IJSTE - International Journal of Science Technology & Engineering | Volume 2 | Issue 10 | April 2016
ISSN (online): 2349-784X

Prediction using ARMA Algorithm and Cloud Data Security

Swati Kendre
Department of Information Technology
SAOE Kondhwa, Pune-48, India

Saurabh Chidrawar
Department of Information Technology
SAOE Kondhwa, Pune-48, India

Shivani Kankate
Department of Information Technology
SAOE Kondhwa, Pune-48, India

Nikhil Aagwane
Department of Information Technology
SAOE Kondhwa, Pune-48, India

N. S. Sharma
Assistant Professor
Department of Information Technology
SAOE Kondhwa, Pune-48, India

Abstract

In this paper there is large amount of data in cloud computing. Data like audio/video images, text file, word files etc. Challenge is to provide security to data. we provide both authentication and authorization to cloud data. We provide identity based access control mechanism for preventing data from being obtained by appropriate users. This mechanism is still work even digital content is duplicated over other system. One more advantage is only one copy of encrypted data is stored on server which is access by multiple user. We use mechanism in bank applications. We also use the ARMA algorithm for prediction of bank status.
Keywords: iDAC, authentication, authorization, ARMA Algorithm, AES

I. INTRODUCTION

In recent years, various multimedia content such as audio, video, e-books, games and so on is digitalized. As the rapid development of cloud computing digital content is easily spread out on Internet.

This simple mechanism is applying to the access control on the trusted content server. The data encrypt according to personal identification such as name, id, date of birth etc. However these traditional approaches have two major problems.

If the traditional access control is employed in cloud environments the digital content has possible to be duplicated to another content server which may not provide access control.

If the traditional encryption is applied to provide access control, there must be multiple copies of the same digital content for multiple users. This will result in the waste of resources.

In order to solve above problems, the identity-based access control for digital content (iDAC) is proposed in this paper.
iDAC is based on cipher text-policy attribute-based encryption which is an identity-based encryption. In iDAC, the access structure which declares the rating system is embedded into the encrypted digital content. Only users with the identity-based key satisfy the access structure could decrypt the digital content.
The main contributions of this paper are described as follows.

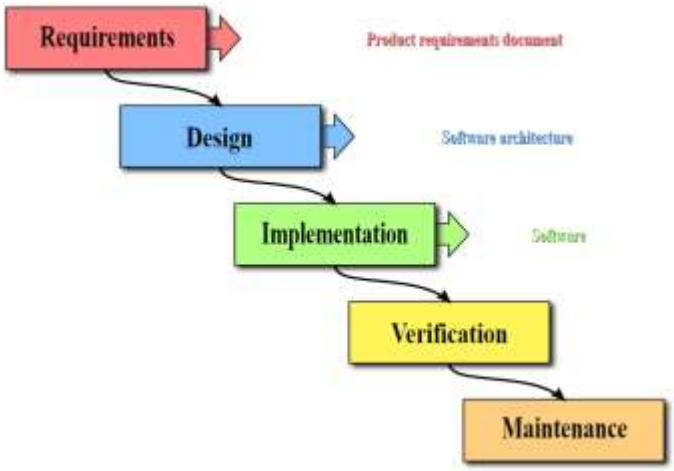
1) The access control still works even the digital content is duplicated to another content server because iDAC is an encryption-based access control approach.
2) Only one copy of encrypted digital content is required to share with multiple users. This could efficiently reduce the overhead of content servers.

ACL-based approaches are typically adopted to carry out fine-grained access control. In ACL-based approaches, an admission controller must be implemented on content servers. A user who request to access a specific content must provide his/her identification. Then the admission controller will determine if this user could access this content based on authentication and authorization. However for availability in cloud environments the digital content is possible to be duplicated to other content servers which may not implement the admission controller.

II. METHODOLOGY

A. Waterfall Model:

The Waterfall Model is a sequential development process, in which progress is seen as following steadily downloads (like a waterfall) through the phages of Conception, Initiation, Analysis, Design, validation, constructions, testing and maintenance.



