3C-Auth: A New Scheme for Enhancing Security

Narasimhan Harini and Tattamangalam R. Padmanabhan
(Corresponding author: Narasimhan Harini)

Department of Computer Science and Engineering & Amrita University
Amritanagar P.O., Ettimadai, Coimbatore 641 112, India
(Email: nharini2003@gmail.com)

(Received Aug. 1, 2013; revised and accepted May 20 & Nov. 3, 2014)

Abstract

A multi factor authentication scheme called '3C-Auth' is proposed in this paper. The scheme carries out a comprehensive authentication process using the smart card, secret-pin, registered finger print, and registered mobile number of the user. The user's password is neither transmitted in plaintext form nor revealed to the authentication server. The scheme is shone to be proof against phishing, password guessing, replay, or stolen-verifier attacks. Resistance to parallel session and denial of service attacks and the use of QR-Code in preference to SMS for OTP transfer together, make the scheme attractive for operation under peak loads. Integration of the "3C-Auth" into Multi-Layered Filtering (MLF) scheme leads to secure handling of peak loads on the server ensuring concurrency and availability as well. This clearly enhances the QoS in terms of making right admittance to right resources.

Keywords: Authentication, peak load, QR-code, smart-card

1 Introduction

As Internet services become more popular and pervasive, a serious problem that arises is managing the performance of services under intense load. One of the most challenging problems for public Internet is the delivery of performance targets to users given the randomness of Web accesses. Internet has become indispensable for business and more and more people rely on it for their day to day activities; in turn it evolves continuously and is subject to more and more cyber security threats. Analysis of security breaches and other cyber security issues with particular focus on personal privacy and data security have been active research issues over the past two decades. A multifactor authentication scheme named "3C-Auth" is presented in this paper that uses true authentication to protect resources with high security requirements; it expects the user to possess all the tokens (smart-card, secret-pin, registered finger print and registered mobile phone) to prove his/her identity.

Rest of the paper is organized as follows: Relevant research in literature which forms the motivation for the present work is reviewed in Section 2. Sections 3 and 4 detail the proposed scheme and analyze its performance. Integration of the scheme with MLF *(*Multi Layer Filtering) architecture [2, 3] is presented in Section 5 and conclusions are in Section 6.

2 Related Work

2.1 Internet Architecture

The changeover from the academic Internet to a multi-functional business Internet puts much higher requirements on the architectural supports to control and balance the interests of all stake holders (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 white board by a standardization or research group. The architectural principles and design model of the Internet are all about processing, storing, transmitting and controlling data. This trend is bound to escalate in the future, pointing to a clear need for extensions, enhancements, and re-engineering in Internet architecture. While improvements are needed in each dimension, these should be cohesive demanding a holistic approach. The architecture can be generalized to suit different categories of applications by integrating the admittance control policies that provide metric based differentiation and consecutively maximize the profit earned for having serviced a certain class of requests [16]. Research in this area has identified some key approaches to face overload, such as admission control (per request, per session), request scheduling, service differentiation, service degradation, and resource management.

2.2 Current State of Internet Services and Authentication Requirement

The following form the key features of the state of art of internet services:

- Generic nature;
- Accommodation of technological innovations;
- Robustness at times of overload.

As access to more and more services is pushed online, the range of sensitive information that a user must protect widens with time. It is also equally important to understand that complicated security schemes will not achieve widespread adoption among Internet users. Today hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, *etc.* – Implying that businesses should use commensurate secure approach. The challenge here is to balance strong security with usability. One Time Passwords (OTPs) for single session/transaction usage have been identified as the best way of protecting online transactions.

