# A Secured and Improved Dynamic ID based Remote User Authentication Scheme using Smart Card and Hash Function for Distributed Systems

S.Ramesh
Assistant Professor, Department of Computer Science and Engineering
Paavai College of Engineering
Namakkal, India
raameshs@gmail.com

Dr. V.Murali Bhaskaran
Professor, Department of Computer Science and Engineering
Dhirajlal Gandhi College of Technology
Salem, India
murali66@gmail.com

***Abstract*—Authentication is a major concern for accessing remote service residing over on server in an distributed systems. It is difficult to remember different identities and passwords for users. In order to solve the flaws encountered in many remote user authentication schemes in multi-server environment, only authentic user login to the remote server has been used. These remote schemes resist various attacks and have some weakness. Leu and Hsieh proposed an efficient and secure dynamic ID based remote user authentication for distributed environment using smart cards but is vulnerable to impersonation attack, leak verifier attack, stolen smart card attack. We propose a strong authentication scheme with user anonymity and secured dynamic ID based remote user authentication using smart cards that remove aforementioned weakness in distributed systems. The function and performance efficiency of our scheme was analysed and proved to provide a strong mutual authentication between user and server when compared with the existing methods.**

***Keywords-Smart Card; hash function; authentication; security; Dynamic ID***

## I. INTRODUCTION

Security breaches are the major issue in the communication environment over the Internet. Authentication is mechanism that allow only the legitimate network users want to access the remote servers provide resources over open public network through insecure channel. The remote user utilizes both identity and password for authentication to access the services stored on the remote server. In traditional authentication schemes, the server maintains the password table or verifier table to save the identity and passwords of the registered users [7]. Two problems are possible in the authentication scheme are being the administrator viewing the password table and the other is that the intruder can impersonate as a legal user and can steal the user ID and password. At worst case the distributed network is vulnerable to various attacks such as forgery attack, server spoofing attack, replay attack, stolen smart card attacks. A secure and efficient remote user authentication scheme must satisfy the following six requirements[9,11]: (1) Single registration (2) Low computational and communication cost (3) No password table (4) Withstand against security attacks (5) Freely chosen password and (6) Proper mutual authentication. In this paper we analyze the security weakness of the recent dynamic ID based multi-server remote user authentication scheme proposed by Lue and Hsieh[10] and we propose a more secure smartcard and dynamic ID based remote user authentication for multi-server environment to tackle the problems. The rest of the paper is organized as follows .Section II shows the related work of the dynamic identity based remote user authentication scheme. In section III we review the Leu Shieh' dynamic ID based remote user authentication scheme[10] using smart card. Section IV describes a cryptanalysis of Leu-Shieh scheme. The proposed remote user authentication scheme and the corresponding security, functionality and performance analysis are discussed in sections VI, VII and VII respectively. Finally we conclude the article in section VIII.

## II. RELATED WORK

In 1981, Lamport [2] proposed the first password based remote user authentication which maintains a password list that cannot resist interpolation attack . In 2000, Lee and Chang [1] presented a user identification scheme that achieve key exchange requirement while preserving user anonymity. The first dynamic ID based remote user authentication using smart card was proposed by Das et al [19] in 2004 that remove the weakness in password based authentication scheme. At the same time Juang [1] proposed two efficient two factor

authenticated key exchange protocol in public insecure network. In 2008, Tsai [5] proposed an efficient multi-server authentication scheme without verification table that use the nonce and hash function. It is suitable for distributed networks use less computational cost. Previous schemes are based on static ID which might be intercepted by an adversary from the public network and be used to trace the legal user. In 2009, Liao and Wang [16] first proposed a dynamic ID based remote user authentication scheme for multi- server environment. However, Hsiang and Shih [15] found that Liao et al.'s scheme [16] vulnerable to insider attack, masquerade attack, server spoofing attack, registration server spoofing attack and is not repairable .Moreover, Liao et al.'s scheme cannot provide mutual authentication. In 2011, Lee et al. [11] pointed out that Hsiang et al. scheme is still vulnerable to a masquerade attack, server spoofing attack and is not repairable, cannot provide mutual authentication. Sood et al. scheme [18] is vulnerable to leak of verifier attack, stolen smart card attack and had a fatal mistake. X.Li et al. [8, 9] proposed scheme is suitable for distributed multi-server architecture since it provide user anonymity, mutual authentication, efficient and security in 2012&2013. Hence through the literature we understand the prevalence of security breaches in distributed systems. Therefore we propose a more secured and improved dynamic identity based remote user authentication scheme that removes the security flaws and increase its efficiency.

