MAKA Protocol: Secure Authenticated Key Management Protocol for Storing the Data below Data Revocation in Cloud Computing

Jittuga Praveen[1], M Durga Satish[2]

[1]M.Tech Student, Department of CSE, Sri Vishnu Institute of Technology
[2]Associate Professor, Department of CSE, Sri Vishnu Institute of Technology

---

ABSTRACT: In modern day's cloud computing has emerge as one the various charming domain names that are hired via way of means of maximum MNC and IT companies. Generally that is fashioned via way of means of interconnecting a huge quantity of structures related all collectively for faraway servers hosted on net to store, get entry to, retrieve statistics from faraway machines now no longer from neighborhood machines. In gift days there has been no safety for the statistics that's saved withinside the cloud server, due to the fact the statistics isn't encrypted via way of means of robust way of encryption and there's no facility to block the person revocation. In order to cope with the troubles associated with statistics safety and person revocation withinside the public network, we attempt to layout a three-issue Mutual Authentication and Key Agreement (MAKA) protocols for accomplishing the ones concepts. Here throughout this modern paper we try to cope with those boundaries of modern cloud server and that we advise a provable dynamic revocable three-issue MAKA protocol that achieves the person dynamic control wherein if any revoked person need to get entry to the cloud sever can't capable of get entry to the cloud together along with his vintage credentials. By undertaking diverse experiments on our proposed approach, simulation consequences simply nation that proposed approach is great in supplying safety in opposition to statistics revocation beneathneath dispensed garage environment.

Keywords: Cloud computing, Revocation, Mutual Authentication, Key Agreement, Encryption, Decryption, Dynamic Revocable.

I.INTRODUCTION

Cloud computing will generate a variety of computation area and garage ability to keep and get entry to the records to and from the faraway places. This will significantly appeal to extraordinary forms of clients (I.e. Mobile Phones, Personal Computers, Automation Companies) to keep and get entry to the records from faraway places with their man or woman necessities and comforts. Among diverse times gave with the aid of using cloud computing, cloud garage administration, for instance, Apple's iCloud, Microsoft's Azure, DriveHQ, Silicon House gives a revolutionary method to proportion the records over the internet, with the aid of using offering a variety of blessings for the overall users. Almost in all of the instances the cloud area is going through a variety of protection troubles took place with the aid of using the intruders. Furthermore, records sharing is often uncovered in open environments with very terrible protection and consequently the cloud server might emerge as an goal of assaults.

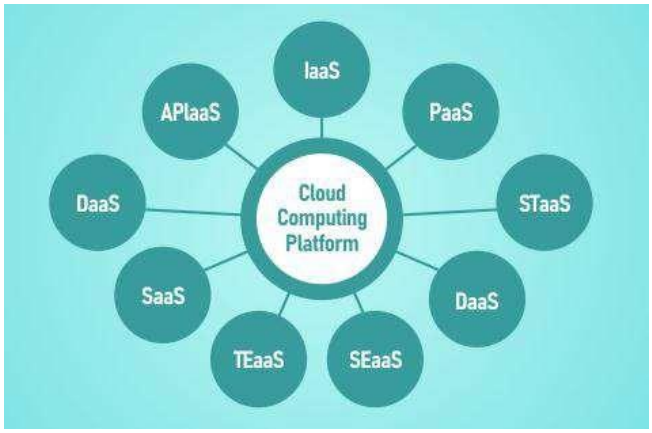

Figure. 1.Several Cloud Services in Real World Environment

In a recent survey we came to know that most of the information from cloud server is revealed by the users who are directly associated with internal server. These internal users may expose the valuable client's information to third party persons who are eagerly waiting for that information. As we know that some users will be terminated from their roles due to some personal cause or under termination process, the key access which is given for that terminated user will not be blocked immediately by the cloud server, hence the user can illegally try to access the same information from outside and gain the valuable information. Hence this process should be dynamically identified and block such revoked users not to access the server with their current credentials. One solution to overcome this problem is to use the cryptography method to include identity based encryption (IBE) to access this security. Here the term identity means the access permissions will be dynamically changes for user periodically and based on user preference only, he/she can

able to access the data from the cloud server.

