE ANALYSIS

Performance analysis of the proposed model is performed into three parts:

A. Method

We are using two-factor authentication mechanisms for identifying the user. Firstly the user will be verified based on biometric keystroke dynamics.

The features of the users are collected at the registration time. We are using dwell time (i.e. Press-Release time of key) as a feature.

For the classification of the user as genuine or imposter, we have used a support vector machine. After implementing the system with the users, gradually the input features extracted during login starts deviating.

In order to deal with this situation, we have used an incremental support vector machine which is more efficient. The number of classes increases with the users. Incremental SVM provides more correct results than SVM.

B. Performance analysis of keystroke and visual color code authentication-

A confusion matrix is used for describing the performance of a classification model on a set of test data for which the true values.

Performance is measured using accuracy, precision, recall, specificity, F_score in Table I.

Table- I: Performance measure of keystroke dynamics using confusion matrix

Sr. No	Performance Measure					
	Method/ Measure	*Accuracy*	*Precision*	*Recall*	*Specificity*	*F_score*
1	SVM	0.9754	0.9733	0.9996	0.9731	0.9992
2	Incr SVM	0.9939	0.9933	0.9999	0.9933	0.9998

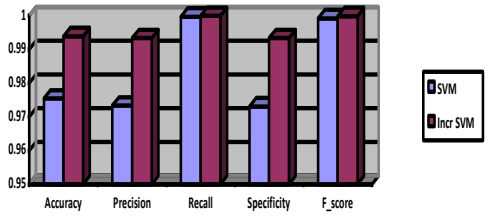

Fig. 2.Performance measure of keystroke dynamics

A binary classifier predicts all the data instances of a test dataset as either positive (true) or negative (false). It produces four outcomes as True positive (TP): Correct positive prediction, False positive (FP): Incorrect positive prediction, True negative (TN): Correct negative prediction, False negative (FN): Incorrect negative prediction.

Table- II: Performance analysis of keystroke dynamics authentication

Sr. No.	Keystroke Dynamics Authentication				
	User Category	*No. of users*	*Total no. of attempts*	*Success Login*	*Fail Login*
1	Registered user	075	171	171	000
2	Registered and imposter user	100	196	157	039

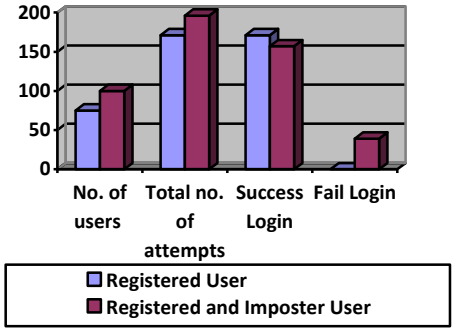

Fig. 3.Performance analysis of keystroke dynamics authentication

C. Method

After identifying a user through keystroke dynamics, the next step was to authenticate using visual color code authentication. By using this technique there is no need to depend upon any other device or application for verification. The user needs to memorize color sequences selected at the time of registration. During login, the user needs to type the code in the same pattern of color selection. If the entered code matches the color selection pattern, the user is authenticated as genuine otherwise imposter. It uses the concept of session password and AES algorithm.

D. Performance analysis of visual color code authentication

The results of visual color code authentication for two scenarios are given in Table III.

Table- III: Performance analysis of visual color code authentication

Sr. No.	Visual Color Code Authentication				
	User Category	*No. of users*	*Total no. of attempts*	*Success Login*	*Fail Login*
1	Registered user	075	200	061	139
2	Registered and imposter user	100	191	103	088

Table- IV: Comparative analysis of Encryption algorithms

Sr. No.	File Size	Encryption Time			Decryption Time		
		AES	*DES*	*BLOWFISH*	*AES*	*DES*	*BLOWFISH*
1	75 MB	126.64	505.16	150.12	65.68	666	157.88
2	100 MB	128.96	970.24	191.52	90.76	1285.2	187.8
3	150 MB	175.04	1809.36	339.4	167.6	2763.04	277.12
4	300 MB	373.2	3243.8	686.04	370.48	4751.48	694.12
5	400 MB	444.24	3597.76	888.08	466.24	5077.68	851.08

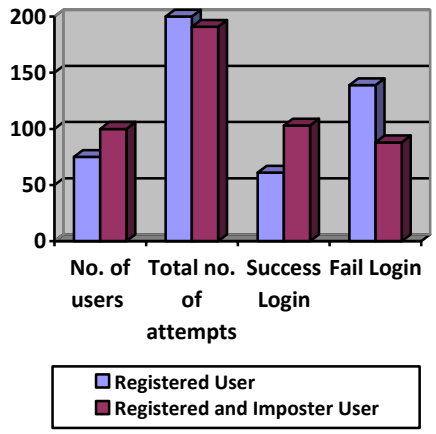

Fig. 4.Performance analysis of visual color code authentication

Table-V: Honey Encryption Time

Sr. No.	Honey Encryption			
	Word size in bits	*File size on Disk (Before Encryption)*	*Encryption time (sec.)*	*File size on Disk (After Encryption)*
1	16	105888897 B	4.773	119135598
2	32	105888897 B	4.423	119135598
3	16	213888897 B	6.067	240646398
4	32	213888897 B	5.845	240646398
5	16	303888897 B	8.759	341905398
6	32	303888897 B	8.274	341905398
7	16	402888897 B	10.423	453290298
8	32	402888897 B	10.244	453290298

