A STUDY ON MIST AND MALACHI ALGORITHM FOR ACCOUNT RECOVERY PROCESS IN CLOUD COMPUTING

***R.ABINAYA[1], DR.T.RAMAPRABHA[2]**

M.Phil Full Time Research Scholar, PG and Research Department of Computer Science1

Professor, PG and Research Department of Computer Science2

Vivekanandha College of Arts and Sciences for Women [Autonomous],

Tiruchengode,Tamilnadu,Namakkal-637 205,

abinayaramani8@gmail.com1,ramaradha1971@gmail.com2

***Address for correspondence:R.Abinaya,M.Phil Full Time Research Scholar, PG and Research Department of Computer Science,Vivekanandha College of Arts and Sciences for Women [Autonomous], Tiruchengode, Tamilnadu, Namakkal-637 205,**

E.mail: abinayaramani8@gmail.com

ABSTRACT-Cloud computing is emerging as a new thing and many of the organizations are moving towards the cloud but lacking due to security reasons. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The security algorithms introduced in this paper, the MIST and Malachi are two new algorithms to protect user data through account security. In the MIST algorithm, when a user logs in for the very first time, they are prompted with three questions and for each of those, they can choose very specific multiple choice answers. After the user provides answers to all given questions, a cloud system is using the MIST algorithm for password recovery.Malachi is a developing algorithm which takes an entirely different approach to account security. Instead of using click-based interfaces like the MIST, Malachi relies entirely on typed user input.

Key words

Cloudcomputing, Mist, Malachi, E.mail, Account recovery.

I.INTRODUCTION

Cloud Computing is cheaper than other computing models; zero maintenance cost is involved since the Cloud Service Provider is responsible for the availability of services, and clients are free from maintenance and management problemsof the resource machines. Due to this feature, CloudComputing is also known as utility computing, or 'IT onDemand'.In this paper focus mainly on eliminating the weak passwords and account recovery vulnerability that are common in today's computing systems.Average users sometimes do not realize the importance ofstrong passwords, and other inconvenient security measures,and thus leave their accounts vulnerable to attacks inexchange for convenience.

This means it is up to the systemarchitects and developers to implement security measures that protect these users adequately, while giving the users the ease and convenience level they expect. This way the user is still protected without being overly inconvenienced by a security system.

The juxtaposition of a user's convenience versus their level of protection is a huge factor in determining the best security algorithm to use in a system.

The MIST security algorithm is an innovative solution that meets these needs. The MIST combines a simple, user friendly interface based approach to account recovery, while also incorporating highly user-specific questions. When the MIST algorithm is integrated in a system, account recovery becomes far more secure. Another solution proposed in the paper is a developing algorithm titled Malachi, which takes an entirely different approach to account security. Instead of using click-based interfaces like the MIST, Malachi relies entirely on typed user input.

II.NEED FOR SECURITY

Security is one of the biggest issues in the cloud computing. Although cloud service providers implement the best security standards and industry certifications, storing data and important files on external service providers always opens up risks. Using cloud-powered technologies means you need to provide your service provider with access to important business data.

Meanwhile, being a public service opens up cloud service providers to security challenges on a routine basis. The ease in procuring and accessing cloud services can also give nefarious users the ability to scan, identify and exploit loopholes and vulnerabilities within a system.

For instance, in a multi-tenant cloud architecture where multiple users are hosted a break into the data of other users hosted and stored on the same server. However, such exploits and loopholes are not likely to surface, and the likelihood of a compromise is not great.

A) Risk And Security Concerns With Cloud Computing

Insecure application programming interfaces; Malicious insiders; Unknown risk profile; Shared technology vulnerabilities; Data loss and leakage; Account, Service and traffic hijacking.

Due to the dynamic nature of the cloud, information may not be located in the event of a disaster immediately. Business continuity and disaster recovery plans must be well documented and tested. ***Recovery time objectives should be stated in the contract.*** When faced with the paradigm change and nature of services provided through cloud computing, there are many challenges for cloud providers.

III.MIST ALGORITHM

MIST is a security algorithm that has security question/answer system that allows an authorized person to access their account, aids in the memorization process to remember their account login credentials, and limits the effectiveness of social engineering to bypass the system.