B. Concept:

1) Encryption & Decryption using AES:

AES is based on a permutation and combination also on combination of both substitution and permutation, and is fast in both software and hardware. Unlike DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. Key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.[5]
AES operates on a 4×4 column matrix. Although some versions order matrix of bytes, called as state have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.[5]
Each round has several processing steps, each step has four similar but quiet different stages, including one that depends on the encryption key itself. A set of reverse steps are applied on ciphertext to convert it in input i.e. plaintext to get a original text.[5]
High-level description of the algorithm[5]

1) Key Expansions—Round keys are derived from the ciphertext. AES requires a 128-bit round key block for each round plus one more.
2) Initial Round
    1) AddRoundKey—Each byte of the state is combined with a block of the round key using bitwise XOR.
2) Rounds
    1) Sub Bytes—A non-linear substitution step where each byte is replaced with different byte according to a lookup table.
    2) Shift Rows—A transposition step in which the last three rows of the state are shifted cyclically to a definite number of steps.
    3) Mix Columns—A mixing operation which operates on the columns of the state, combining the four bytes in each column.
4) Final Round-Add round key(no Mix Columns)
    1) Sub Bytes
    2) Shift Rows
    3) Add

2) Data based on Position:

In this data access is based on position of employee to prevent specific digital content from being obtained by inappropriate users [2]. For example, there is many employees like manager, cashier, assistance manager etc. Manager can access all document and data of bank, cashier can access only transaction of Account holder etc.

3) ARMA Algorithm:

(Autoregressive-Moving-average model)
An ARMA model contains two parts, first is an AR and second is MA model i.e. ARMA (p,q). The model is usually referred to (p,q) model where p is the order of the autoregressive part and q is the order of the moving average part.[4]

1) Autoregressive

The notation AR(p) refers to the autoregressive model of order p. The AR(p) model is written
X_t = c + \sum_{i=1}^p \varphi_i X_{t-i}+ \varepsilon_t .
where \varphi_1, \ldots, \varphi_p are parameters, c is a constant, and the random variable \varepsilon_t is white noise.

2) Moving-average

The notation MA(q) refers to the moving average model of order q:
X_t = \mu + \varepsilon_t + \sum_{i=1}^q \theta_i \varepsilon_{t-i}\,
where the ?1, ..., ?q are the parameters of the model, ? is the expectation of X_t (often assumed to equal 0), and the [4]

3) Autoregressive-Moving-average model:

The notation ARMA(p, q) refers to the model with p autoregressive terms and q moving-average terms. This model contains the AR(p) and MA(q) models,[4]
X_t = c + \varepsilon_t + \sum_{i=1}^p \varphi_i X_{t-i} + \sum_{i=1}^q \theta_i \varepsilon_{t-i}.

The general ARMA model was described in the 1951 thesis of Peter Whittle, who used mathematical analysis (Laurent series and Fourier analysis) and statistical inference.ARMA models were popularized by a 1971 book by George E. P. Box and Jenkins, who expounded an iterative (Box–Jenkins) method for choosing and estimating them. This method was useful for low-order polynomials[4]
\varepsilon_t, \varepsilon_{t-1},... are again, white noise error terms.

III. LITERATURE SURVEY

Sr no	*Authors*	*Work done*	*Published journal name*
1.	*Win-Bin Hung,Wei-Tsung Su*	*Attribute base encreption [1]*	*IEEE 2015*
2.	*Dan Sahai,and Boneh ,Amit Brent Waters*	*Access control list[2]*	*ACM 2012*
3	*John Bettencourt, Amit Sahai Brent Waters*	*Cipher text-Policy Attribute-Based Encryption[3]*	*IEEE 2007*
4.	*Sheng Lu, Ki*	*ARMA Algorithm*	*IEEE 2001*
5	*Guang-liang Guo, Quan Qian *, Rui Zhang*	*AES Algorithm*	*IEEE 2015*
6.	*Carl Almond*	*cloud computing Security*	*2009*
7.	*Yong Pan, Ning Hu*	*cloud computing*	*IEEE 2014*

A. Problem Identified:

Traditional approaches have two major problems.
1) If the traditional access control is employed, in cloud environments, the digital content is possible to be duplicated to another content server which may not provide access control.
2) If the traditional encryption is applied to provide access control, there must be multiple copies of the same digital content for multiple users. This will result in the waste of resources.

B. Solution Proposed:

In order to solve above problems, the identity-based access control for digital content (iDAC) is proposed in this paper.
iDAC is based on cipher text-policy attribute-based encryption which is an identity-based encryption. In iDAC, the access structure, which declares the rating system, is embedded into the encrypted digital content. Only users with the identity-based keys, which satisfy the access structure, could decrypt the digital content.