## III. REVIEW OF LEU–HISEH AUTHENTICATION SCHEME

In this section we review Leu-Hsieh dynamic identity based remote authentication scheme [10] using smart card for multiserver environment which has four phases namely registration phase, login phase, verification phase and password change phase. In this scheme three entities are involved: the user ($U_i$), the server ($S_j$) and the registration center ($RC$). The $RC$ selects the master secret key $x$ and a secret number $y$ to compute $h(x \| y)$ and $h(y)$.and then share them with $S_j$ through a secure channel. Figure 1 shows the entire protocol structure of Hsieh-Leu scheme. The notations used throughout this paper are summarized in TABLE I.

TABLE I

Notations used in the schemes

| Symbol | Description |
|---|---|
| $U_i$ | Client / User |
| $S_j$ | Server |
| $ID_i$ | User i's Identity |
| $PW_i$ | $U_i$'s Password |
| h(. ) | One way hash function |
| $SID_j$ | Server Identity |
| $CID_i$ | Dynamic User Identity |
| X | Master secret key |
| Y | Secret number |
| B | User's random number |
| $R_s$ | Server $S_i$'s random number |
| $\|\|$ | Concatenation operator |
| $\oplus$ | XOR operator |
| $\longrightarrow$ | Communication channel |
| $. \Rightarrow$ | Secure Channel |

*A. Registration Phase*

The user $U_i$ wants to login to the remote server $S_j$ the user initially register with the registration server $RC$ and perform the following activities.

Step 1. $U_i \Rightarrow RC: ID_i, h(b \oplus PW_i)$. User $U_i$ select his/her identity $ID_i$ and password $PW_i$ and choose a random number $b$. The user $U_i$ computes the masked password $h(b \oplus PW_i)$. Then user $U_i$ sends $ID_i$ and $h(b \oplus PW_i)$ to the registration center $RC$ through a secure communication channel.

Step 2. $RC$ computes

$$A_i = h(R_c \| x)$$

$$B_i = R_c \oplus ID_i \oplus h(b \oplus PW_i)$$

$$C_i = A_i \oplus h(ID_i \| h(b \oplus PW_i))$$

$$D_i = h(b \oplus PW_i) \oplus ID_i \oplus h(h(b \oplus PW_i \oplus R_c) \| h(x \| y))$$

$$E_i = h(A_i)$$

Step 3. $RC \Rightarrow U_i : SC$. The registration center $RC$ stores the values $h(.)$ and $B_i, C_i, D_i, E_i, h(y)$ on the smart card $SC$ and issues it to the user $U_i$ via a secure channel.

Step 4. After receive the smart card, the user $U_i$ enter $b$ into his/her smart card. Finally the smart card contains $b, B_i, C_i, D_i, E_i, h(y)$ and $h(.)$. At the end of this phase, user $U_i$ need not remember $b$.

*B. Login Phase*

When the user $U_i$ wants to login to the remote server $S_j$ after receive the smart card $SC$ from the registration center $RC$ the following steps to be performed.

Step 1. User $U_i$ inserts his/her smart card into the smart card reader and enters his/her identity $ID_i$ , password $PW_i$ and server identity $SID_j$.

Step 2. The smart card computes

$$R_c = B_i \oplus ID_i \oplus h(b \oplus PW_i)$$

$$A_i = C_i \oplus h(ID_i \| h(b \oplus PW_i))$$

$$E_i^{'} = h(A_i)$$

And check whether the computed $E_i^{'}$ is equal to $E_i$ .If they are equal, user $U_i$ is a legal user and proceeds with next steps. Otherwise the smart card aborts the session.

Step 3.The smart card generates a nonce $N_i$ and computes

$$T_i = h(b \oplus PW_i) \oplus ID_i \oplus D_i$$

$$= h(h(b \oplus PW_i \oplus R_c) \| h(x \| y))$$

$$H_i = h(A_i \| h(y) \| N_i)$$

$$CID_i = h(b \oplus PW_i \oplus R_c) \oplus h(A_i \| H_i \| N_i)$$

$$P_{ij} = A_i \oplus h(h(y) \| N_i \| SID_j)$$

$$Q_i = h(T_i \| H_i \| N_i)$$

Step 4. $U_i \rightarrow S_j : CID_i, P_{ij}, Q_i, N_i$ : The user $U_i$ sends the login request message $CID_i, P_{ij}, Q_i, N_i$ to the server $S_j$.