2.3 Authentication Schemes

In 1981, Lamport proposed a scheme to authenticate a remote user on a remote server over an insecure network. The requirement for storing verification tables used by the scheme was overcome by a scheme proposed in by [7]. Later [10] proposed a new remote authentication based on ElGamal crypto scheme exploiting tamper resistance property of smart cards. Most of the remote identity based remote authentication schemes proposed by researchers [7, 10, 13, 16] rely primarily on passwords for security. The schemes are vulnerable to dictionary attacks [6]. To overcome this problem random cryptographic secret key could be used [14]. However, such large key values (are difficult to be remembered and hence) require to be stored somewhere. Further these strong passwords and secret keys fail to provide non repudiation. An authentication scheme of Khan et al and Li et al uses biometric keys with advantages like “cannot be lost”, “difficult to forge”, “cannot be guessed” *etc.* [10] proposed an efficient biometric based smart card authentication scheme. [7] showed that the scheme makes two assumptions to ensure its correctness and security that may restrict its use for real time applications. [8] proposes a generic framework for preserving security in distributed systems. The three factor authentication scheme in [7] is based on password, smart card and biometric characteristics. The authors claim two benefits in the usage of fuzzy extractor:

- Elimination of the assumption of Li-Hwangs scheme that stores the hash of biometric template;
- Use of biometric authentication that supports reasonable tolerance.

In the analysis of their scheme the authors have shown how their protocol is secured against attackers of Type I (smart card and biometric), Type II (password and Biometric), and Type III (smart card and Password). Although the generic construction proposed by Huang et al satisfies the security requirements of three factor authentication the system may fail to secure resources that require very high degree of security the reason being biometric systems that are fast with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are rare even today.

2.4 Security with OTP

Authentication of users in a distributed environment is an increasingly difficult task. As network and software grow in sophistication so do means and methods of malicious attackers. Today computer crackers use enormous resources to obtain information necessary to impersonate other users. Authentication systems based on one time passwords [5] provide more reliability than those based on remembered/stored ones. Hence, security sensitive industries (banks, government *etc.*) deploy one time password systems to reduce the damage of phishing and spyware attacks.

2.4.1 SMS-OTP

Most of the two factor authentication schemes authenticate users based on what they know and what they have, incorporating token-less second factor *(e.g. mobile)*. Each method has a reason to exist based on design criteria for the overall usage.

Online banking is a 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 the practical difficulty for an attacker to simultaneously compromise the operating environment of both the particular phone and the web browser where the user part of the serving application runs.

2.4.2 Problems with SMS-OTP

The main problems with the SMS-OTP design are under overloaded situations. These are:

- Delay in delivery of SMS;
- Low Coverage Areas;
- Non-availability of Mobile Phone;

- Downtime with SMS Gateway;
- Non-availability of service for roaming user;
- High Cost for roaming user;
- Complexity associated with sequence of operations in obtaining OTP from SMS when mobile phone is used for connecting to the Internet.

2.4.3 Authentication Using QR Code

In 2002, Clarke et al. suggested the usage of camera-based devices as an alternative but more secured authentication method for critical transactions with un-trusted computers. With the explosive growth in the amount of camera-equipped smart phones around us mobile based authentication [11] may become a popular authentication method in the near future. QR-code (a two-dimensional barcode) - as introduced by Japanese company Denso-Wave in 1994 is a more effective alternative. Its error correction capability facilitates data restoration even under conditions when substantial parts of the code are damaged. Modern cellular phones are natively equipped with the QR-code decoding software. Fortunately, for camera phones that are not equipped with QR-code readers, Quick-Mark and i-nigma are free tools that are available for many manufactured models and devices to decode QR-Codes free of cost. Depending on the data recognized and the nature of the application.

2.4.4 Summary of Findings

Internet has become the most important platform for business relations and social interactions. The rapid growth of Internet of Things and Services clearly shows 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, has led to the escalation in the number of security threats and violation attempts that existing systems do not appear robust enough to address. Internet architecture of tomorrow must meet the changing requirements of the Internet, ISPs (Internet Service Providers), 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 particularly at times of overloads. It is also important to understand that the internet and its users are under continuous attacks *i.e.*, security is the underlying problem for many of the Internet services. One has to clearly understand that the impact of an attack can be major, and can include costly and embarrassing service disruptions, down-time, lost productivity, stolen data, regulatory fines, 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 present sophistication level of hackers, demands authentication schemes to be based on more than one factor. Evaluating multi-factor authentication solutions calls for a look into the following measures:

- Security and scalability of the technology;
- Hurdles to user adoption;
- Cost;
- Deployability.