E. Performance analysis of encryption algorithms

Data is facing threat to its security in two states; data at rest and data in transit. Data at rest implies data is stored in the cloud and data in transit when the data that is moving in and out of the cloud. For providing data protection in the cloud environment, the encryption algorithm plays a very important role. We have used two encryption algorithms-

- AES algorithm- When the user is uploading or downloading the data (data in transit), AES encryption algorithm is used for encrypting and decrypting the data on the fly. A comparative analysis of AES, DES, and Blowfish encryption algorithm with respect to encryption and decryption time is given in Table IV for different file sizes.
- Honey Encryption- This algorithm is used for encrypting and decrypting data at the rest. When the user is identified as a genuine user, the HE will generate the original data. But on the other hand, if the intruder is identified, and he is trying to download the file at that time a bogus decrypted file will be downloaded with some file extension. In the same session if the user is trying to download the same file again, then a different bogus decrypted file will be downloaded with another file extension. In this way, the intruder is not allowed to get the original file's decrypted content with the same key. The intruder is not able to identify which is the correct decrypted file content; he will get struck within all the files. Hence the data remains confidential. The encryption time for various file sizes is given in Table V.

IV. SECURITY ISSUES OF MAINTENANCE FOR CLOUD DATABASE

While using services provided by cloud computing, data is an important thing from the user's perspective. The user's data is stored in the cloud database and all the operations done by the user on it will be reflected in the cloud database. It's very important to look at how the cloud database is protecting user information. The cloud database management system is divided into five layers the first layer as External Layer, the second layer Conceptual Middleware Layer, the third layer is the Conceptual Layer, the fourth layer Physical Middleware Layer, and the last layer is the Physical Layer. According to this layer classification we have provided the security issues of maintenance for it in Table VI. Maintenance is basically performed so that the cloud database will perform more efficiently in working; provide security, recovery from disaster and etc. [7] [8] [9] [10]

A. External Layer

This layer is used to provide services with full transparency and security.

- **Access Control Policy:** Access policies should be maintained with high security because it provides access rights to the user or group of users.
- **Auditing & Monitoring:** It is used for observing how the database is accessed and by whom. This information should be maintained secured in order to find unauthorized users or access.
- **Security:** The authentication and authorization mechanism used by the cloud should be kept secured in order to provide secured access.
- **Transparency:** This physical placement of data is not known to the users.

Table- VI: Security issues of maintenance for cloud database

External Layer	***Access Control Policy***		***Auditing & Monitoring***
	Security		***Transparency***
Conceptual Middleware Layer	***Data Loss Prevention***	***Data Migration***	***Data Interoperability***
	Distributed System Security	***Auditing & Monitoring***	
Conceptual Layer	***Data Confidentiality***	***Data Integrity***	***Data Consistency***
	Data Sanitization	***Security***	***Data Locality***
	Data Lockdown	***Auditing & Monitoring***	
Physical Middleware Layer	***Interoperability between Platforms***		***Data Leakage Detection***
	Secure key management		***Auditing & Monitoring***
Physical Layer	***Data Storage***	***Data Security***	***Data remanence***
	Data Recovery	***Backup & Replication***	***Fault Tolerance***
	Auditing & Monitoring		

B. Conceptual Middleware Layer

This heterogeneity among different databases will be hidden by this layer.

- **Data Loss Prevention:** It is used for protecting data at rest, in-transit, and on endpoints to reduce data theft or unauthorized availability.
- **Data Migration:** When data is transferred from one place to another data migration is performed with no data loss in between.
- **Distributed System Security:** Accessing data in a distributed system should be secure.
- **Data Interoperability:** Interoperability is provided irrespective of underlying databases.
- **Auditing & Monitoring**

C. Conceptual Layer

Logical structure of the entire database is represented by this layer along with internal processing on data, programming techniques, query processing and optimization.

- **Data Confidentiality**: It used for protecting user data from intruder confidentiality. Thus the data should be securely maintained in cloud database.
- **Data Integrity:** Unauthorized users should be prevented from modifying sensitive information; to accomplish this secured access mechanism for cloud database should be used.
- **Data Consistency:** When the authorized user accesses the data, the changes should be securely reflected in all data copy. This information should be properly maintained from the security point of view.
- **Data Sanitization:** This is the process of permanently removing or destroying the data stored on a memory device. This is very important from the maintenance perspective of data.
- **Security:** The main concern is that data should be protected from any unauthorized user.
- **Data Locality:** Moving compute to the data is faster than moving data to compute.
- **Data Lockdown**
- **Auditing & Monitoring**

D. Physical Middleware Layer

The heterogeneity across different platforms is kept hidden by this platform.