*C. Authentication Phase*

After receiving the login request message from the user $U_i$ , the server $S_j$ execute the following steps for mutual authentication and agree a shared session key for secure communication.

Step 1. Server $S_j$ computes

$$A_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$$

$$H_i = h(A_i \| h(y) \| N_i)$$

$$h(b \oplus PW_i \oplus R_c) = CID_i \oplus h(A_i \| H_i \| N_i)$$

$$T_i = h(h(b \oplus PW_i \oplus R_c) \| h(x \| y))$$

Step 2. $S_j \rightarrow U_i : M_{ij}, N_j$ : Next server $S_j$ computes $h(T_i \| H_i \| N_i)$ and compare with $Q_i$. If they are not equal, $S_j$ rejects the login request message and terminate this session. Otherwise, server $S_j$ accepts the login request message. Then $S_j$ generate a nonce $N_j$ to computes $M_{ij} = h(T_i \| N_i \| H_i \| SID_j)$. Finally the server $S_j$ sends the message $M_{ij}, N_j$ to the user $U_i$.

Step 3. $U_i \rightarrow S_j : M_{ij}^{"}$: User $U_i$ computes $M_{ij}^{'} = h(T_i \| N_i \| H_i \| SID_j)$ and compare with the received message $M_{ij}$. If they are not equal, user $U_i$ rejects the incoming message and rejects this session. Otherwise, user $U_i$ authenticates $S_j$ successfully and computes the mutual authentication message $M_{ij}^{"} = h(T_i \| N_j \| H_i \| SID_j)$. Next the user $U_i$ send back the message $M_{ij}^{"}$ to the server $S_j$.

Step 4. Upon receiving the message $M_{ij}^{"}$, $S_j$ computes $h(T_i \| N_j \| H_i \| SID_j)$ and checks it with the received message $M_{ij}^{"}$. If they are equal, $S_j$ authenticates $U_i$ successfully. At the end of the authentication phase, both $U_i$ and $S_j$ agree to compute a common session key $SK = h(T_i \| N_i \| N_j \| H_i \| SID_j)$ for secure communications.

*D. Password Change Phase*

In this phase, user $U_i$ can change his/her password any time if he/she wishes. The steps of the password change phase are as follows.

Step 1. $U_i \Rightarrow RC : ID_i, h(b \oplus PW_i \oplus R_c)$ : The user $U_i$ inserts his/her smart card $SC$ in to the smart card reader and then input his/her identity $ID_i$ and password $PW_i$ .The smart card $SC$ computes to obtain $A_i^* = C_i \oplus h(ID_i \| h(b \oplus PW_i))$. Next it computes $E_i^* = h(A_i^*)$ and compares it with the stored value $E_i$ in the smart card. If they are same the smart card computes $R_c = B_i \oplus ID_i \oplus h(b \oplus PW_i)$. Then user $U_i$ choose a new password $PW_i^{new}$ and a new random number $b_{new}$ to computes $B_i^{new} = R_c \oplus ID_i \oplus h(b_{new} \oplus PW_i^{new})$ , $C_i^{new} = A_i \oplus h(ID_i \| h(b_{new} \oplus PW_i^{new})$ . Finally user $U_i$ sends $ID_i, h(b \oplus PW_i \oplus R_c)$ to the registration center $RC$ in a secure channel.

Step 2. $RC \Rightarrow U_i$ : $B_i^{new}$ : The registration center $RC$ computes

$$D_i^{new} = h(h(b_{new} \oplus PW_{new} \oplus R_c) \| h(x \| y)$$

$RC$ sends $B_i^{new}$ to the user $U_i$.

