2CAuth: A New Two Factor Authentication Scheme Using QR-Code

N. Harini[1] and Dr. T.R Padmanabhan[2]
Department of Computer Science and Engineering,
Amrita Vishwa Vidyapeetham, Coimbatore, India.
n_harini@cb.amrita.edu , trp@amrita.edu

Abstract - Password based schemes has been the standard means of authentication over decades. Enhancements use entities like ownership (something one possess), knowledge (something one knows), and inherence (something one is) as first factor and mobile phones as token less second factor, in combinations, to offer different levels of security assurances, trading off usability. In this paper we present '2CAuth' a new two factor authentication scheme that enhances secure usage of application information and preserves usability, without sacrificing user's privacy. A significant feature of the scheme is that it DOES NOT call for any synchronization between Mobile Network Operator (MNO) and users. The analysis of the scheme clearly brings out its effectiveness in terms of its usability even at times of peak loads on mobile networks. The scheme has the dual advantage of carrying out the verification of transactions which involve the physical presence of the user as well as those to be done in his absence.

Keywords - Two factor authentication (2FA), QR-code, privacy, authentication, peak load, security, 2CAuth

I Introduction

Many of the services that we use daily, for example banking, have transformed from traditional customer services into Internet services. As services that contain sensitive data are moved to Internet, strong authentication is required to provide a high enough level of security and privacy. With computing becoming pervasive, people increasingly rely on public computers to do business over the Internet thus making it a preferred environment for a multitude of e-services like e-commerce, e-banking, etc. Security for these applications is an important enabler.

In general, the password based authentication mechanism provides the basic capability to prevent unauthorized access. One-time passwords make it more difficult to gain unauthorized access to restricted resources. Many researchers have devoted efforts to implement various OTP schemes using smartcards, time-synchronized token or SMS etc.

Security risks are more pressing as attacks become more daring. This makes systems that rely on single factor authentication more vulnerable and at risk calling for authentication using multiple factors. In this paper, we introduce, implement and analyze an efficient, robust, scalable, and easy to use web authentication system called '2CAuth'. The proposed method is based on ownership (smart code and Mobile) and knowledge (Security Code) factors. It combines the above factors with OTP and challenge response methods without requiring any time synchronization between user's mobile phone and service provider's server for authentication purpose.

The rest of the paper is organized as follows section 2 presents literature review, section 3 describes the motivation for the work and the contributions of this paper. Section 4 discusses the proposed scheme and its details. Section 5 presents the analysis of the scheme and finally Section 6 presents the conclusions.

II Literature Review

2.1 Authentication

Despite the advantages, Internet is vulnerable to various threats from cyber criminals, hackers, unprincipled authorities, etc. Such threats take varied forms like unauthorized access, unprivileged activity, repudiation, manipulations on stored content. Implementation of strong solutions for authenticating an individual's identity before allowing access to resources is a major requirement for any Internet service. In general, an individual must prove his/her identity; a credential is then established that asserts proof of the individual's identity. Three types of factors are available to tie an individual to an established credential [2]: ownership (something one possess, such as a Badge), knowledge (something one knows, such as a password), and inherence (something one is, biometric data-fingerprint/iris pattern). The specific evidence an individual provides to support each factor (the card, the password, the fingerprint) is called an authentication token. Multiple factors can be used, and each can be supported by a variety of apt tokens, ranging from simple passwords to information encrypted using the public key infrastructure (PKI). Empirical research on information quality delivery over the Internet application clearly brings out that online security during exchange of information on the Internet is still a critical issue[3].

2.2 Multifactor Authentication

As hacking technologies have become more diversified and advanced, security offered by single-factor authentication has been found to be vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, , dictionary attacks, shoulder surfing etc. In order to increase the security it has now become very common to combine multiple authentication factors. In recent times, there has been an increase in usage of multi-factor authentication. The required number of authentication factors may be decided based on, transaction types, risk levels, threats and vulnerabilities.