- **Interoperability between Platforms:** While providing the functionality of interoperability, various track of information like user sessions and user authentication has to be maintained.
- **Data Leakage Detection:** The unauthorized transmission of data should be detected and an error report should be generated. This incident should be observed while performing the maintenance routine.
- **Secure key management:** The keys should be placed securely and maintain to avoid unauthorized access.
- **Auditing & Monitoring**

E. Physical Layer

Physical Layer concerns with data storage in order to be easily accessible.

- **Data Storage:** This layer ensures lesser time for accessing and exploring data along with less time for maintenance.
- **Data Security:** This layer provides a mechanism for securing data and thus needs to performed maintenance accordingly.
- **Data Remanence**: It represents the existence of residual data even after deletion so that it is not possible to recover original data by an intruder.
- **Data Recovery:** During the disaster, how effectively and securely the data is restored depends on how maintenance of data is performed.
- **Auditing & Monitoring**
- **Backup & Replication:** Backups restore and replications are used during maintenance for ensuring no data loss of the user.
- **Fault Tolerance:** Handling failures, concurrency control, and deadlock detection should be effectively handled for maintaining system operational during failures.

V. CONCLUSION

A secure access mechanism for users of cloud database services is provided with the help of strong authentication using honey encryption and decryption algorithm. The user's data will be securely placed inside the cloud database. Even if the intruder has found out the key for decryption, it won't work for the other data files stored in the cloud database. So we are trying to keep data secure under such circumstances. This work can be further improved by using another algorithm. At the same time, we have also discussed importance of maintenance and its security issues for the cloud database. It can act as a security checklist for the cloud service providers.

REFERENCES

1. Chandralekha Jadhav, Siddhi Kulkarni, Sagar Shelar, Kaustubh Shinde, Nagaraj V. Dharwadkar, "Biometric Authentication Using Keystroke Dynamics" , International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017 IEEE, pp. 870-875
2. Antonella De Angeli, Lynne Coventry, Graham Johnson, Karen Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", Int. J. Human-Computer Studies 63, 2005 Elsevier, pp. 128–152
3. Manish M. Potey, Dr. C. A. Dhote, Deepak H. Sharma, "Secure Authentication for Data Protection in Cloud Computing using Color Schemes", 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, 2016 IEEE, pp. 424-427.
4. Ari Juels, Thomas Ristenpart, "Honey Encryption: Security Beyond the Brute-Force Bound", Version 1.2, February 28, 2014, pp. 1-24
5. Nirvan Tyagi, Jessica Wang, Kevin Wen, Daniel Zuo , "Honey Encryption Applications- Implementation of an encryption scheme resilient to brute-force attacks", Massachusetts Institute of Technology, 13 May 2015, pp. 1-16
6. Swati V. Khidse , Dr. Santosh S. Lomte, "SECURITY ISSUES OF MAINTENANCE FOR CLOUD DATABASE: AN ANALYSIS", Journal of Emerging Technologies and Innovative Research (JETIR), November 2017, Volume 4, Issue 11, pp. 231-234.
7. Huang Yi , Liang Xiongjian , Zhang Wenjian, Fang Lei, "Operation and Maintenance System of Public Cloud Service", 2013 International Conference on Cloud Computing and Big Data , 2013-14 IEEE, pp. 84-91.
8. Bashir Alam , M.N. Doja , Mansaf Alam , Shweta Mongia, "5-Layered Architecture of Cloud Database Management System", 2013 AASRI Conference on Parallel and Distributed Computing and Systems, ELSEVIER Procedia 5 (2013) pp. 194-199.
9. Joel Weis and Jim Alves-Foss, "Securing Database as a Service," IEEE 2011, pp. 49-55.
10. F. Yahya, V. Chang, R.J. Walters, and G.B. Wills, "Security Challenges in Cloud Storage," in 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, pp. 1052–1056.

AUTHORS PROFILE

Swati Vithal Khidse received the Master of Engineering degree in Computer Science and Engineering from Government College of Engineering, Aurangabad (MH), India, in 2014. She is currently working toward her Ph.D. degree in the Department of Computer Science, Dr. B. A. M. University, Aurangabad, (MS), India. Her research interests include Cloud Computing, Database, Machine Learning and Image Processing. In particular her research focuses on developing Securing Access and Security Issues of Maintenance for Cloud Database mechanisms.

Dr. Santosh Lomte received the Master of Applied Science in Computer from Marathwada University, Aurabgabad (MS), India, M.E Computer Science and Engineering from Dr. B. A. M. University, Aurangabad. He received Ph.D in Computer Science with research area "Computer Programming In Operations Research -Simulation Based Techniques" in 2010. He has published more than 35 research papers in various reputed Journals.