Step 3. Finally, the smart card replaces $B_i, C_i, D_i$ with $B_i^{new}, C_i^{new}, D_i^{new}$.

| User($U_i$) | [Registration Phase] | Registration Center($RC$) |
|---|---|---|
| Select $ID_i, PW_i, b$ | $ID_i,\ h(b \oplus PW_i)$ → | Compute $A_i = h(R_c \| x)$ |
| | | $B_i = R_c \oplus ID_i \oplus h(b \oplus PW_i)$ |
| | | $C_i = A_i \oplus h(ID_i \| h(b \oplus PW_i))$ |
| | | $D_i = h(b \oplus PW_i) \oplus ID_i \oplus h(h(b \oplus PW_i \oplus R_c) \| h(x \| y))$ |
| | | $E_i = h(A_i)$ |
| | ← $SC[b, B_i, C_i, D_i, E_i, h(y), h(.)]$ | |
| Enter $b$ into the Smart Card | | |

| User($U_i$) | [Login Phase] | Server($S_j$) |
|---|---|---|
| Insert smart card $SC$ | Smart Card($SC$) | |
| Input $ID_i, PW_i$ | $R_c = B_i \oplus ID_i \oplus h(b \oplus PW_i)$ | |
| | $A_i = C_i \oplus h(ID_i \| h(b \oplus PW_i))$ | |
| | $E_i^{'} = h(A_i)$ | |
| | Check if $E_i^{'} \stackrel{?}{=} E_i$ | |
| | Generate a random number $N_i$ | |
| | Compute $T_i = h(b \oplus PW_i) \oplus ID_i \oplus D_i$ | |
| | $= h(h(b \oplus PW_i \oplus R_c) \| h(x \| y))$ | |
| | $H_i = h(A_i \| h(y) \| N_i)$ | |
| | $CID_i = h(b \oplus PW_i \oplus R_c) \oplus h(A_i \| H_i \| N_i)$ | |
| | $P_{ij} = A_i \oplus h(h(y) \| N_i \| SID_j)$ | |
| | $Q_i = h(T_i \| H_i \| N_i)$ | $CID_i, P_{ij}, Q_i, N_i$ → |

User($U_i$) [Authentication Phase] Server($S_j$)

Compute $A_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$

$H_i = h(A_i \| h(y) \| N_i)$

$h(b \oplus PW_i \oplus R_c) = CID_i \oplus h(A_i \| H_i \| N_i)$

$T_i = h(h(b \oplus PW_i \oplus R_c) \| h(x \| y))$

Check if $Q_i \stackrel{?}{=} h(T_i \| H_i \| N_i)$

Generate a random number $N_j$

Compute $M_{ij} = h(T_i \| N_i \| H_i \| SID_j)$

Else reject login request

$M_{ij}, N_j$ ←

Compute $M_{ij}^{'} = h(T_i \| N_i \| H_i \| SID_j)$

Verify if $M_{ij} \stackrel{?}{=} M_{ij}^{'}$

$M_{ij}^{''} = h(T_i \| N_j \| H_i \| SID_j)$ $M_{ij}^{''}$ → $M_{ij}^{'''} = h(T_i \| N_j \| H_i \| SID_j)$

Check if $M_{ij}^{'''} \stackrel{?}{=} M_{ij}^{''}$ authentication success

Else authentication failure Else authentication failure

$SK = h(T_i \| N_i \| N_j \| H_i \| SID_i)$

User($U_i$) [Password Change Phase] Registration Center($RC$)

Insert smart card $SC$ Smart Card($SC$)

Input $ID_i, PW_i, PW_i^{new}$ Comupte $A_i^* = C_i \oplus h(ID_i \| h(b \oplus PW_i))$

$E_i^* = h(A_i^*)$

Verify if $E_i^{'} \stackrel{?}{=} E_i$

$R_c = B_i \oplus ID_i \oplus h(b \oplus PW_i)$

Choose a new random number $b_{new}$

$B_i^{new} = R_c \oplus ID_i \oplus h(b_{new} \oplus PW_i^{new})$

$C_i^{new} = A_i \oplus h(ID_i \| h(b_{new} \oplus PW_i^{new})$

$ID_i, h(b \oplus PW_i \oplus R_c)$

$D_i^{new} = h(h(b_{new} \oplus PW_{new} \oplus R_c) \| h(x \| y)$

Replace $B_i, C_i, D_i$ with $B_i^{new}, C_i^{new}, D_i^{new}$

Figure 1. Leu Hsieh Scheme

## IV. CRYPTANALYSIS OF LEU HSIEH SCHEME

In this section we will demonstrated that Leu Hsieh scheme is vulnerable to insiders attack, password guessing attack, stolen verifier attack, server spoofing attack and does not provide the two factor security. Leu Hsieh scheme is inefficient in error password login when the public key of the server is compromised, the adversary can obtain all the previous session keys between user and the server $S_j$ .