2.3 Mobile phones on Internet

The use of the Internet on smart phones and other mobile devices has changed the way people communicate and use information, creating an exponential rise in the acceptance, adoption, and usage of data. The rise of the mobile systems and the widespread adoption of the cell phones make it an exciting domain for Internet applications. Mobile phones have evolved from simple voice communication dominated electronic devices to powerful digital handsets with multiple roles such as digital camera, video recorder, radio, MP3 player, web browser, gaming terminal, GPS navigator etc. Mobile phones provide secure 2FA that does not require the user to carry around an additional physical device and hence have opened up the possibility of being used as token less authentication factor.

2.4 QR Code based authentication

QR-code(Quick Response Code) based OTP authentication protocol [4], eliminates the usage of the password verification table and also is a cost effective solution since most internet users already have mobile phones. There are many advantages to use the QRcode [8] in mobile phones such as Omni-direction readability and error correction capability.

2.5 Existing 2FA schemes

So far, researchers have proposed many remote authentication schemes that combine several factors including simple passwords, one time passwords either SMS-based or time synchronized, public-key infrastructures (PKIs), biometrics etc. Most of the 2FA schemes authenticate users based on what they know and what they have incorporating token less second factor (mobile) for authentication. Each method has a reason to exist, based on design criteria for the overall usage. Online banking is the good example where strong remote authentication is guaranteed using two-factors as de facto standard. In practice, the first factor is usually in the form of PIN or password that the user types, for instance, into a web-based Internet application. The second factor is usually in the form of mobile phone that is known to be able to receive OTP as SMS directed to a particular mobile phone number. If the user successfully retypes this OTP into the web application, the second authentication factor is regarded as successfully verified (i.e. the user has the mobile phone). Security of the aforesaid scenario relies on practical difficulty for an attacker to compromise the operating environment of both the particular phone and the web browser where the user part of the serving application runs. The SMS transmission delay represents one of the major limitations of the traditional system. Turning off the roaming service will prevent the bank from sending the SMS-OTP, which in turn, stops the user from resuming any further processes. To overcome the aforementioned problem researchers have also proposed authentication using mobile phone generated OTP. These methods require time synchronization between users mobile and service provider.

2.1 Internet Architecture

The changeover from the academic Internet to a multifunctional business Internet puts much higher requirements on the architectural supports to control and balance the interests of all stakeholders (like users, service providers, data owners, etc.).Their hopes and expectations for new applications and services demand new architectures that overcome the fundamental limitations of Internet like lack of data identity, lack of methods for reliable processing , real-time dispensation, scaling to deal with flash crowds and so on.

Since its creation, the Internet is driven by a small set of fundamental design principles rather than being based on a proper formal architecture that is created on a whiteboard by a standardization or research group. The architectural principles and design model of the Internet is all about processing, storing, transmitting and controlling data. As this trend is definitely expected to escalate in the future, there is a clear need for extensions, enhancements and re-engineering in Internet architecture. While improvements are needed in each dimension, these should be combined by undertaking a holistic approach.

A recent work reported “A secured-concurrent-available architecture for improving performance of web servers MLF (Multi Layer Filtering)” [1] is an end-to-end framework that achieves robust performance on a wide range of Internet services subject to huge variation in load. The model categorizes resources into two types namely replicated (e.g. E-commerce) and non-replicated (E.g. intelligence reports).

However enabling users to use Internet Services safely and efficiently using an authentication method that is generic as far as possible and can accommodate technological innovations and contributes particularly at times of overload is required.

2.7 Summary of Findings

The Internet has evolved as the most important means for information exchange and a foremost communication environment for business relations and social interactions. The rapid growth of Internet of Things and Services clearly illustrates that the ever increasing amount of physical items of our daily life which become addressable through a network could be made more easily manageable and usable through the use of Internet services. This course of exposed resources along with the level of privacy and value of the information they hold, together with increase in their usage, escalates the number of the security threats and violation attempts that existing systems do not appear robust enough to address.