C. Diagrams of Output

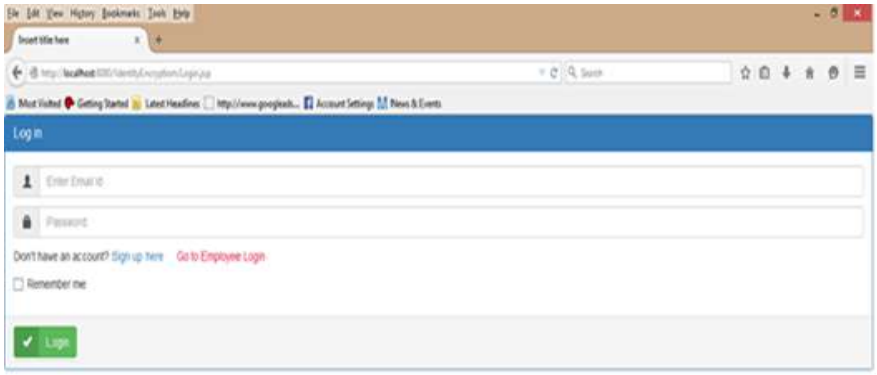


Fig. 1:

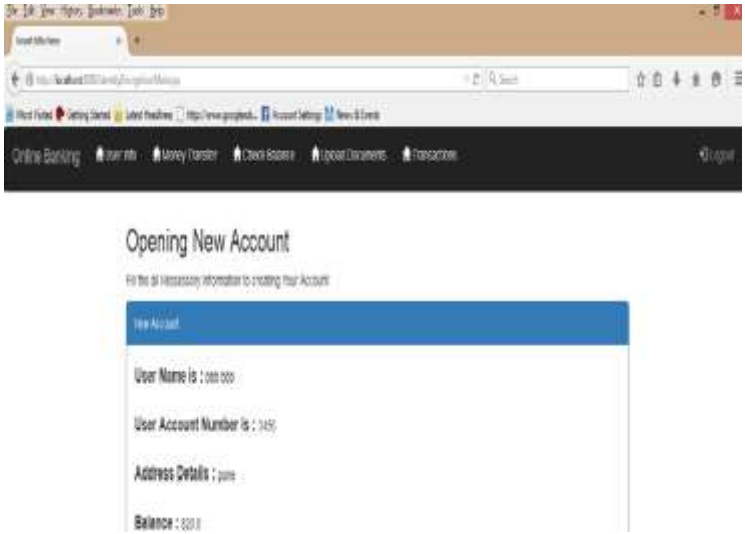


Fig. 2:

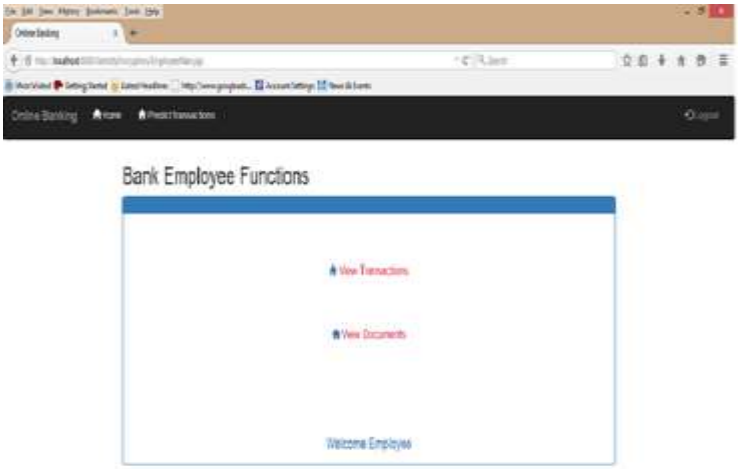


Fig. 3:

