An Implementation of Multi-Factor Authentication Scheme for Secured Cloud Data Storage Framework

Himanshu Panadiwal[1], C.P. Patidar[2]
[1, 2] Department of Information Technology
[1, 2] Institute of engineering and technology, Indore, India

Abstract- *With the recent development of IT society, the value of knowledge information has been focused more importantly. However, the accidents of personal and corporate secrets being leaked frequently happen, and also the damage is getting bigger day by day. The important information of individuals and businesses is leaked or processed by outside attacks or personal mistakes, thus misused, and thereby considerable damage is occurring. Data Security is the most critical issues in a cloud computing environment. Authentication is a key technology for information security, which is a mechanism to establish proof of identities to get access of information in the system. Traditional password authentication does not provide enough security for information in cloud computing environment to the most modern means of attacks. In this paper, we propose a new multi-factor authentication scheme for cloud computing. In this paper a novel framework of Multifactor authentication access control is proposed for cloud computing, which provides a multi -step and multiple verification of a user. The model proposed is well-organized and provably secure solution of access control for superficially presented applications.*

Keywords- MFA, Cryptography, Cloud Data, Access Control, Security, OTP

I. INTRODUCTION

Cloud computing is a flexible way to allocate Information Technology (IT) resources i.e. storage, software; infrastructure and bandwidth etc. hpuniversityout of a pool, enabling to consume processing power according to user's needs [1]. It makes easy to set up and use server instances, allowing the size of the infrastructure to grow when there is a need to scale up business while saving costs when the users do not need the extra power anymore.

As information technology is growing rapidly, there has been very fast advancement in various computing technologies likes multimedia, internet technology etc. With the advancement of internet technology, many works are done online. This includes banking, shopping, e-learning, entertainment, chatting, information retrieval and financial transactions etc. All these online activities require some type of authentication. Authentication means to check the identity of the user, which means whether the person is same which he pretends to be. In case of financial transactions, security of information is required to carry out secure transaction. Information in case of online financial transaction includes individual's authentication parameters and some other account related information etc. There are various authentication techniques that are already in use, e.g. user name, passwords, biometric face recognition, public key infrastructure and symmetric key based authentication schemes etc. Authentication schemes are key techniques to verify the correctness of the identities of all communication entities [2].

Authentication is quite challenging and difficult in the case of cloud computing. In cloud computing, a third party is responsible for providing computational power, storage space and application support etc. Every data which is used by a user is stored in cloud database. Cloud database is maintained by third party cloud provider, so user hesitates to keep his data at cloud database. In order to utilize the resources of cloud, user has to provide some identity stating that it is valid person seeking permission to use their resources. If a user needs to use or control a remote server or process financial transactions, the user needs to pass the authentication phase first [3].

1.1 Essential Characteristics [4]

1) **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2) **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3) **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.

4) **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
5) **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Given figure show the Cloud Architecture reference model composed of three service models, four deployment models and five essential characteristics**.**

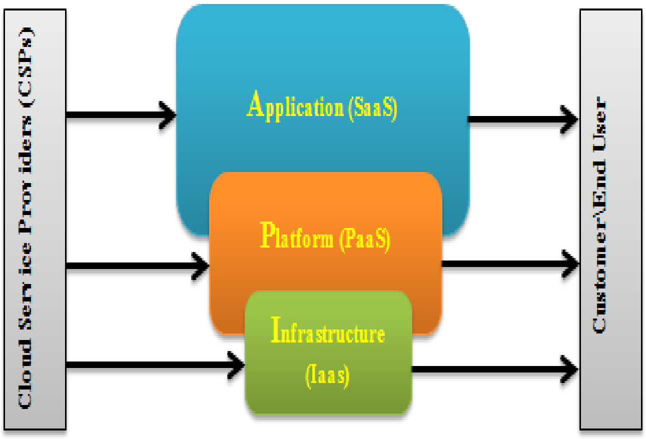


Figure 1 Cloud Architecture Reference Model [5]

1.2 Authentications

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artefact by carbon dating, or ensuring that a product is what its packaging and labelling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification [6].