In the MIST algorithm, when a user logs in for the very first time, they are prompted with three questions and for each of those, they can choose very specific multiple choice answers. After the user provides answers to all given questions, a cloud system is using the MIST algorithm for password recovery. If a user forgets their password, then they are provided sixteen seconds to pick the correct for the security questions that were initially given during setup. With MIST, the answer to the security question is shown randomly shuffled with other possible answers of same category.

For instance if the user sets his/her security question as "What is your favorite laptop brand?", the MIST algorithm provides fifty, as of now, different laptop brands as possible answers among which all the choices including the correct answer will be positioned on random spot. When a user selects all three correct answers, they are redirected to reset their password. While using MIST to reset a password, a user is only allowed a preset number of attempts at answering the questions. An attempt would each time that a user was to answer a question incorrectly. The individual user's account would become locked after the set number of attempts has been reached. The user would then have to get in contact with a server administration, providing additional credentials, to have their account unlocked. These additional credentials could be a state issued Driver license or a student identification card

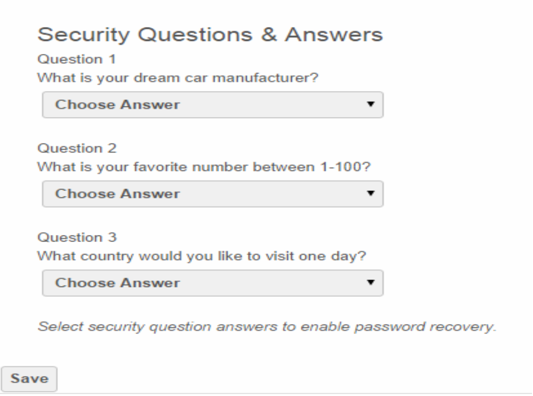
This method would allow enhanced security while maintaining the integrity of the data stored on the server by the user.

The initial question selection was:

1) What is your favorite car brand?

2) Which country would you like to visit one day?

3) What is your lucky number between 1-100?



Security Questions & Answers

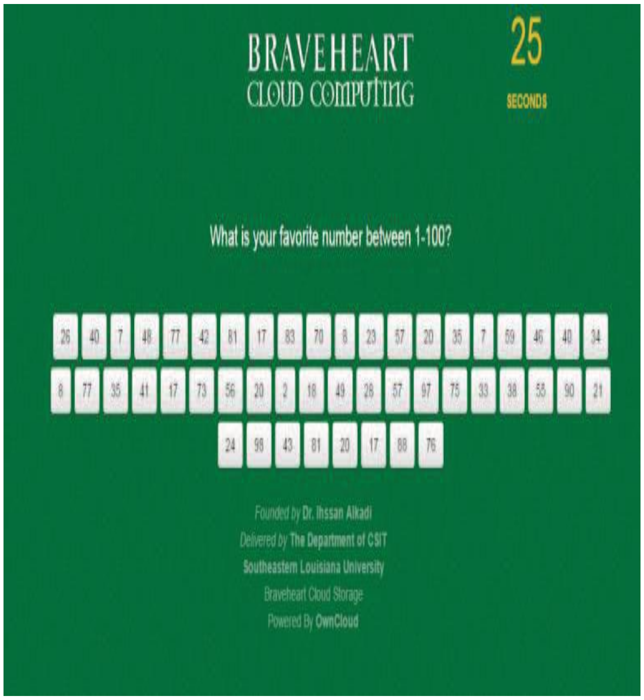
Question 1
What is your dream car manufacturer?
Choose Answer ▾

Question 2
What is your favorite number between 1-100?
Choose Answer ▾

Question 3
What country would you like to visit one day?
Choose Answer ▾

Select security question answers to enable password recovery.