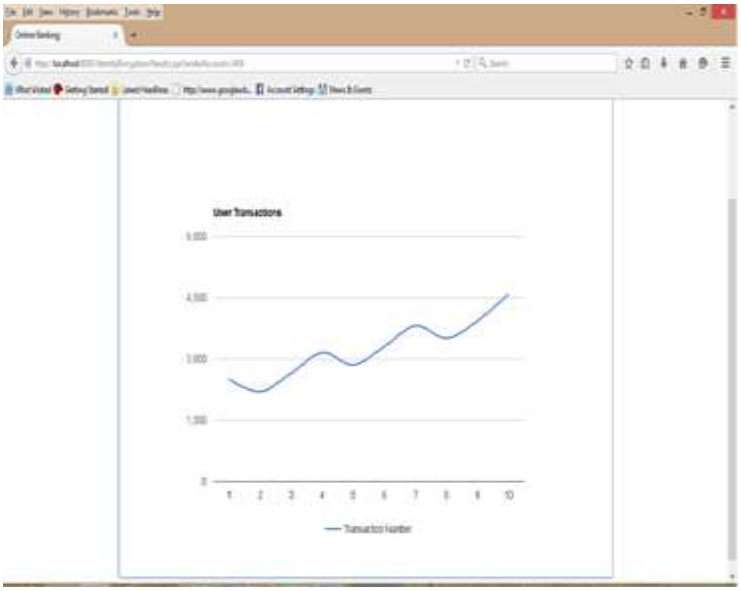


Fig. 4:

D. Title and Authors:

The title (Helvetica 18-point bold), authors' names (Helvetica 12-point) and affiliations (Helvetica 10-point) run across the full width of the page – one column wide. We also recommend e-mail address (Helvetica 12-point). See the top of this page for three addresses. If only one address is needed, center all address text. For two addresses, use two cantered tabs, and so on. For three authors, you may have to improvise.

IV. FIGURES/CAPTIONS

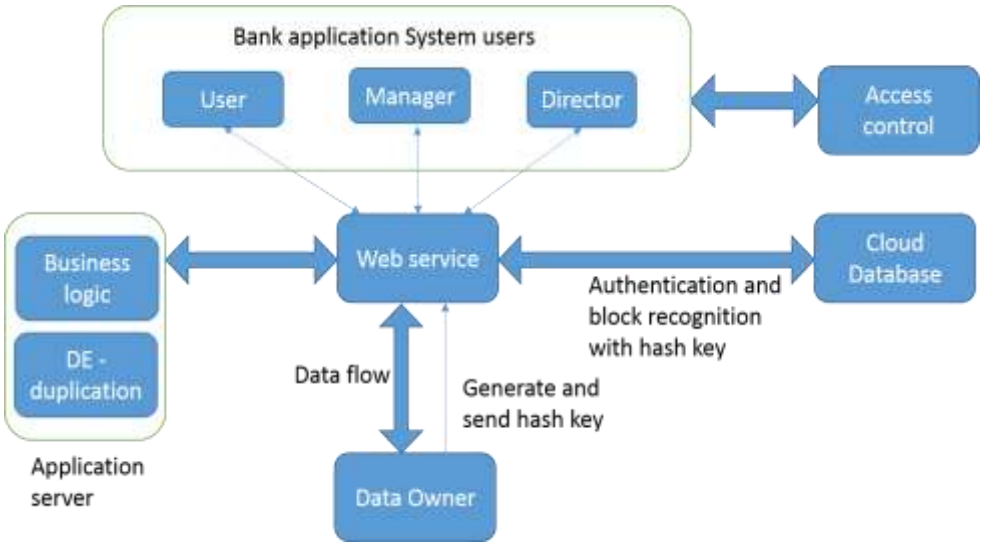


Fig. 5: Block Diagram

V. CONCLUSION

We are providing security of data on cloud. We have also done prediction using ARMA (Autoregressive-Moving-average model) algorithm in machine learning. As a case study. we are using AES algorithm for encryption purpose

This project focuses on the issues related to the data security aspect of Data Storing. As data and information will be shared with a third party, cloud users want to avoid an un-trusted cloud provider. Protection of user's important data is the most significant part of this project. we are using AES algorithm for encryption purpose., we have used bank application.

ACKNOWLEDGMENTS

We take this opportunity to express gratitude towards all the people who have been a part of this project, right from the initial phases. We extend our gratitude towards our internal project guide Mr.Nakul Sharma, who has been a source of great help whenever needed. Our Head of Department Prof. Abhay Adapanawar has also been very helpful and we appreciate the support he provided us with. We would like to convey our gratitude to all the teaching and non-teaching staff members of Information technology department, our friends and families for their valuable suggestions and support.

REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.
[2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.
[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems
[4] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.
[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.
[6] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.
[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.
[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.
[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender