© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Transient Authentication for Cloud Data Security

Rishikesh Shukla, Ankit Rai, Atul Dobhal, Ankur Srivastava, Uday Patkar

Department of Computer Engineering, Bharati Vidyapeeth Lavale, Maharashtra, India

ABSTRACT

Cloud Computing becomes the next generation architecture of IT Enterprise. In contrast to traditional solutions, Cloud computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges which have not been well understood. In cloud computing, both data and software are fully not contained on the user's computer; Data Security concerns arises because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers with different demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. Even multi-tenancy feature of cloud give rise to security issue related to data and also the authentication of users.

We provide a secure scheme which protects the sensitive data of the user stored in the cloud. We solve the problem which existing systems faces with Transient Authentication, in which a small hardware token (Mobile Phone) continuously authenticates the user's presence over a short-range, wireless link to the machine through which the user is accessing cloud. This machine in turn provides this authentication information to cloud. When the user departs, the token and machine lose contact and the machine stops exchanging the information with cloud making the data secure. We show how to leverage this authentication framework to secure sensitive and confidential data on to the cloud.

Keywords: Cloud Computing, transient system, token, RSA Algorithm.

I. INTRODUCTION

Cloud solutions are scalable and ubiquitous, and follow a pay per use approach at all levels. One of the main barriers to the adoption of Cloud Computing is security. User data are stored on provider servers and there is no guarantee that this information will not be accessible to a third party. This can contravene legal requirements when the stored data are sensitive, as occurs in health care or banking environments. There is no guarantee that the data will be safe and secure at the server side. Here we presented a solution for secure storing of data in the cloud environment through the use transient authentication.

II. METHODS AND MATERIAL

A. Literature Survey

Computing authentication requires that a user supply some proof of identity–via password, smartcard, or biometric–to advice. Unfortunately, it is infeasible to ask users to provide authentication for each request made of a device. Imagine a system that requires the user to manually compute a message authentication code for each command. The authenticity of each request can be checked, but the system becomes unusable. Instead, users authenticate infrequently to devices. User authentication is assumed to hold until it is explicitly revoked, though some systems further limit its duration to hours or days. Regardless, in this model authentication is persistent and creates tension between security and usability. To maximize security, a device

must constantly re-authenticate its user. Tobe usable, authentication must be long-lived. Unfortunately, authentication between people and their computer devices is both infrequent and persistent. Should a device fall into the wrong hands, the imposter has the full rights of the legitimate user. Researchers at the University of Michigan have developed a new model, called "transient authentication," in which a user wears a small token, equipped with a short-range wireless link and modest computational resources. This token is able to authenticate constantly on the user's behalf. It also acts as a proximity cue to applications and services; if the token does not respond toan authentication request, the device can take steps to secure it. This technology provides an improved method and system to maintain application data security on machines that are running or have been suspended. Applications are protected transparently by encrypting in-memory state when the user departs and decrypting this state when the user returns. This technique is effective, requiring just second's to protect and restore an entire machine. In the second embodiment, applications utilize an API for transient authentication, protecting only sensitive state. Ports of three applications, PGP, SSH, and Mozilla are described with respect to this API.