3 Proposed Scheme

The primary goal here is to enhance the performance of Multi-layered Filtering (MLF) scheme and enable real world applications to take advantage of this added functionality.

A scheme that performs admission control with enhanced multi factor authentication “called 3CAuth”, is proposed in this paper and the same evaluated for efficiency. The scheme provides true authentication by expecting the user to possess all the relevant tokens (smart card, secret-pin, registered finger print, and registered mobile phone) to prove his/her identity.

The benefits of the scheme include:

- NOT revealing users password to the server;
- NOT transmitting passwords in plaintext over the Internet, and at the same time;
- RESISTING the major possible attacks like replay attack, password guessing attack, stolen-verifier attack, and phishing attack.

The scheme operates in two phases namely registration and login-authentication. Table 1 is the notations used in the two phases.

3.1 Registration Phase

Figure 1 depicts the activities in the registration process. As shown in Figure 1 it involves the steps/activities in Algorithm 1.

The sequence of operations for registering ONE user is illustrated in Figure 2.

3.2 Login Phase

When U_i wishes to login to server (S), he/she must insert the smart card into a card reader, provide biometric data BF_i' , capture the QR code displayed on the web page, decrypt it using the software installed in the mobile, and present the OTP for authentication purpose. The sequence is shown in block diagram form in Figure 3.

Table 1: Table of notations

Notations	Description
U_i	i^{th} User
ID_i	Unique Identifier of i^{th} User
PWD_i	Password of the i^{th} User
d	Private key in RSA
e	Public key in RSA
n	Computed as product of chosen prime numbers (p and q)
g	Generator element primitive to $GF(p)$ and $GF(q)$
SID_i	Smart card Identifier of i^{th} User
IMEI	International Mobile Station Equipment Identity
IMSI	International mobile subscriber identity
MID_i	Unique Key for mobile of i^{th} user
R_1 and R_2	Random numbers chosen for verification
T_s	Time at which the request is generated
BF_i	Biometric feature of i^{th} user
R_c	Random Challenge (in this context - One Time Password)

Figure 1: Registration process

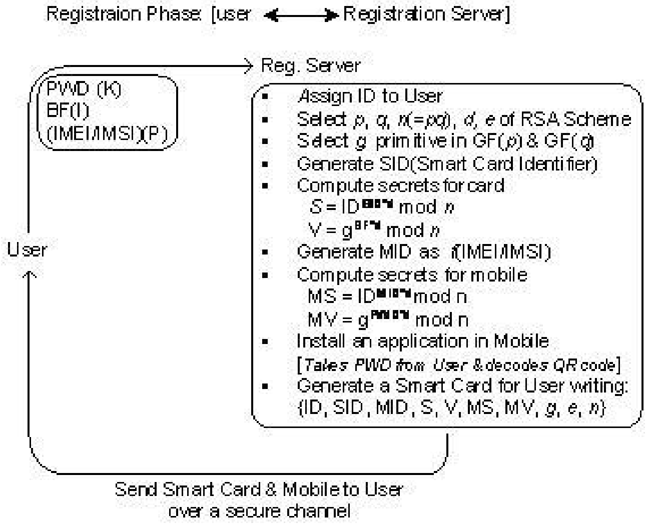
Registraion Phase: [user ⟷ Registration Server]
Reg. Server
PWD (K)
BF(I)
(IMEI/IMSI)(P)
Assign ID to User
Select p, q, n(=pq), d, e of RSA Scheme
Select g primitive in GF(p) & GF(q)
Generate SID(Smart Card Identifier)
Compute secrets for card
S = ID mod n
V = g mod n
Generate MID as f(IMEI/IMSI)
Compute secrets for mobile
MS = ID mod n
MV = g mod n
Install an application in Mobile
[Takes PWD from User & decodes QR code]
Generate a Smart Card for User writing:
{ID, SID, MID, S, V, MS, MV, g, e, n}
User
Send Smart Card & Mobile to User
over a secure channel