Or authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. The permissions and folders returned define both the environment the user sees and the way he can interact with it, including hours of access and other rights such as the amount of allocated storage space [7].The process of an administrator granting rights and the process of checking user account permissions for access to resources are both referred to as authorization. The privileges and preferences granted for the authorized account depend on the user's permissions, which are either stored locally or on the authentication server. The settings defined for all these environment variables are set by an administrator

1.3 Multifactor authentication (MFA)

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target [8].

Typical MFA scenarios include:

- Swiping a card and entering a PIN.
- Logging into a website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the requester's phone or email address.
- Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to a network.
- Swiping a card, scanning a fingerprint and answering a security question.
- Attaching a USB hardware token to a desktop that generates a one-time passcode and using the one-time passcode to log into a VPN client.

In the past, MFA systems typically relied upon two-factor authentication. Increasingly, vendors are using the label "multifactor" to describe any authentication scheme that requires more than one identity credential.

1.3.1 Authentication factors

An authentication factor is a category of credential used for identity verification. For MFA, each additional factor is intended to increase the assurance that an entity involved in some kind of communication or requesting access to some system is who, or what, they are declared to be. The three most common categories are often described as something you know (the knowledge factor), something you have (the possession factor) and something you are (the inherence factor) [8].

Knowledge factors – information that a user must be able to provide in order to log in. User names or IDs, passwords, PINs and the answers to secret questions all fall under this category. See also: knowledge-based authentication (KBA)

Possession factors - anything a user must have in their possession in order to log in, such as a security token, a one-time password (OTP) token, a key fob, an employee ID card or a phone's SIM card. For mobile authentication, a smartphone often provides the possession factor, in conjunction with an OTP app.

Inherence factors - any biological traits the user has that are confirmed for login. This category includes the scope of biometric authentication methods such as retina scans, iris scans fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry, even earlobe geometry.

Location factors – the user's current location is often suggested as a fourth factor for authentication. Again, the ubiquity of smartphones can help ease the authentication burden here: Users typically carry their phones and most smartphones have a GPS device, enabling reasonable surety confirmation of the login location.

Time factors – Current time is also sometimes considered a fourth factor for authentication or alternatively a fifth factor. Verification of employee IDs against work schedules could prevent some kinds of user account hijacking attacks. A bank customer can't physically use their ATM card in America, for example, and then in Russia 15 minutes later. These kinds of logical locks could prevent many cases of online bank fraud.

Location factors – the user's current location is often suggested as a fourth factor for authentication. Again, the ubiquity of smartphones can help ease the authentication burden here: Users typically carry their phones and most smartphones have a GPS device, enabling reasonable surety confirmation of the login location.

II. LITERATURE SURVEY

Authentication via more than one factor, Multi-Factor Authentication (MFA), has become an increasingly essential component for cloud systems - a vital means to ensure that users, no matter where they are, are in fact who they claim to be and thus are authorized to gain access to cloud resources. A number of researchers have proposed the design and implementation of MFA systems

The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Authors comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desire benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to us. Beyond this analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals [9].

Keystroke dynamics—the analysis of typing rhythms to discriminate among users—has been proposed for detecting impostors (i.e., both insiders and external attackers). Since many anomaly-detection algorithms have been proposed for this task, it is natural to ask which are the top performers (e.g., to identify promising research directions). Unfortunately, they cannot conduct a sound comparison of detectors using the results in the literature because evaluation conditions are inconsistent across studies. Authors' objective is to collect a keystroke-dynamics data set, to develop a repeatable evaluation procedure, and to measure the performance of a range of detectors so that the results can be compared soundly. Authors collected data from 51 subjects typing 400 passwords each, and they implemented and evaluated 14 detectors from the keystrokedynamics and pattern-recognition literature. The three top-performing detectors achieve equal-error rates between 9.6% and 10.2%. The results—along with the shared data and evaluation methodology—constitute a benchmark for comparing detectors and measuring progress [10].