The practical requirements for the Internet have changed considerably since 1975, and they will continue to change. Architecture of tomorrow must meet the changing requirements of the Internet, ISPs, and Users etc. Perhaps one of the most compelling problems of the modern Internet is the lack of a comprehensive and unifying approach to deal with service concurrency, security, and availability.

Web applications are increasingly the preferred targets of cyber-criminals looking to profit from identity theft, fraud, etc. The impact of an attack can be major, and includes costly and embarrassing service disruptions, down-time, lost productivity, stolen data, regulatory fines, angry users and irritated customers.

Strong authentication has no precise definition; it is not a strictly mathematical concept with quantitative measurements but rather a qualitative measure that is evaluated using a relative scale. The potency of an authentication process depends on the number of factors involved, the trustworthiness of the token associated with each factor, and the assurance level that an authentication token is neither compromised nor circumvented.

Smartcard [5] technology provides an excellent platform for implementing strong authentication. Smartcards can support and protect authentication tokens, storing password files, PKI certificates, one-time password seed files, and biometric image templates securely. A smartcard used in combination with one or more authentication tokens provides strong multifactor authentication that can significantly strengthen logical access security.

The SMS-OTP [7] is a simple idea that can be used for two factor authentication. It is based on password that is generated by the service provider and transmitted to user using the SMS service. This kind of system is being used in many services, for example some e-banks. In fact SMS-OTP is overall fairly good mobile authentication method, at least for services that do not require very heavy protection.

The following two aspects of the underlying problems are of relevance here:

- Sending an SMS-OTP to the user for every logon which may be costly with the consideration of statistics of transactions.
- Sending a fairly short password (usually as plain text) which is valid only once and only for a short period of time. The MNOs cannot guarantee SMS text message delivery within an acceptable timeframe for 100 percent of all SMS messages delivered (SMS traffic is not sent point to point, it is queued and then sent on to the required network cell where it is again queued and finally sent to the end users phone). There are times when the mobile network is overloaded, e.g. peak times at events and natural disasters. Late delivery of an OTP contained in an SMS text message can be problematic for a time critical login that can mean no access to critical enterprise resources [6].

This brings out a clear need for a new authentication process that overcomes the problems associated with SMS-OTP.

2.7 Problem Statement

The primary goal is to implement an efficient, robust, scalable, and easy to use web authentication system. We present and analyze the authentication scheme 2CAuth that combines ownership factors (something the user has mobile, smartcard) with knowledge factors (OTP). The method is based on smart card and optical challenge response solution in which a camera equipped mobile phone is used for the purpose of authentication. The security of the scheme is improved by using a type of knowledge-based authentication challenge to the user's smart phone rather than a code displayed in clear text. This solution has high usability due to its ease of use, easy deployment and cost effectiveness.

III Motivation

We understand that the privacy information of the user is closely related to the security in authentication. The motivation of this work is to propose and analyze a systematic 2FA which protects user's privacy as well.

3.1 Contributions

The main contribution of this paper is the proposed 2CAuth scheme that has the following merits:

Firstly, smartcard used does not have any secret code to be stored. Secondly, the scheme uses true authentication by expecting the user to possess the Smartcard, Secret-pin and Registered Mobile Phone with him to carry out a transaction without requiring any synchronization with MNOs. Thirdly, the server that authenticates the user does not require any credential (secret) of the user to be stored in it. Finally, the significant feature of the scheme is its usability even at times of peak load on mobile network.

IV The Proposed Scheme

In the proposed method the entity being authenticated must possess the following

- Valid smartcard
- A camera for capturing QRcode.