From the above parent 1, we are able to discover there are lot of cloud offerings gift withinside the actual time surroundings and out of all the ones offerings one will especially speak approximately the 4 forms of offerings like:

1. IaaS,

2. PaaS,

One some of the first-rate carrier is DaaS, wherein this DaaS is especially used for storing and gaining access to the touchy data from different customers who're linked to faraway servers for storing the touchy data and attempt to offer get admission to for the asked users. In contemporary days this isn't always having right safety subsequently on this proposed thesis we attempt to offer safety for this DaaS carrier through the use of primitive cryptography approach and through the use of an stable protocol referred to as MAKA for green key control

3. SaaS and

4. DaaS. and multi authority surroundings approach.

II. LITERATURE SURVEY

Literature survey is that the maximum important step in software program improvement process. Before growing the tool, it is important to exercise session the time factor, financial system and business enterprise strength. Once these things is satisfied, ten subsequent steps are to exercise session which OS and language used for growing the tool. This literature survey is especially used for figuring out the listing of assets to assemble this proposed application. MOTIVATION A famous creator.In this paper the authors focused extra at the cloud computing and additionally approximately the maximum crucial functions of the cloud. In trendy a brand new technique for consumer password authentication is mentioned that is extra steady even supposing an outsider try and study the structures data. The proposed technique can capable of become aware of a one-manner encryption characteristic and may be carried out the usage of a small micro gadgets to govern and display the consumer need. A famous creator Sherali Zeadally [7], has written a paper on" An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture". In this paper the authors especially focused on the hassle of constructing and organising a steady cloud server at the pinnacle of all public cloud infra structures. They especially diagnosed the excessive degree safety choice and additionally approximately the latest cryptographic primitives.

The authors mainly concentrate on the cryptography techniques which were used for providing security for the data encryption and decryption. Here the authors conducted a survey on cloud and its importance in public storage area.

A famous creator Azeem Irshad [8], has written a paper on "An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-

Server Architecture". In this paper the authors specially focused approximately the In the multi-server authentication (MSA) paradigm, a subscriber would possibly avail more than one offerings of various provider providers, after registering from registration authority. In this approach, the person has to keep in mind most effective a unmarried password for all provider providers, and servers are relieved of individualized registrations. Many MSA-associated schemes were offered so far, but with numerous drawbacks.

III. THE PROPOSED SECURE AUTHENTICATED KEY MANAGEMENT PROTOCOL FOR STORING THE DATA UNDER DATA REVOCATION

In this proposed thesis we try to layout a idea known as MAKA PROTOCOL: Mutual Authentication and Key Agreement Under facts revocation for building a aid which can be glad through all of the primitive objectives. Here we strive to deal with a few formal definitions to MAKA set of rules and attempt to listen greater approximately its security. We strive to speak about greater approximately the implementation of RS-IBE set of rules and its advantages. The proposed safety model is mainly proposed or designed based totally mostly on the same old model much like the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) supposition. In extraordinary terms we're capin a position to mention that proposed scheme can supply greater safety for the encoding and interpreting of man or woman authentication. The proposed approach is first-rate in following strategies like : this could provide secrecy of facts in every in advance and backward strategies. The primary feature of this proposed plan is all the facts can be first of all converted in easy text manner in advance than it is stored into the server location. As the facts is stored in an encrypted manner for gaining access to the file, the man or woman goals the get proper of access to permission from the cloud server.

This get proper of access to permission will try to limition un-felony users One predominant function of the proposed method is the cipher textual content that is transformed want to have the get entry to permission like read/write after which put up the ones encryption plans on that and on the quit we want to calculate the parameter's like: the calculation and capacityunpredictability, that are offered in with the aid of using the mystery, is all higher restricted with the aid of using O (log (T) 2),wherein T is the all-out

variety of services.
From the above parent 2,we will truely pick out the proposed MAKA protocol has the subsequent four entities like:

1. Data Provider

2. Data User

3. Storage Server and

4. Key Authority

Once the software is commenced the information proprietor and information person want to sign up first into the software with all of the fundamental details. Once they get registered now the information proprietors and information customers gets authorization from garage server that they could login and carry out their person operations. At this level the information proprietor can capable of login and add