The Pointcheval-Zimmer scheme was designed to combine three authentication factors in one system, including a password, a secure token (that stores a private key) and biometrics. In a formal model, Pointcheval and Zimmer formally proved that an attacker had to break all three factors to win. However, the formal model only considers the threat that an attacker may impersonate the client; it however does not discuss what will happen if the attacker impersonates the server. Authors fill the gap by analyzing the case of the server impersonation, which is a realistic threat in practice. Assume that an attacker has already compromised the password, and then present two further attacks: in the first attack, an attacker is able to steal a fresh biometric sample from the victim without being noticed; in the second attack, he can discover the victim's private key based on the Chinese Remainder theorem. Both attacks have been experimentally verified. [11]. Ever-growing popularity of mobile devices, such as smart phones and netbooks, coupled with anytime and anyplace availability of high-speed network access is changing the ways how we compute and communicate. Mobile devices play an increasingly important role in our lives and tend to become representations of our digital selves when we trust these devices with sensitive information. Consequently, the problem of securing mobile devices against unauthorized access has never been more important. We present an RFID-based Authentication Middleware (RFID-AM) that combines point of entry and continuous authentication with transparent on-demand encryption of user files. This paper details the architecture of RFID-AM, discusses its fully functional prototype, and presents experimental results demonstrating its performance in various conditions. This paper also surveys different methods and technologies that have been proposed and implemented on mobile devices [12].

Cloud computing contains many enterprise applications that require from each user to perform authenticate at first step. Then, he will gain a permit from the service provider to access resources at second step. The issue breach remains facing a modern computing model. A more secure scheme is the two-factor authentication (2FA) that requires a second factor (such as finger print, token) with username/password. Nevertheless, the feasibility of 2FA is largely limited by high device cost, malicious attack and the deployment complexity. In this paper, A. Yassin propose a scheme of 2FA in cloud computing systems that depends on One-Time Password (OTP), Asymmetric Scalar-product Preserving Encryption (ASPE) and RSA digital signature as two factors. Furthermore, it overcomes aforementioned issues and does not require extra devices such as token device, card reader in smart card and scanner in physiological biometrics. The proposed scheme distinguishes to resist practical attacks, high-security level, anonymous password, mutual authentication, identity management, the cloud server and a user can establish authenticated session keys, reduces the cost, and good performance[13].

III. PROPOSED SYSTEM

3.1 Domain Overview

A number of cloud applications are developed with the help of cloud infrastructure. Among most of them are consuming the sensitive and private data of the account holder such as banking applications, social network and other applications. These applications collect confidential and sensitive data on storage and utilized when necessary. But the leak of data or week authentication and access control policies can harm the data owner’s privacy and can produce losses socially and economically. Therefore a strong cryptographic manner is required to keep in track the security as well as authenticity of data. Thus there are two key issues are addressed for finding the promising solution:

1. Confidential Data and data owner privacy management: the cloud applications of SaaS need sometimes confidential and private information. Additionally sometimes the private data is hosted on cloud servers for long time use. The security of data and their confidentiality management is the primary issue of the proposed study. Thus for managing the security a strong authentication scheme is required. That technique regulates the user’s private data and their access.

2. Secure access of data and identification of user: in further for securing the data access and to control unauthorized access for the data is secondary issue of the security management. In this process the efforts are required to make by which the data is handover only when the authentication credentials are verifies the actual data owner’s identity or the shared data entity.

Therefore in this presented work a secure and effective cryptographic authentication technique is needed to develop. The cryptography is used to handle the secure communication between client and server and also helps to regulate the data owner identity during the sharing of data. Additionally the proposed multifactor authentication technique helps to protect the unauthorized access and confidentiality of data owner’s privacy.

3.2 Methodology

The proposed work provides the multi-factor authentication scheme for securing the data as well as providing the effective access control of the data. Therefore there are three main factors are estimated for utilization:

a. User attributes: these attributes are recovered from the original data which is provided by user for registration purpose and among them some selected attributes are used for preparing the authentication key as the first factor.

b. Data attributes: a number of different kinds of data is used by the end user such as images, some text files and other contents. Thus a part of original data is used as second factor which is request by the user for access.

c. System attributes: in this phase the system properties are extracted to use with the authentication technique development. Thus the system property by which the request is made or data is uploaded is also considered as the factor for the authentication.