Figure 2: Registration process

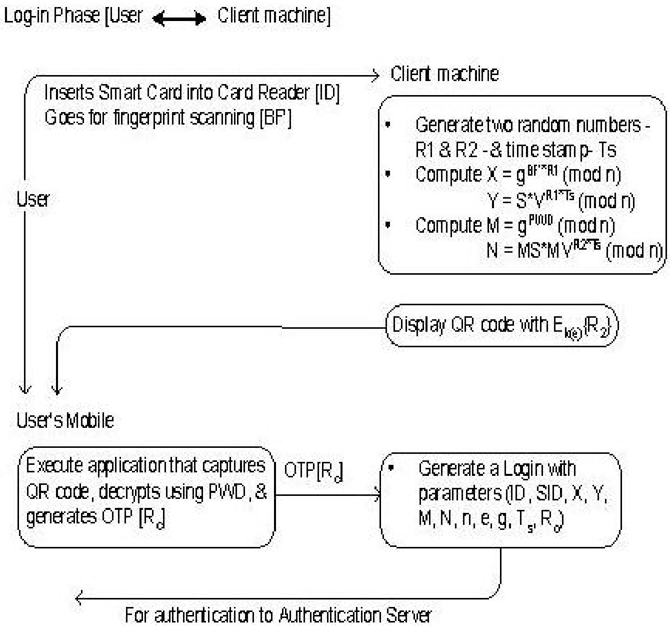
Log-in Phase [User ⟷ Client machine]
Client machine
Inserts Smart Card into Card Reader [ID]
Goes for fingerprint scanning [BF']
Generate two random numbers - R1 & R2 - & time stamp- Ts
Compute X = g^BF'*R1 (mod n)
Y = S*V^R1*Ts (mod n)
Compute M = g^PWD (mod n)
N = MS*MV^R2*Ts (mod n)
User
Display QR code with E_k(e)(R_2)
User's Mobile
Execute application that captures QR code, decrypts using PWD, & generates OTP [R_c]
OTP[R_c]
Generate a Login with parameters (ID, SID, X, Y, M, N, n, e, g, T_s, R_c)
For authentication to Authentication Server

Figure 3: Login phase

Algorithm 1 Steps in registration process

```
Begin
The user $U_i$ chooses a password $PWD_i$ and provides his/her biometric feature $BF_i$.
The registration server sequences through the following further steps:
while More users to Register do
    Assigns an $ID_i$ for the user and generates two large prime numbers $p$ and $q$, and computes
        $n = p * q.$
    For security reasons, the lengths of $p$ and $q$ are recommended to be 512 bits at least.
    Chooses integers $e$ and $d$ which satisfy
        $e * d \bmod ((p-1)*(q-1)) \equiv 1$
    Further it also finds an integer $g$ which is a primitive element in both $GF(p)$ and $GF(q)$.
    Generates a smart card identifier $SID_i$ for the user $U_i$. In addition it generates a mobile phone identifier: $MID_i = (IMEI, IMSI)$ for the user $U_i$.
    Calculates $U_i$'s secret information as
        $S_i \equiv ID_i^{(SID_i * d)} \bmod n$
        $V_i \equiv g^{(d * BF_i)} \bmod n$
        $MS_i \equiv ID_i^{(MID_i * d)} \bmod n$
        $MV_i \equiv g^{(d * PWD_i)} \bmod n.$
    Stores ($ID_i$, $SID_i$, $MID_i$, $S_i$, $V_i$, $MS_i$, $MV_i$, $n$, $e$, $g$) in the smart card, installs an application (for capturing and decoding QR code after obtaining secret pin from the user) in user's mobile and issues the smart card to the user $U_i$ over a secure channel.
end while
End
```