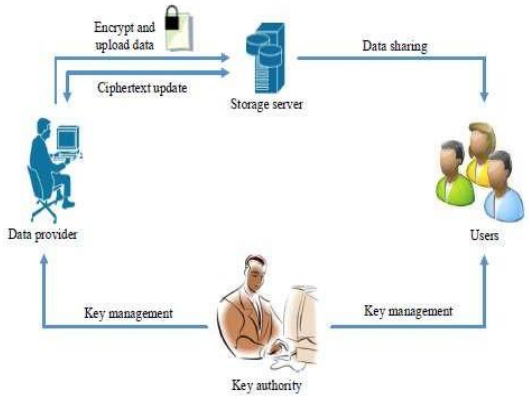

Figure. 2. MAKA Protocol Under Data Revocation

The record into the garage server. As all of us realize that during present day days the information that's uploaded into the cloud server will continually be saved in plaintext way, for a safety reason we strive to encrypt the information after which shop the encrypted files in to the garage location. Here we strive to use a superior encryption method like revocable garage identification primarily based totally encryption (RS-IBE) set of rules for encrypting the information and storing the parameters withinside the centralized server location. As we use RS- IBE for encrypting the information the keys are managed with the aid of using the important thing authority that's found in our software. If any information person who need to get entry to the record in undeniable textual content way then that person want to request the important thing authority for granting key permissions after which handiest the information may be opened in a undeniable textual content way. During the manner of information add and information download, if any person who neglect about to replacement the keys wrongly furnished with the aid of using the important thing authority, then the person becomes as revoked person and this kind of person can't capable of get entry to the documents which he's having permission to get entry to earlier.This is due to the motive like revoked customers are blocked with the aid of using the MAKA protocol and people who're found in lively kingdom handiest can get entry to the documents from the cloud server and ultimate all can't capable of get entry to the record blocks from the cloud server. If this became applied in present day cloud environments we will obtain plenty extra protection for the statistics that's saved and accessed from the cloud server.

IV. IMPLEMENTATION PHASE

Implementation is the degree wherein the theoretical layout is transformed into programmatically manner. In this degree we are able to divide the software into some of modules after which coded for deployment. The the front give up of the software takes JSP,HTML and Java Beans and as a Back-End Data base we took My SQL statistics base. The software is split specially into following four modules. They are as follows:

1) Data Provider

2) Storage Server /Cloud Server

3) Key Authority

4) Data User

Now allow us to talk approximately every and each module in detail

1. DATA PROVIDER MODULE

The statistics company is one that try and sign in into the software and as soon as he receives registered he can capable of login into his account and he can do following operations like :

1. He can capable of add the touchy documents

2. He can encrypt the statistics via way of means of the usage of mystery key

3.View Key request from Data user

4. Allow or Deny key request of statistics user

5. See records of statistics users

2. STORAGE SERVER MODULE

Here the garage server is not anything however cloud wherein this could try and keep all of the touchy records in a steady manner. The garage server has the subsequent centers likes:

1. View Storage Server Files

2. View End person and View Owners

3. View Secret Keys

4. View Attackers

5. Unblock Revoked Users

6. View Transactions

7. View Results in Chart manner

3. KEY AUTHORITY MODULE

Here the important thing authority is 0.33 celebration auditor that is used to furnish keys and permissions for the records proprietors and give up customers. This may also has the power to limition the un-legal customers now no longer to get admission to the cloud records. This Key authority as soon as getting login into its account, it has following operations like:

1. Generate Secret Key

2. View End customers and their request

3. View Attackers

4. DATA USER MODULE

The records person is person who can capable of check in into the utility with all his primary info and as soon as he/she receives registered he can be capable of do following operations:

1. Request Secret Key from Service Provider

2. View Secret Key this is generated with the aid of using Key Authority

3. Download the Data in a undeniable textual content manner

4. Verify whether or not as real person or Attacker

V. CONCLUSION

To resist the exhaustion of password attack on the two-factor MAKA protocols, a large number of three-factor MAKA protocols have been proposed. However, almost all three factor MAKA protocols don't provide formal proofs and dynamic user management mechanism. In order to achieve more flexible user management and higher security, this paper proposes a new three-factor MAKA protocol that supports dynamic revocation and provides formal proof. The security shows that our protocol achieves the security properties of requirements from multi-server environments. On the other hand, through the comprehensive analysis of performance, our protocol doesn't sacrifice efficiency while improving the function. On the contrary, the proposed protocol has great advantages in terms of the total computation time.

VI. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1,pp. 50–55, 2008.

[2] iCloud.(2014) Apple storage service.[Online]. Available: https://www.icloud.com/

[3] Azure.(2014) Azure storage service.[Online]. Available: http://www.windowsazure.com/

[4] Amazon.(2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G.Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on,vol. 25, no. 2, pp. 384–394, 2014.