4.1 Notations

Table 1. Notations

Sl No	Notation	Particulars
1	U_i	i^{th} User
2	ID_i	Unique Identifier of i^{th} User
3	$PWDi_1$,$PWDi_2$	Password 1 and 2 of the i^{th} User
4	d	Private key in RSA
5	e	Public key in RSA
6	n	Computed as product of chosen prime numbers (p and q)
7	g	Generator element
8	SID_i	Smartcard Identifier of i^{th} User
9	IMEI	International Mobile Station Equipment Identity
10	IMSI	International mobile subscriber identity
11	K	Unique Key for mobile of i^{th} user
12	R_1 and R_2	Random numbers chosen for verification
13	P	Prime number chosen during registration phase (Different from primes chosen for RSA key pair initialization(p,q))

4.2 Registration Phase

Firstly, the user needs to become a legal registered user of the server. The registration process is assumed to be done in the physical presence of the user. In case the scheme has to be modified for a case where the registration is to be done in user's absence then a private secret channel may be established to carry out the below said operations. The overall registration process is illustrated in Fig. 1.

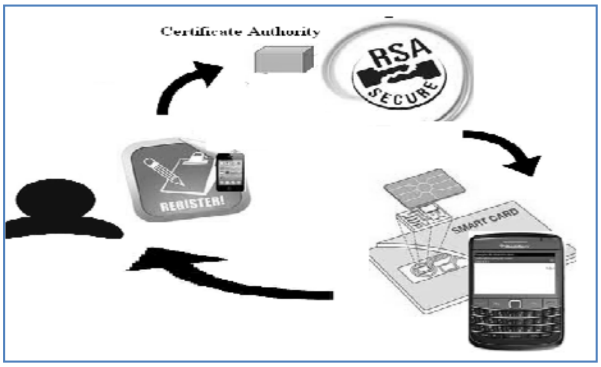

Fig.1. Registration Phase

4.2.1 Registration Process

The sequence of operations that takes place during registration are as follows:

1) User Ui submits his IDi and the chosen passwords - $PWDi_1$,$PWDi_2$
2) AS then generates an RSA key pair, namely a private key d and a public key (e; n). and publish (e; n); d is kept secret with AS itself.

3) AS determines an integer g, which is a primitive in both GF_p and GF_q where p and q are the prime numbers used when generating RSA key.
4) AS generates a smart card identifier SIDi for Ui and calculates the user's secret information as
   $Ai = ID^{SIDi * d}$ mod n.
   Where n = p * q.
5) AS computes $Bi = g^{PWDi1*d}$ mod n
6) The user also needs to register a mobile number with the server.
7) AS generates a unique ID K = f (IMEI,IMSI).
8) AS computes $C_{i1} = g^{K*PWDi2}$ mod P
9) The following Information {ID_i, SID_i, A_i, B_i, C_{i1}, e, n, validity period} is written on the smartcard. The computed C_{i2} is stored in the registered mobile.