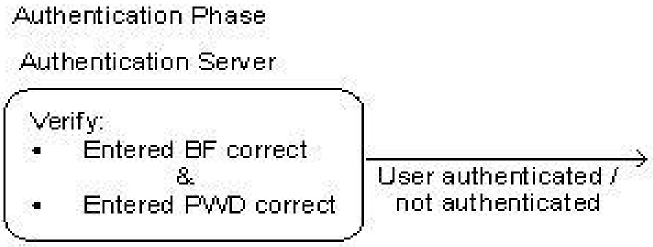

Figure 4: Authentication phase

Algorithm 2 Verification of possession of biometric characteristics and smart card

```
Begin
Check if $ID_i$ is a valid user identity and $SID_i$ is a legal smart card identity; if not reject the login request.
Check if $T_s$ is within the legal time interval limit due to transmission delay (may be initialized in SLA-service level agreement); if not reject the login request.
Verify if $Yi^e \overset{?}{\equiv} (ID_i^{(SID_i)} * Xi^{Ts} \bmod n)$;
The above equation holds iff $BF_i = BF_i'$.
i.e. the correct biometric value is provided during login phase. That is because
    $Yi^e \equiv (S_i * V_i^{(R1*Ts)} \bmod n)^e$
    $\equiv ID_i^{(SID_i*d*e)} * g^{(d*BF_i*e*R1)} \bmod n.$
    (Since $d * e \equiv 1 \bmod n$ we have)
    $\equiv ID_i^{(SID_i)} * g^{(BF_i*R1)} \bmod n$
and
    $ID_i^{(SID_i)} * (Xi^{Ts}) \equiv ID_i^{(SID_i)} * g^{(BF'i*R1)} \bmod n;$
End
```

3.3 Authentication Phase

The authentication phase (Figure 4) is executed by the remote host to determine whether U_i is allowed to login or not. The steps in login process are shown in Figure 3.

The authentication server upon receiving the login request from the user verifies the possession of smart card, biometric feature, and mobile phone as described in Algorithms 2 and 3.

4 Strengths of 3C-Auth

Resistance of the proposed method to different possible security attacks is explained here.

4.1 Parallel Session Attack

Here an attacker impersonates a legitimate user by intercepting the login request (ID_i, SID_i, S_i, V_i, M_i, N_i, n, e, g, T_s) and attempting to modify it to succeed in authentication. However the attacker has no way of obtaining the Biometric feature BF_i, PWD_i, and the random numbers R_1 and R_2; hence he/she cannot compute M_i, N_i, X_i, and Y_i which are dependent on PWD_i and R_1; a valid request cannot be created and the attempt fails. Hence it follows that the proposed scheme is secured against this type of attack.

4.2 Password Guessing Attack

The attacker attempts to guess user's secret parameters here. Although, one can extract parameters (n, e, g, S_i, V_i, SM_i, VM_i) from the user's smart card, obtaining BF_i or PWD_i from the smart card without the knowledge of d from $g^{(d*BF_i)}$ and $g^{(d*BF_i)}$, is not possible. Thus the difficulty of obtaining the discrete logarithm secures the scheme from password guessing attack even under stolen smart card situations.