3.1.1 Proposed Security Algorithm

This section provides the summarized algorithm steps for demonstrating the proposed system using the algorithm steps. In addition of the key concepts of the use of password are also provided.

Table 1: Proposed Algorithm

```
Input: User Database D, Input User File F, Client ID CID
Output: cryptographic secure file CF

Process:
1.  User Request for System Access
2.  $D_v = extractDeviceInfo$
3.  $A = selectUserAttribute$
4.  $FF = extractFileFeatures(F)$
5.  $[CD_v, CA, CFF] = MD5.GenrateHash(D_v, A, FF)$
6.  $if(CID.Info == CD_v, CA)$
        a. Get Access to server
7.  Else
        a. Error
8.  End if
9.  $K = CD_v + CA + CFF$
10. $CF = DES.encrypt(K, F)$
11. Return CF
```

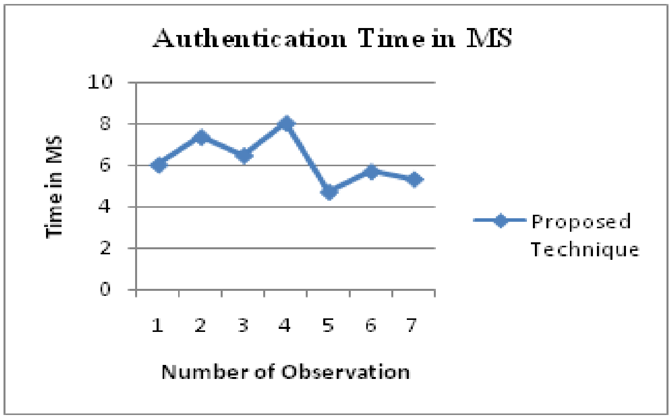
IV. RESULT ANALYSIS

This section provides the evaluation of the proposed cryptographic technique and the proposed multifactor authentication system. Therefore different performance parameters are evaluated.

4.1 Authentication Time

The amount of time required for performing the authentication using the proposed multifactor authentication technique is termed as authentication time. The amount of time taken is computed using the following formula.

time taken = end time - start time

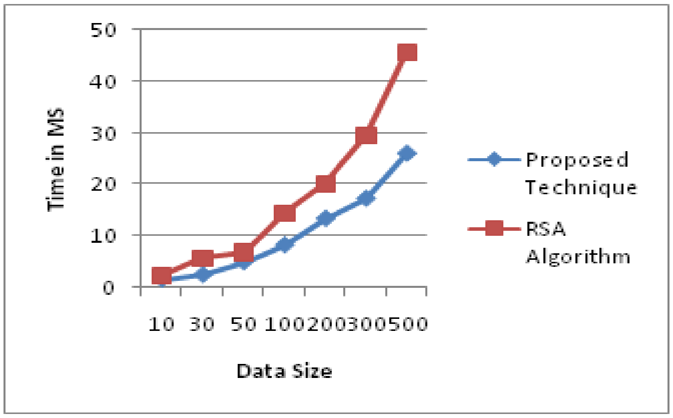


Graph 1Authentication Time

The amount of time required to perform secure authentication using the proposed multifactor authentication technique is demonstrated in above graph. X axis contains the different experimental observations and the Y axis contains the amount of time required to authenticate the user. The obtained results show the proposed technique not consumes much time for authenticating the end user for accessing the system. Thus the proposed system provides the efficient authentication even when more than one parameter is computed during the system access.