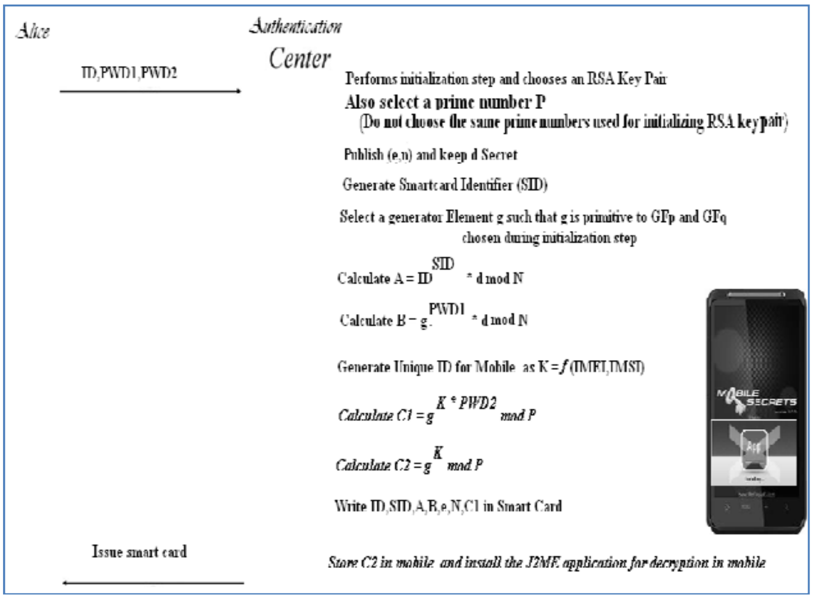
Alice
Authentication Center
ID,PWD1,PWD2
Performs initialization step and chooses an RSA Key Pair
Also select a prime number P
(Do not choose the same prime numbers used for initializing RSA key pair)
Publish (e,n) and keep d Secret
Generate Smartcard Identifier (SID)
Select a generator Element g such that g is primitive to GFp and GFq chosen during initialization step
Calculate A = ID^SID * d mod N
Calculate B = g^PWD1 * d mod N
Generate Unique ID for Mobile as K = f (IMEI,IMSI)
Calculate C1 = g^K * PWD2 mod P
Calculate C2 = g^K mod P
Write ID,SID,A,B,e,N,C1 in Smart Card
Issue smart card
Store C2 in mobile and install the J2ME application for decryption in mobile
MOBILE SECRETS

Fig.2. Steps in Registration process

Fig. 2 illustrates the steps during registration process. The following clarifications regarding the above sequence are in order here:

- The scheme has a clear need to make the identity of the card holder to be explicitly available to the verifier without revealing the secret *d*. The integer *g* selected here ensures this by making only $g^{PWDi1*d}$ *mod n* available for the verifier.
- Steps 1 to 5 in the sequence pertain to smart card registration, 6 to 8 to mobile registration, and step 9 specifies the tokens made available to the user for authentication purpose.

4.3 Authentication procedure

A detailed structure of verification procedure associated with smart card and mobile of the user is presented in this section. Fig. 3 illustrates the verification phase of the 2CAuth scheme.

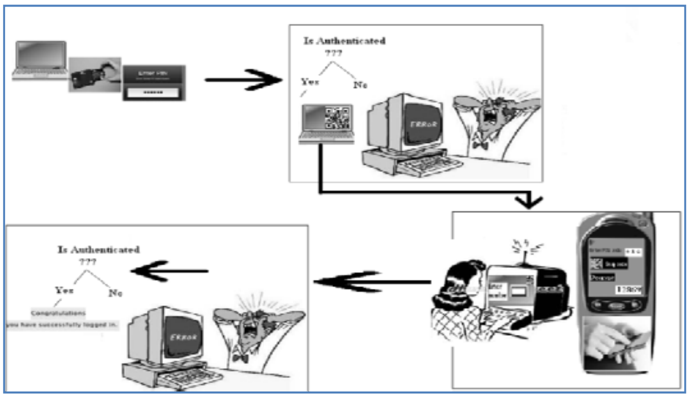

Fig.3. Verification Phase

4.3.1 Possession of smartcard

The user is required to provide the card information. The card Reader selects a random number R_1 and computes

$\mathbf{X_i = A_i{}^{R}{}_{1}\ mod\ n}$ and

$\mathbf{Yi = B_i * X_i\ mod\ n}$.

The reader then verifies the authenticity of the user by verifying

IF $\mathbf{Yi^{e\,=}{}_{IDi}{}^{SIDi} * X_{i.}}$

Fig. 4 illustrates the verification of possession of smartcard as carried out by the card reader.