Algorithm 3 Verification of possession of secret-pin and mobile phone

```
Begin
Confirm if $ID_i$ is a valid user identity and $MID_i$ is a legal mobile phone identity; if not reject the login request.
Confirm if $T_s$ is within the legal time interval limit due to transmission delay (may be initialized in SLA-service level agreement) , if not, reject the login request.
Check whether the following equation holds: $Ni^e = ID_i^{(MID_i)} * Mi^{(Rc*Ts)} \bmod n$
    The equation here holds iff $R_2$ = Rc i.e the correct OTP is provided by the user during login phase. The correct OTP can be obtained only in the mobile on which the application software is installed during registration phase and only if the password provided to it is correct . This is because
    $Ni^e \equiv (MS_i * MV_i^{(R2*Ts)})^e \bmod n$
    $\equiv ID_i^{(MID_i*d*e)} * g^{(d*PWD_i*e*R2*Ts)} \bmod n$
    $\equiv ID_i^{(MID_i)} * g^{(PWD_i*R2*Ts)} \bmod n$
    and
    $ID_i^{(MID_i)} * Mi^{(Rc*Ts)} \bmod n$
    $\equiv ID_i^{(MID_i)} * g^{(PWD_i*Rc*Ts)} \bmod n;$
    If the login request is rejected three times the user account is locked. He/She has to contact registration server to unlock the account.
End
```

4.3 Resistance to Replay Attack

Intercepting the login request message (ID_i, SID_i, S_i, V_i, M_i, N_i, n, e, T_s) of a user U_i and replaying the same message to the server becomes useless because the card reader puts a new timestamp in each new login request. The equations

$$\begin{aligned} Y_i^e &\equiv ID_i^{(CID_i*X_i)} \bmod n \quad \text{and} \\ N_i^e &\equiv ID_i^{(MID_i)} * M_i^{r_1} \bmod n \end{aligned}$$

will fail during the authentication phase.

4.4 Denial of Service Attack

In the proposed scheme an adversary can use invalid ID, PWD and BFs and overload the server by continuously keeping it busy. Even though an initial filtering for this type of attacks takes place in Stage I of MLF architecture non-legitimate requests that pass Stage I of MLF are blocked by the proposed scheme. This is obvious from the fact that a valid login request cannot be created (as discussed in Section 4.1). Further after three unsuccessful attempts the scheme automatically locks the user's account; the same can be unlocked only with the help of registration server.

4.5 Resistance to Phishing Attacks

The aim of phishing is mainly to collect private information that can be used to impersonate victims. A possible reading of the QR code (and extracting the OTP) by a hacker yields only the encrypted value of R_1; even if he manages to access the data typed by user, the private key remains inaccessible thanks to the strength of the RSA scheme. Thus the phishing attempt fails.

5 Integration of 3C-Auth with MLF

MLF is a practical (secured-concurrent-available) end-to-end framework based on admission control policies - a strategy that achieves robust performance on a wide range of Internet services subject to huge variation in load. MPAC (Multi Phase Admission Control) [3] enhances MLF to maximize the reward earned for having serviced a particular class of requests. 3C-Auth scheme described here can be integrated with this enhanced MLF framework to make it more comprehensive by adding security assurance. The integration involves two steps namely:

1) Enhancing SLA to include new features specific to authentication;

2) Modifying admission control policy to support 3C-Auth.

The 3C-Auth process is to be inserted at Stage II of the MLF framework at the Access Node component. Request processing in Stage II of the comprehensive MLF scheme is illustrated in Figure 5.

5.1 Service Level Agreement

The SLA that spells out the scope of service providers' allotment to the e-commerce in terms of resource capacity and time commitment used in MPAC is shown as follows:

```
Contract: Ecommerce System
{
Service : Classification of Customers
Customer Class = {Premium, Ordinary, New}
Inter-session States = {Home, Browse, Item, Addcart,
BuyReq, BuyConfirm}
} { Service : Processing Requests (Peakload)
{
Availability >$minAvailability;
TimeBound <$maxDelay;
Throughput >$minThroughput;
Utilization <$maxUtilization;
WeightAdjustment(Forward) = $weight(Positive)
```