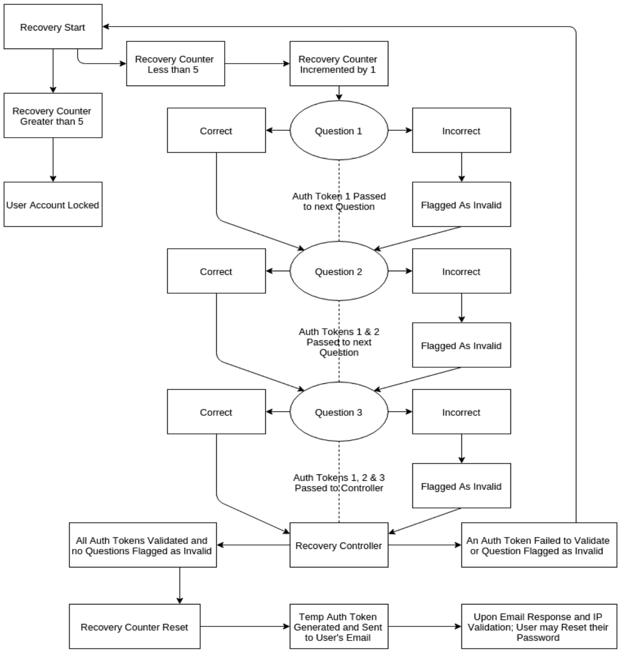
Fig 1.User is Prompted To Choose Answers To The Security Question



What is your favorite number between 1-100?

Founded by **Dr. Ihssan Alkadi**
Delivered by **The Department of CSIT**
Southeastern Louisiana University
Braveheart Cloud Storage
Powered By **OwnCloud**

Fig2. MIST Answer Selection Screen



Recovery Start
Recovery Counter Less than 5
Recovery Counter Incremented by 1
Recovery Counter Greater than 5
User Account Locked
Correct
Question 1
Incorrect
Auth Token 1 Passed to next Question
Flagged As Invalid
Correct
Question 2
Incorrect
Auth Tokens 1 & 2 Passed to next Question
Flagged As Invalid
Correct
Question 3
Incorrect
Auth Tokens 1, 2 & 3 Passed to Controller
Flagged As Invalid
All Auth Tokens Validated and no Questions Flagged as Invalid
Recovery Controller
An Auth Token Failed to Validate or Question Flagged as Invalid
Recovery Counter Reset
Temp Auth Token Generated and Sent to User's Email
Upon Email Response and IP Validation; User may Reset their Password

Fig3.Diagram of MIST Algorithm

IV.MALACHI ALGORITHM

Another solution proposed in the paper is a developing algorithm titled Malachi, which takes an entirely different approach to account security. Instead of using click-based interfaces like the MIST, Malachi relies entirely on typed user input. The algorithm is as follows: when a user creates an account for a cloud service,

The user must do the following steps is given below:

(1) Create an alphanumeric user name, and a password consisting of at least one capitalized letter, at least two numbers and at least one special character, with a minimum length of eight characters. Next, the user must,

(2) Type in four custom security questions ,and provide corresponding answers. The user will enter each question and answer twice to verify spelling before being allowed to proceed.

(3) The security questions and answers will then be hashed and stored in the database with the corresponding account information.

(4) These security questions and answers will need to be provided at each login attempt unless the user has selected a checkbox to indicate “I trust this computer” on a previous login on the same machine. T his checkbox will alleviate the inconvenience of entering the four questions and answers constantly on the user’s home computer, but when the account is being accessed from a computer that is not trusted, the questions will once again be required. The idea behind this algorithm is that in order for the account to be as invulnerable as possible, the security computer, but when the account is being accessed from a computer that is not trusted, the questions will once again be required. The idea behind this algorithm is that in order for the account to be as invulnerable as possible, the security questions associated with it should be entirely of the user’s design. Whereas typically, the security question approach involves a dropdown list of possible questions, this new approach depends entirely on the user entering the question and answer exactly as entered when the account was created. It is possible through social engineering to find out the maiden name of someone’s mother, or the place they became engaged, but this depends on the intruder already knowing which security question they should search for the answer to. This makes a successful breach into these accounts much more difficult than a typical security question from a drop down list. 3 Another fail safe in place in this algorithm is that

(5) There is no confirmation until after submitting the three questions and answers, each on a different page with a continue button at the bottom, as to whether the information provided was right or wrong.