4.2 Encryption Time

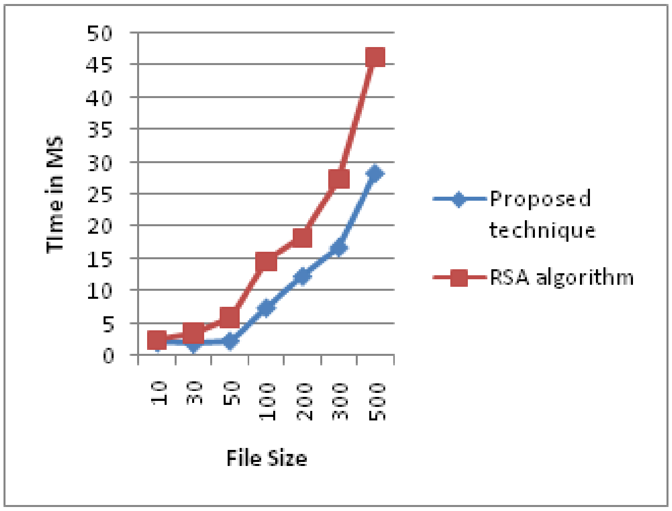
The total amount of time required to encrypt the data during the file exchange between server and user is termed here as the encryption time or the time complexity of the system. The following graph shows the encryption time of the implemented cryptographic technique for securing the data during the communication. In this graph, X axis of the system contains the different size of files used for experiments and the Y axis shows the amount of time consumed for processing the file. The proposed technique is compared with the traditional algorithm RSA for comparative performance study. According to computed performance the proposed technique is more efficient than the traditional RSA based encryption technique.



Graph 2 Encryption Time

4.3 Decryption time

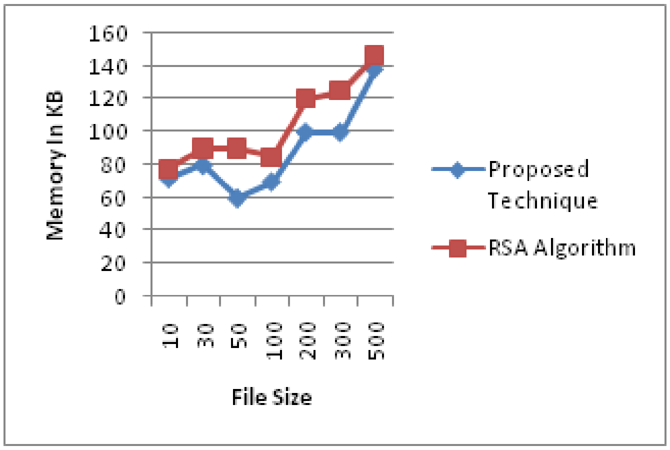
The total amount of time required to decrypt or recover the original files by the cipher text is termed here as the decryption time. The decryption time sometimes also termed as the time complexity of decryption algorithm. The decryption time complexity of the proposed and traditional RSA algorithm for similar experimental file size is reported using given graph, X axis contains the different amount of file size and the Y axis contains the corresponding time consumption for processing of the files. According to the obtained performance the proposed cryptographic technique consumes less amount of time as compared to traditional RSA algorithm.



Graph 3 Decryption Time

4.4 Encryption Memory

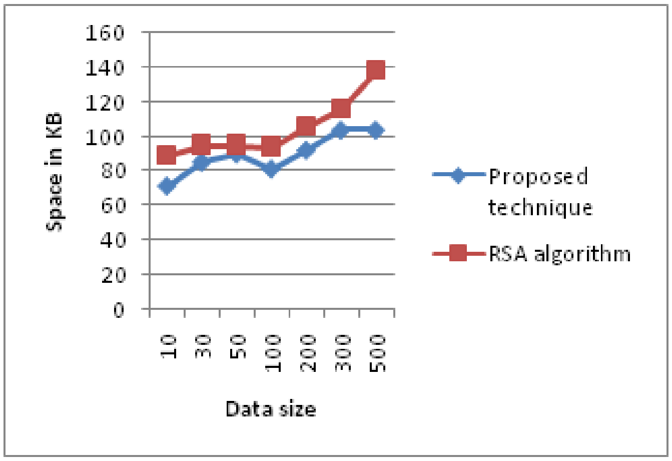
To execute the encryption process for encryption of the input file is termed here as the encryption memory. The memory consumption is also known as the space complexity of the algorithm. InGiven graph X - axis shows the amount of file size utilized for experimentation and the Y axis shows the corresponding amount of main memory used. The memory consumption of algorithms is measured in terms of KB (kilobytes). Additionally to represent the performance of the techniques the blue line shows the performance of the proposed technique and the red line shows the performance of traditional RSA algorithm. According to the obtained results the proposed technique efficient and consumes less amount of memory as compared to the traditional cryptographic technique.