### *A. Masquerading user attack*

An attacker $A$ can intercept the login request message $CID_i, P_{ij}, Q_i, N_i$ sent from the user $U_i$ to the server $S_j$ .Then the attacker $A$ can compute $A_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$ .In order to masquerade as user login request message to communicate with the server $S_k$ .The attacker generates a random number $N_k$ then he/she computes $H_i^* = h(A_i \| h(y) \| N_k)$ ,

$CID_i = h(b \oplus PW_i \oplus R_c) \oplus h(A_i \| H_i^* \| N_k)$ , $P_{ik} = A_i \oplus h(h(y) \| N_k \| SID_k)$ ,

$Q_i^* = h(T_i \| H_i^* \| N_k)$ .Then the attacker send the forgery message $CID_i^*, P_{ik}^*, Q_i^*, N_k$ to the server and computes

$A_i = P_{ik}^* \oplus h(h(y) \| N_k \| SID_k)$ , $H_i^* = h(A_i \| h(y) \| N_k)$ ,

$h(b \oplus PW_i \oplus R_c)^* = CID_i^* \oplus h(A_i \| H_i^* \| N_k)$ and

$T_i^* = h(h(b \oplus PW_i \oplus R_c)^* \| h(x \| y))$ $h(h(b_k \oplus PW_i \oplus R_c)^* \| h(x \| y)) = T_k$ .So

$h(T_k \| H_i^* \| N_k) = Q_i^*$ and server accept the login request.

### *B. Server Spoofing attack*

Assume that legal server $S_j$ might try to masquerade as another malicious server $S_k$ to fool any legal user and Leu-Hsieh scheme cannot withstand the server spoofing attack. The illegal server act as like the original server hold the secret information $h(x \| y)$ and $h(y)$ .When the user $U_i$ submits his/her login request $CID_i, P_{ij}, Q_i, N_i$ to the legal server $S_j$ ,but malicious server $S_k$ can interpret the message and compute $A_i, H_i, h(b \oplus PW_i \oplus R_c), T_i$ by using $h(x \| y)$ , $h(y)$ and $SID_j$ . To check $Q_i \stackrel{?}{=} h(T_i \| H_i \| N_i)$ .Then he/she generate a nonce $N_k$ and compute $M_{ij} = h(T_i \| N_i \| H_i \| SID_j)$ and submit $M_{ij}, N_k$ to $U_i$ . $U_i$ computes $h(T_i \| N_i \| H_i \| SID_j)$ and compares it with $M_{ij}^{'}$ .If both the values are equal, $U_i$ responds with the message $M_{ij}^{''}$ and can compute the session key $SK = h(T_i \| N_i \| N_j \| H_i \| SID_j)$ .Therefore, a legal and malicious server can masquerade as another server to fool any legal user and Leu-Shieh scheme is vulnerable to server spoofing attack..

### *C. Password Guessing attaack*

An attacker $A$ steals or user $U_i$ lost the smart card $SC$ the significant information in the card is derived by the attacker, there is a chance of password guessing attack. The attacker $A$ can read the data $b, B_i, C_i, D_i, E_i, h(y), h()$ from the smart card by select any word guessing from the dictionary $PW_i^{'}$ . $A$ compute $A_i = C_i \oplus h(ID_i \| h(b \oplus PW_i^{'}))$ and $E_i^{'} = h(A_i)$ . $A$ check if $E_i^{'}$ equal $E_i$ . If $E_i^{'}$ equals $E_i$ then $A$ find the correct password. Otherwise, $A$ repeat it until the correct password if found.

### *D. Improper mutual authentication*

In the verification phase attacker $A$ intercepts the authentication message $M_{ij}, N_j$ from server $S_j$ to the user $U_i$ fabricate this message as $M_{ij}^*, N_j^*$ . Leu-Shieh scheme [10] does not verify the validity of $N_j$ which

provides attackers with an opportunity to tamper with the message. Therefore $U_i$ cannot distinguish the valid authentication message $M_{ij}, N_j$ from the fabricated authentication message $M_{ij}^*, N_j^*$ which leads to $S_j$ thinking $U_i$ is a cheater, whereas $U_i$ is a legal user. So that Leu-Shieh scheme [10] fails to provide proper mutual authentication under the condition that the authenticated message was partly interpolated by an attacker.