(6) After three failed attempts to log in using the security questions, ***the account is locked for 10 minutes. The further development of the Malachi security algorithm is a future plan of this work.***

V.PARAMETERS FOR ANALYSIS

There are certain inherent requirements that must be met by any Security protocol developed for the cloud computing. We present these parameters below:

A) Access Control

The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

B) Data Confidentiality

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

C) Anonymity and Traceability

Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

D) Efficiency

The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users.That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

VI.EMAIL ON THE GO

Email communication now plays a central role in most of our busy lives. That's fine if you don't go out much but if you travel a lot, this may cause problems. Unless you carry a mobile WiFi-enabled laptop with you everywhere you go or use push email on your cell phone, having an email client sitting on your computer at home means that while out and about you risk spending time outside of the communication loop.T his is one area where the cloud finds it is most frequent and useful application.

Online email has been offered by all the big names ***(such as Microsoft, Yahoo and of course Google)*** for a number of years and I have tried a lot of different services. Wherever in the world I have found myself, my emails have (almost) always been made available to me. The easiest and most convenient for me is Google Mail, although each has its pros and cons. of course, using webmail makes you a slave to an internet connection.

The first thing you do when you find yourself in a new or unfamiliar location is to try and locate an internet café or public library to launch your secure portable browser and check your emails. Privacy concerns are never far from the surface either, especially when stories of passwords to private accounts being leaked online hit the headlines.How much of your life have you given away during email exchanges? And then there's the issue of possible data loss, which nicely leads onto the next incarnation of cloud computing.

Fig 4.Email Process

VII.ANALYSIS AND RESULT

MIST is a one kind of algorithm used for an account recovery process. It consists of set of pre-defined questions.-It is used only when the account recovering time. MALACHI is also a one kind of algorithm used for an account recovery process. In MALACHI user must generate and type theirown questions and answer to that question at that time of account creation and also in an each login attemptbut there is adifference between these two algorithm .

MALACHI is more secure when compared to the MIST algorithm because MIST consists of a set of pre-defined questions.so there is a lot of chances for data to be loss.

In Malachithe question should be generated by the user in an own choices at the time of account creationprocess and also in the login attempt in the new system.so it is more secure when compared to MIST.

s

Table.1 Comparison Table For MIST And s

MALACHI Algorithms

MIST	MALACHI
Used for Account Recovery process	Used for Account recovery process
Set of Pre-defined questions.	User should Generate their Own Questions.
Used at the time of Account recovery time only.	Used at the time of Account Creation Process and also in each Login attempt.
Least Security	High Security.

VIII.CONCLUSION

Cloud Computing is the future of the information technology industry. Because so much vulnerable private data is being stored on the cloud, research into data integrity and security on the cloud has become one of the fastest growing disciplines in Computer Science. The security approaches covered in this paper are all strong individually, but the best way to ensure optimum security is to use these methods in concurrence. The MIST algorithm introduces an innovative method for account recovery. The Malachi algorithm offers a new approach to protecting accounts in regular logins. The goal in implementing these security algorithms into a cloud infrastructure is protecting the private data stored there even more effectively Security will never be an exact science, and it is impossible to predict the changes in security threats coming in the future. In the last decade the cloud has transformed the way data is handled on the internet. With all the research going into cloud and cloud security now, one can only imagine where the cloud will be in another ten years. The best way to keep up with the most recent security threats is to always stay current security methods, and to always strive to find new ways to improve cloud security.

REFERENCES

[1.] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu“Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[2.]S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.

[3] D. Devkota, P.Ghimire, J. Burris, I. Alkadi, IEEE,“Comparison of Security Algorithms in Cloud Computing”,2015.

[4]Constine, Josh, “Facebook Has Users Identify Friends .InPhotos To Verify Accounts, PreventUnauthorizedAccess”,

http://www.insidefacebook.com/, 2010.

[5] Aloul, F.; Zahidi, S.; El-Hajj, W., "Two factorauthentication using mobile phones," Computer Systemsand Applications, 2009.

[6] M. N. Omar, M. Salleh, M. Bakhtiari, 2014 International Symposium on Biometrics and Security Technologies (ISBAST), “Biometric Encryption to Enhance Confidentiality in Cloud Computing”, 2014.

[7] F. Mouton, M. M. Malan, L. Leenen, H. S. Venter, Social Engineering Attack Framework sInformation Security for South Africa (ISSA), 2014.