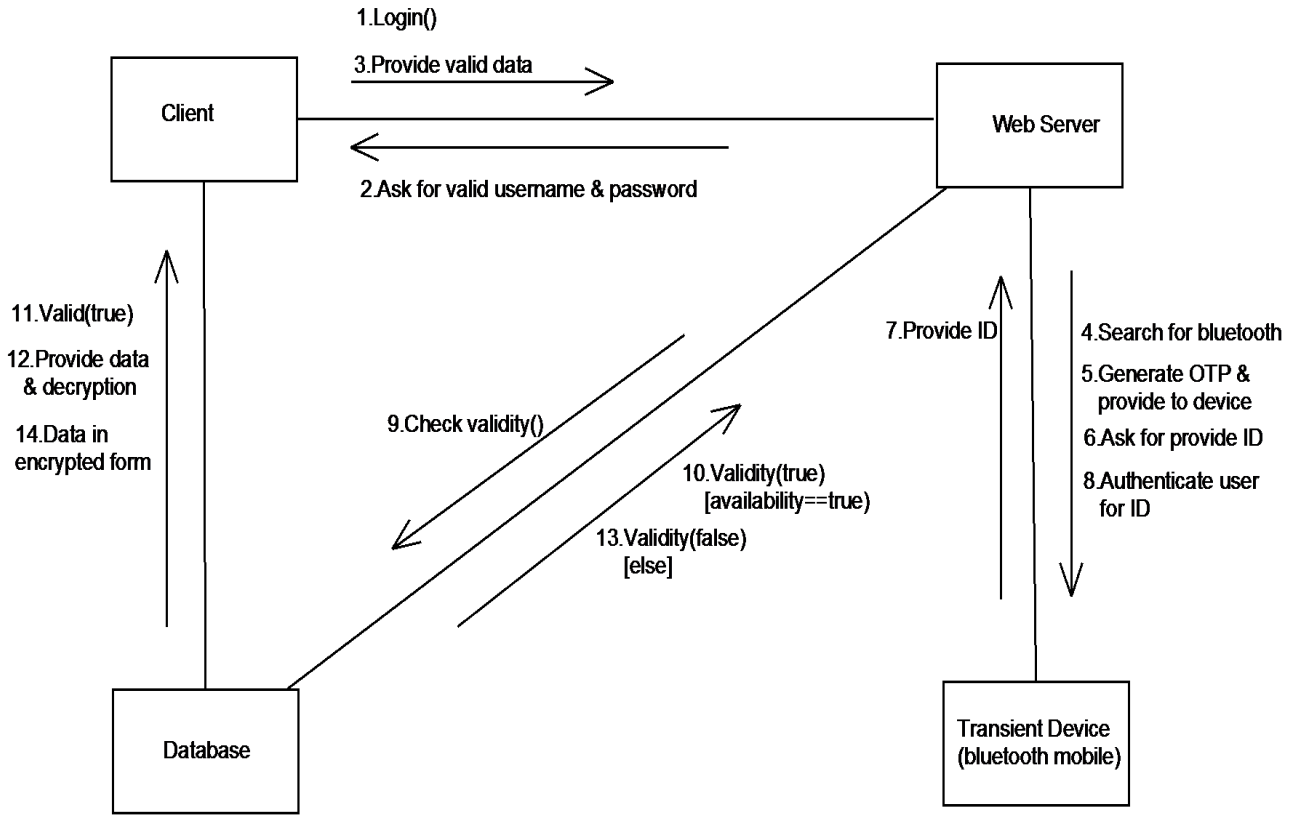
B. Problem Definition

Develop college based transient authentication system cloud security during the data transfer in the cloud by providing token to any device which consist of unique code such mobile or Bluetooth device this system is also at basic college level testing in this system we are using RSA algorithm for encryption and decryption

C. Proposed System

Transient Authentication

Transient authentication is temporary authentication. User provides his authentication information i.e. username and password once and it may not be modified ever. How the system will come to know whether the person typing the user name and password is authenticated or not. One solution is to ask user to enter his username and password frequently but this would be a tedious job. And user will remove his authentication system. Transient authentication resolves this problem. A hardware token on behalf of the actual user will communicate the authentication information frequently to the system. When the hardware token (a mobile) will be in Bluetooth range of the desktop the token i.e. the authentication information will be passed. And the moment when the device is out of the Bluetooth range the data is encrypted again and user cannot access the data. This transient authentication technique can be extended to the cloud computing for securing the data stored on to the cloud. The proposed solution on the security issue related to data stored on the cloud is "Transient Authentication". Transient Authentication is temporary authentication. Cloud users can store their data and also can deploy their applications on to the cloud. Cloud users are dependent on the cloud provider for the security of data kept onto the cloud. But due to the multi-tenancy feature of cloud there is a great security issue related to cloud data. Unauthorized user may access the private data of cloud user. Also the issue of trust evolves. Cloud users cannot trust cloud providers. Hence to access data cloud must check whether the user accessing the data is authorized user of not. Providing username and password for the cloud user is one of the solutions. But how will the cloud confirm that the user typing the password is authorized user or not who has provided the password days back. So to overcome this, cloud user has to provide his identity after particular time duration. Also this process is tedious to the user. Thus transient authentication technique can be used in such situations. Here a mobile device, which is in the Bluetooth range of the host machine through which user will be accessing cloud, will provide the users identity to cloud on behalf of the user. The mobile device will exchange its information to the host machine and host machine in turn will pass this information to the cloud. This will prove the users identity periodically.When the mobile device is not within the Bluetooth range of the host machine there will be no exchange of data within the three entities i.e. the mobile device, the host and the cloud. Hence the user will not be able to access the data from cloud.



III. ACKNOWLEDGMENT

I would like to take this opportunity to thank my internal guide U. C. Patkar, Head of Computer Engineering Department, BVCOEL for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

In the end our special thanks to Co-guide for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

IV. REFERENCES

[1] M. Baker, R. Buyya, and D. Laforenza, "Grids and gridtechnologies for wide-area distributed computing," International Journal of Software: Practice andExperience, vol.32, pp. 1437-1466, 2002.

[2] C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya,"Autonomic metered pricing for a utility computing service", Future Generation Computer Systems, vol. 26,issue 8, pp. 1368-1380, October 2010.

[3] R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1,Springer, pp. 79-88. 2005.

[4] William Stallings, lawrieBrown,"Computer Security", Pearson