## V. PROPOSED SCHEME

In this section, we proposed an improved efficient and secured scheme to overcome the weakness in the Leu Shieh scheme [10]. Also three entities is involved: the user ($U_i$), the service providing server ($S_j$) and the registration center ($RC$). The $RC$ selects the master secret key $x$ and a secret number $y$ to compute $h(x \| y)$ , $h(SID_j \| y)$ and $h(y)$ and then shares them with $S_j$ through a secure channel. Figure 2 shows the entire protocol structure of our proposed scheme. The proposed scheme which has six phases namely setup phase, registration phase, login phase, verification phase and password change phase.

### *A. Setup Phase*

Setup Phase consist of three steps.

Step 1. Server setup: This process is performed by the server $S_j$ consulted with the registration center $RC$, to share the values $h(x \| y)$ , and $h(y)$ through a secure channel.

Step 2. Client setup: This process is performed by the user $U_i$ initialize the secret random number $b$ for masking the password.

Step 3. Registration Center setup: This process is performed by the registration center $RC$ to choose a master secret key $x$ and secret number $y$ to compute $h(x \| y)$ and $h(y)$ .These values are only known to $RC$.

### *B. Registration Phase*

The user $U_i$ wants to login to the remote server $S_j$ the user initially register with the registration server $RC$ and perform the following activities.

Step 1. $U_i \Rightarrow RC: ID_i,\ h(b \oplus PW_i)$. User $U_i$ select his/her identity $ID_i$ and password $PW_i$ and choose a random number $b$. The user $U_i$ computes the masked password $h(b \oplus PW_i)$. Then user $U_i$ sends $ID_i$ and $h(b \oplus PW_i)$ to the registration center $RC$ through a secure communication channel.

Step 2. $RC$ computes

$$T_i = h(ID_i \| x)$$

$$V_i = T_i \oplus h(ID_i \| h(b \oplus PW_i) \| h(y))$$

$$B_i = h(h(b \oplus PW_i) \| h(x \| y))$$

$$H_i = h(T_i)$$

Step 3. $RC \Rightarrow U_i: SC$. The registration center $RC$ stores the values $h(.)$ and $V_i, B_i, H_i, h(y)$ on the smart card $SC$ and issues it to the user $U_i$ via a secure channel.

Step 4. After receive the smart card, the user $U_i$ enter $b$ into his/her smart card. Finally the smart card contains $b, V_i, B_i, H_i, h(y)$ and $h(.)$. At the end of this phase, user $U_i$ need not remember $b$.

*C. Login Phase*

When the user $U_i$ wants to login to the remote server $S_j$ after receive the smart card $SC$ from the registration center $RC$ the following steps to be performed.

Step 1. User $U_i$ inserts his/her smart card into the smart card reader and enters his/her identity $ID_i$ , password $PW_i$ and server identity $SID_j$ .

Step 2. The smart card computes

$$T_i = V_i \oplus h(ID_i \,||\, h(b \oplus PW_i) \,||\, h(\mathrm{y}))$$

$$H_i^* = h(T_i)$$

And check whether the computed $H_i^{'}$ is equal to $H_i$ .If they are equal, user $U_i$ is a legal user and proceeds with next steps. Otherwise the smart card aborts the session.

Step 3.The smart card generates a nonce $N_i$ and computes

$$CID_i = h(b \oplus PW_i) \oplus h(\mathrm{T}_i \,||\, h(y) \,||\, N_i)$$

$$P_{ij} = T_i \oplus h(h(y) \,||\, N_i \,||\, SID_j)$$

$$M_1 = h(P_{ij} \,||\, CID_i \,||\, h(y) \,||\, N_i)$$

$$M_2 = h(SID_j \,||\, h(y)) \oplus N_i$$

Step 4. $U_i \rightarrow S_j \; CID_i, P_{ij}, M_1, M_2$ : The user $U_i$ sends the login request message $CID_i, P_{ij}, M_1, M_2$ to the server $S_j$ .

*D. Authentication Phase*

After receiving the login request message from the user $U_i$ , the server $S_j$ execute the following steps for mutual authentication and agree a shared session key for secure communication.