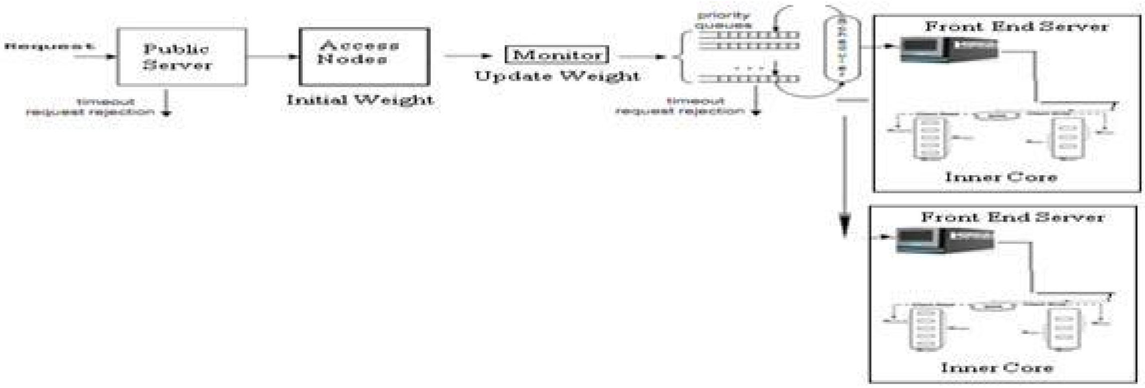

Figure 5: Request processing in Stage II of enhanced MLF (MLF+MPAC)

```
WeightAdjsutment(Backward) = $weight(zero,negative)
}
```

The template can be modified to support 3C-Auth by including the following specifications:

```
Security: Authservice
{
Service : Servicename /* Generic */
Resource Class = {Unclassified, secret,topsecret}
Factors Class = {Password/PIN, Hardwaretoken, Bio-Hard, Softtoken}
Protocol Class {None, 2CAuth,3C-Auth}
{ Service : News /* instance*/
Resource Class Unclassified
Registration{ }
Factors Class{}
Protocol Class {None}
} Service : Internet Banking
{ /* Announcements regarding new schemes for loans
{
Resources Class {Unclassified}
Registration { }
Factors Class { }
Protocol Class { }
} // Online banking
{
Resources Class {topsecret}
Registration {REQUIRED }
Factors Class {PIN, Hardwaretoken (Smart card), Softtoken}
Protocol Class {2CAuth[3]}
}
}
}
}
```

5.2 Admission Control Policy

MPAC uses a reward function defined by the application/service provider to improve the QoS using service differentiation. It computes the Expected Reward and the Cost Incurred in servicing the request and uses them as basic parameters to prioritize customers for E-commerce applications. The scheme can be made more comprehensive by re-computing priorities with authentication factors as well, for better security assurances. This is achieved in the comprehensive MLF framework (MLF + MPAC + 3C-Auth) as follows:

- Resources added to the pool are tagged with weights (based on SLA) that specify the number of factors required to access it;
- Incoming requests from Stage I are directed to the Access nodes by the public server for authentication;
- The access nodes proceed to authenticate users by assigning an initial weight of 0 to each request and updating it as per the credentials (number of factors) validated;
- Possessed weights are compared with the tagged weights associated with resources and in case of match in their weights access to the resource is permitted.

5.3 Results of Integration

The performance analysis demonstrated that the presented scheme performs a comprehensive authentication process satisfying the important requirements including friendliness, resistance to various kinds of sophisticated attacks, and stolen credentials. Further resistance offered by the scheme to parallel session attack and denial of service attack made the scheme more suitable for operation under peak loads. QR-Code based OTP has been found to show improved performance at peak load times compared to SMS-OTP method. With instantaneous SMS delivery the performance was on par with that of SMS-OTP scheme. The vulnerability associated with the in-absentia verification of the user is effectively handled by the scheme. Moreover, the scheme was found to be more user-friendly without sacrificing security assurances. With all these benefits contribution of the scheme towards improvement in QoS in terms of granting right access to resources can be considered significant.