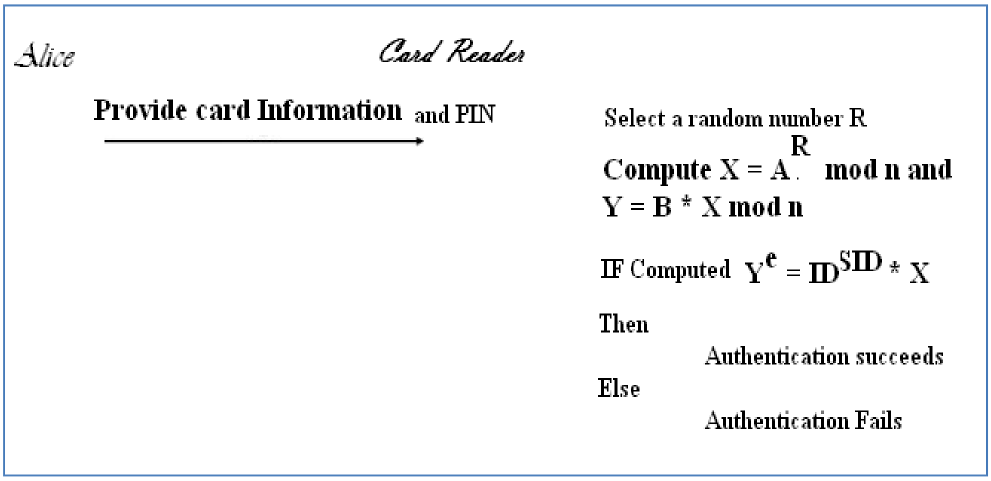

Fig.4. Verification of smartcard

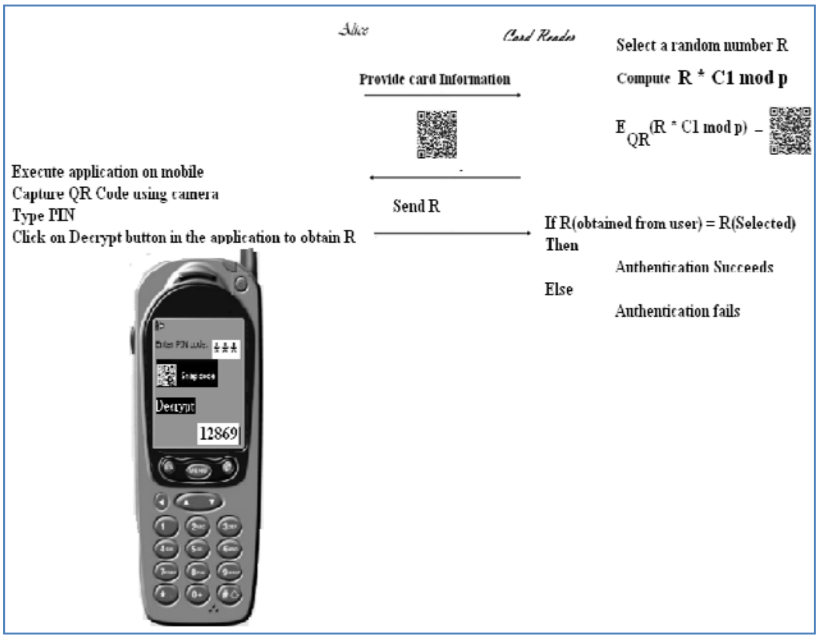

Fig.5. Verification of Mobile phone

4.3.2 Possession of mobile phone

The card reader selects another random number $R_{2.}$ It encrypts (R_2 * C_{i1} mod p) into a QRcode and displays it for the user. The user has to capture the QRcode displayed and execute the software installed on his mobile that gets C_{i2} stored in the mobile and PWD_{i2} from the user, and decrypts the captured code as $D_{QR}(Ci2^{-PWD2i} * E_{QR})$ where E_{QR} is the encrypted QRcode clicked and captured by the user. The obtained result of decryption is then typed into the web application by the user. If the user types the random number correctly it is regarded as the second factor is verified. Fig. 5 illustrates the verification of possession of mobile phone.

4.4 Changing Factor

Our framework also supports changing the mobile numbers, and any other authentication factor of users. To do this the user needs to contact the administrator and redo the registration phase with the new mobile number and existing Unique ID. Change of public and private keys is also possible in the same manner.