Graph 4 Encryption Memory

4.5 Decryption Memory

The amount of main memory required to compute the original file is termed as the memory consumption of algorithm or the space complexity of the decryption algorithm. The space complexities of both the implemented algorithms are given using graph. In the given graph X axis includes the different files that are used for experimentation and the Y axis show the memory required to execute the encryption algorithm. According to the obtained performance the proposed technique requires less amount of main memory as compared to traditional RSA algorithm.



Graph 5 Decryption Memory

V. CONCLUSION AND FUTURE WORKS

The cloud computing is new generation computational and storage infrastructure. A number of individual users and the organizations are getting benefits from the cloud infrastructure. Due to their popularity and the dynamicity of network and storage context the security of the data storage and access are the key area of concern. In this presented work the cloud security and the access control mechanism is investigated in this work. In access control a key component is authentication and data access. Therefore in this work the authentication is the key area of study in the cloud environment. Additionally to secure the data the cryptographic technique is also implemented that provides the security during the data access and network based attacks. To secure the data in cloud environment the data attributes are used to prepare the key for data and the user access on the data by including the three factors. Additionally to secure the data in cryptographic manner the DES algorithm is also used that preserve the data during the network transmission and storage on server. The proposed work to enhance the technique of authentication and security of cloud data access is studied and a new technique for encryption and authentication is proposed and implemented. The proposed technique found adoptable due to less resource requirements.

Future Works

1. The proposed technique only considers three factors for computing the authentication requirements for the specific data and their access in near future more parameters are required to involve for improving security and data access
2. The technique is currently used with the a file sharing technique, in near future that is provided for secure data sharing in social media domain for finding the real performance and impact of the proposed methodology.

REFERENCES

[1] Peter Mell and Tim Grance, "The NIST definition of cloud computing", at National Institute of Standards and Technology, Gaithersburg, MD 20899-28930, September 2011.

[2] Chun-I Fan, Pei-Hsiu Ho and Ruei-Hau Hsu, “Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications”, IEEE/ACM Transactions on Networking, Vol. 18, No. 3, June 2010.

[3] Wen Shenq, Juang, Sian Teng Chen and HorngTwuLiaw, “Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards”, IEEE, Transaction on Industrial Electronics, Vol. 55, No. 6, June 2008.

[4] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus, NIST Special Publication 800-63-1 “ Electronic Authentication Guideline” [online] Available.

[5] PrachiSoni, (Asst. Prof.) MonaliSahoo, “Multi-factor Authentication Security Framework in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, January 2015.

[6] T.S SadhamHussain, Mr.M.MohammedSithik M.E, “An Identity based Batch Verification Scheme ForAuthentication Provision in VANETs”, International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)Vol. 2, Issue 4, April 2016

[7] TalapareddySusmitha,Endela Ramesh Reddy, “Implementation of Security for Web Services Using of TrusteeBasedAuthentications from User Friends”, international journal & magazine of engineering and technology, management and research vol 2 (2015), issue no 8

[8] “Multifactor authentication (MFA)”. Available online: http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

[9] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in Proc. of the IEEE Symposium on Security and Privacy, 2012, pp. 553–567.

[10] K. Killourhy and R. Maxion, “Comparing anomaly-detection algorithms for keystroke dynamics,” In Dependable Systems Networks, 2009 DSN09, IEEE/IFIP International Conference on, 2009, pp. 125–134.

[11] F. Hao and D. Clarke, “Security Analysis of a Multi-Factor Authenticated Key Exchange Protocol”, TECHNICAL REPORT SERIES, Newcastle University, 2012

[12] E. Syta, S. Kurkovsky, and B. Casano, "RFID-Based Authentication Middleware for Mobile Devices," in System Sciences (HICSS), 2010 43rd Hawaii International Conference on, 2010, pp. 1-10.

[13] A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud Authentication Based on Anonymous One-Time Password," Ubiquitous Information Technologies and Applications Volume 214 of the series Lecture Notes in Electrical Engineering PP. 423-431, 20 November 2012.