6 Discussions and Conclusions

The proposed protocol is simple, fast and efficient if the user provides valid credentials for authentication. A detailed analysis of the proposed scheme has clearly brought out its advantages over authorization methods that use SMS to thwart attacks. Moreover, the scheme aptly fits at the access nodes in the enhanced MLF architecture making it more user-friendly without sacrificing security assurances. Improving in computational efficiency of the scheme is an interesting area of work; it can add substantially to its effectiveness.

References

[1] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments", *International Journal of Network Security*, vol. 16, no. 4, pp. 318–321, 2014.

[2] N. Harini and T. R. Padmanabhan, "A secured-concurrent-available architecture for improving performance of web servers", in *Proceedings of 6th International Conference on Information Processing (ICIP 2012)*, pp 621-631, Bangalore, India, Aug. 10-12, 2012.

[3] N. Harini and T. R. Padmanabhan, "Admission control and request scheduling for secured-concurrent-available Architecture", *International Journal of Computer Applications*, vol. 63, no. 6, pp. 24–30, 2013.

[4] N. Harini and T. R. Padmanabhan, "2CAuth: A new two factor authentication scheme using QR-code", *International Journal of Engineering and Technology (IJET)*, vol. 5, no. 2, pp. 1087–1094, 2013.

[5] N. Harini, T. R. Padmanabhan and C. K. Shyamala, *Cryptography and Security*, Wiley India, First Edition, 2011.

[6] D. He, W. Zhao, and S. Wu, "Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards", *International Journal of Network Security*, vol. 15, no. 5, pp. 350–356, 2013.

[7] C. H. Huang, J. S. Chou, Y. Chen, "Improved multi-server authentication protocol", *International journal of Security and Communication Networks*, vol. 5, no. 3, pp. 331–341, 2012.

[8] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems", *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390–1397, 2011.

[9] Qi Jiang, J. Ma, G. Li, and Li Yang, "Robust two-factor authentication and key agreement preserving user privacy", *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.

[10] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[11] K. C. Liao and W. H. Lee, "A novel user authentication scheme based on QR-code", *Journal of Networks*, vol. 5, no. 8, pp. 937–941, 2010.

[12] J. J. Shen and P. W. Hsu, "A fragile associative watermarking on 2D barcode for data authentication", *International Journal of Network Security*, vol. 7, no. 3, pp. 301–309, 2008.

[13] J. J. Shen, C. W. Lin and M. S. Hwang, "Security enhancement for the timestamp-based password authentication", *Computers and Security*, vol. 22, no. 7, pp. 591–595, 2003.

[14] H. Tang, X. Liu, L. Jiang, "A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance", *International Journal of Network Security*, vol. 15, no. 6, pp. 446–454, 2013.

[15] A. Totok, V. Karamcheti, "RDRP: Reward-driven request prioritization for e-Commerce Web sites", *Electronic Commerce Research and Applications*, vol. 9, pp. 549–561, 2010.

[16] Li Yang, J. F. Ma, and Qi Jiang, "Mutual authentication scheme with smart cards and password under trusted computing", *International Journal of Network Security*, vol. 14, no. 3, pp. 156–163, 2012.

[17] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A simple password authentication scheme based on geometric hashing function", *International Journal of Network Security*, vol. 16, no. 4, pp. 271–277, 2014.

N. Harini is an Assistant Professor in the department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham. She has 3 years of industrial and 15 years of teaching and research experience. She is currently pursuing her Ph D in Security. Her research interests include cryptography, security. She has currently co-authored a book on Cryptography and Security.

T. R. Padmanabhan with MTech and PhD at the IIT Kharagpur, was in the faculty there from 1964 to 1979. With 20 years of development experience in the industry and an equal period in academic institutions, he is currently a Professor Emeritus at the Amrita School of Engineering. His research interests are security, digital communication, and VLSI design. He has (co)authored five books.