V Analysis of the protocol

As the focus is on investigation of a systematic approach for the design of secure multifactor authentication scheme it is almost like all generic constructions. This paper does not address the benefits that could be realized from the computational point of view

5.1 Feasibility Evaluation

The convenient integration of the web-based application and the mobile devices' usage makes our scheme more practical. The mobile phone embedded with a camera only need to carry out a QR-code decoding operation. Obviously the overall computational load is acceptable. In addition, no extra cost is incurred for creating and maintaining the password table that store long-term secret keys of users. This substantially decreases the risk of tampering and maintenance cost successfully.

5.2 Correctness

If **ALL** authentication factors {*Smartcard, Smartcard_Pin, Mobile_Init_Secret, Mobile_Pin* } are correct then authentication succeeds else authentication Fails.

5.3 Security evaluation

This section shows how the proposed method resolves possible threats.

5.3.1 Password Guessing

The scheme avoids threats related to the password guessing/stealing via social engineering and so on; are avoided by using two-factor authentication which requires attackers require both tokens (mobile and smartcard) in order to reconstruct the necessary information.

5.3.2 Resistance to impersonation

A hacker H who tries to get authenticated has only a negligible probability in impersonating an honest user U. This remains to be true unless he steals the smart card, mobile phone and the two pins used for authentication.

5.3.3 Smart card holder

This type of attacker has the smart-card, and can read and modify the data in the smart-card. It is required to restrict (read/modify) access to data in the smart-card using appropriate techniques. However, from the security point of view, the proposed authentication method will be more robust as it requires the users to have both the factors (Mobile with pin and smartcard with pin) for authentication purpose.

5.3.4 Mobile holder

The attacker is assumed to have the mobile of the user but is not given the smart-card and secret PINS of the legitimate user.

5.3.5 Resistance to Replay attack

As only new session keys (OTP) are used to authenticate the users and these are used with strict time constraints the probability of this type of attack is negligible. Resistance to this attack

is achievable by setting the time limit for which the random number is valid and by restricting the number of login attempts.

5.3.6 Resistance to DDoS attack

The MLF framework effectively filters DDoS attacks well ahead of request reaching the verification phase as can be seen from Fig. 6. The proposed authentication process happens in Stage II of the MLF framework at its Access Node component. Details are available in [1].

VI Conclusions

The established password based authentication schemes need to be enhanced to counter the powerful and varied attacks of today. The problem has been addressed by researches by resorting to two and three factor authentications. These schemes offer different types and levels of security and demand corresponding complex authentication sequences and computational efforts.

The ubiquitous use of smart phones has been taken advantage of in the 2FA proposed in the paper. The scheme - '2CAuth' (based on RSA & El-Gamal) uses the users password as one factor and ID embedded in the smartcard and smart phone as the second factor.

A detailed analysis of the proposed scheme has clearly brought out its advantages. Possibility of authentication at peak load times without need for synchronization with MNO is the first of these. Further the vulnerability associated with the *in absentia verification* of the user is effectively handled by the scheme. Moreover, this scheme aptly fits at the access nodes in the MLF architecture making it more user-friendly without sacrificing security assurances.

The proposed scheme opens up the need for a critical look into the practical threats and related analysis. This can possibly lead to the development of a generic and concrete Three-Factor Authentication (3FA) scheme that can offer security assurances for protecting even classified data.

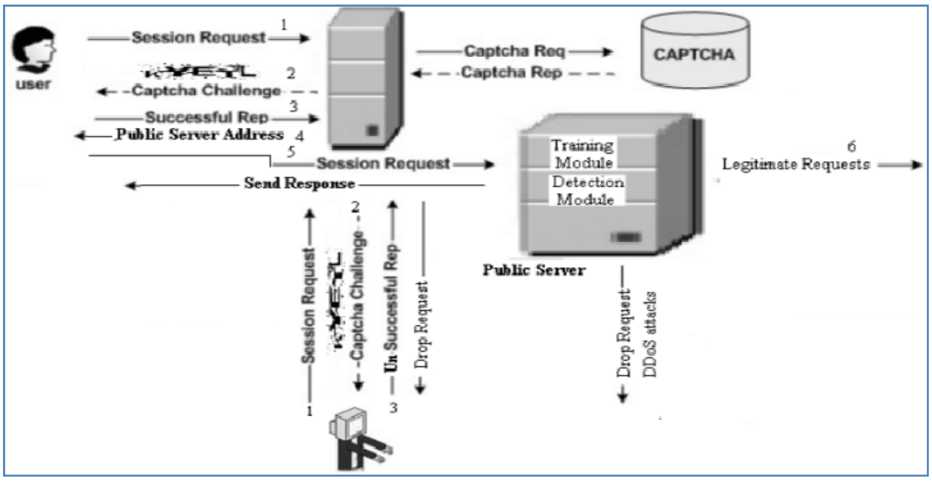

Fig.6. Stage I of MLF architecture

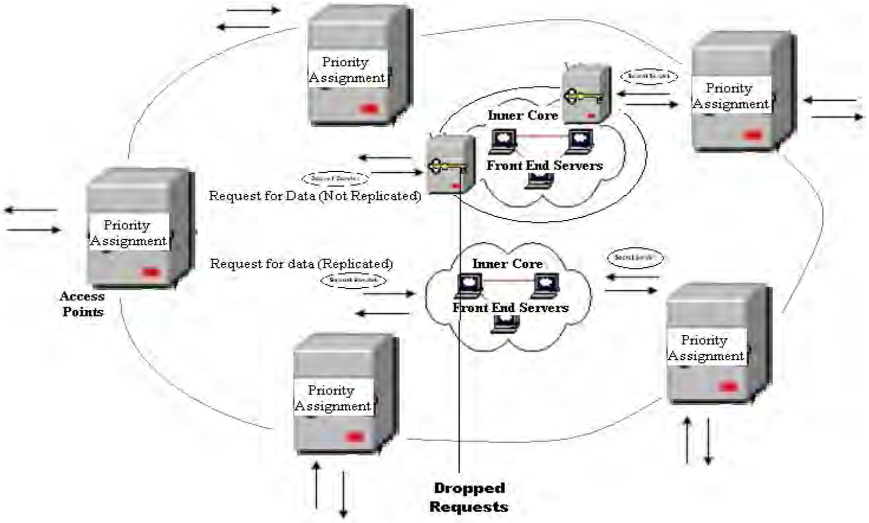

Fig.7. Stage II of MLF architecture

REFERENCES

[1] N. Harini and Dr. T.R. Padmanabhan, "A Secured-Concurrent-Available architecture for improving performance of web servers", Journal of Communications in Computer and Information , August 2012, Springer.

[2] N Harini, Dr T.R Padmanabhan and C.K Shyamala, " Cryptography and security", Wiley India, First Edition, 2011.

[3] African Journal of Marketing Management Vol. 3(8), pp. 188-194, August 2011 Available online http://www.academicjournals.org/ AJMM ISSN 2141-2421 ©2011 Academic Journals

[4] Kuan-Chieh Liao and Wei-Hsun Lee, "A Novel User Authentication Scheme Based on QR-Code",Journal of Networks, VOL. 5, NO. 8, AUGUST 2010

[5] Rajaram Ramasamy and Amutha Prabakar Muniyandi, " An Efficient Password Authentication Scheme for Smart Card", International Journal of Network Security, Vol.14, No.3, PP. 180-186, May 2012

[6] "Two-Factor authentication goes mobile", First Edition September 2012, www.goodeintelligence.com.

[7] Fadi Aloul, Syed Zahidi , Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones"

[8] A. Sankara Narayanan, "QR Codes and Security Solutions", International Journal of Computer Science and Telecommunications ,Volume 3, Issue 7, July 2012.