Step 1. Server $S_j$ computes

$$N_i = M_2 \oplus h(SID_j \,||\, h(y))$$

$$T_i = P_{ij} \oplus h(h(y) \,||\, N_i \,||\, SID_j))$$

$$h(b \oplus PW_i) = CID_i \oplus h(T_i \,||\, h(y) \,||\, N_i)$$

$$B_i = h(h(b \oplus PW_i) \,||\, h(x \,||\, y))$$

Step 2. $S_j \rightarrow U_i : M_3, M_4$ : Next the server computes $h(P_{ij} \,||\, CID_i \,||\, h(y) \,||\, N_i)$ and compare with $M_1$ . If they are not equal, $S_j$ rejects the login request message and terminate this session. Otherwise, server $S_j$ accepts the login request message. Then $S_j$ generate a nonce $N_j$ to computes $M_3 = h(B_i \,||\, N_j \,||\, SID_j)$ . Finally the server $S_j$ sends the message $M_3, M_4$ to the user $U_i$ .

Step 3. $U_i \rightarrow S_j : M_5$ : User $U_i$ computes $N_j = M_4 \oplus h(B_i \,||\, SID_j) \oplus N_i$ to obtain the server nonce $N_j$ .Next compute $h(B_i \,||\, N_j \,||\, SID_j)$ and compare with the received message $M_3$ . If they are not equal , user $U_i$ rejects the incoming message and rejects this session. Otherwise, user $U_i$ authenticates $S_j$

successfully and computes the mutual authentication message $M_5 = h(B_i \| N_i \| SID_j)$. Next the user $U_i$ send back the message $M_5$ to the server $S_j$.

Step 4. Upon receiving the message $M_5$, $S_j$ computes $h(B_i \| N_i \| SID_j)$ and checks it with the received message $M_5$. If they are equal, $S_j$ authenticates $U_i$ successfully. Otherwise, rejects the authentication request.

*E. Session Key generation Phase*

At the end of the authentication phase, the user $U_i$ and the server $S_j$ can agree a common session key for secure communication with authentication.

Step 1.Server $S_j$ generate the session key $SK = h(CID_i \| N_i \| N_j \| SID_j \| B_i)$

Step 2.Client $U_i$ generate the session key $SK = h(CID_i \| N_i \| N_j \| SID_j \| B_i)$

Step 3. Finally both of the user $U_i$ and the server $S_i$ can utilize the session key $SK = h(CID_i \| N_i \| N_j \| SID_j \| B_i)$ to securely communicate with each other.

*F. Password Change Phase*

In this phase, user $U_i$ can change his/her password any time if he/she wishes. The steps of the password change phase are as follows.

Step 1. $U_i \Rightarrow RC : ID_i, h(b_{new} \oplus PW_i^{new})$: The user $U_i$ inserts his/her smart card $SC$ in to the smart card reader and then input his/her identity $ID_i$ and password $PW_i$ .The smart card $SC$ computes to obtain $T_i = V_i \oplus h(ID_i \| h(b \oplus PW_i) \| h(y))$. Next it computes $H_i^* = h(T_i)$ and compares it with the stored value $H_i$ in the smart card. If they are same the user $U_i$ choose a new password $PW_i^{new}$ and a new random number $b_{new}$ to computes $h(b_{new} \oplus PW_i^{new})$ , $V_i^{new} = T_i \oplus h(ID_i \| h(b_{new} \oplus PW_i^{new}) \| h(y))$ . Finally user $U_i$ sends $ID_i, h(b_{new} \oplus PW_i^{new})$ to the registration center $RC$ in a secure channel.

Step 2. $RC \Rightarrow U_i$: $B_i^{new}$: The registration center $RC$ computes

$$B_i^{new} = h(h(b_{new} \oplus PW_i^{new}) \| h(x \| y))$$

$RC$ send back $B_i^{new}$ to the user $U_i$.

Step 3. Finally, the smart card replaces $B_i, V_i$ with $B_i^{new}, V_i^{new}$.

| User($U_i$) | [Registration Phase] | Registration Center($RC$) |
|---|---|---|
| Select $ID_i, PW_i, b$ | $ID_i$, $h(b \oplus PW_i)$ | Compute $T_i = h(ID_i \| x)$ |
| | | $V_i = T_i \oplus h(ID_i \| h(b \oplus PW_i) \| h(y))$ |
| | | $B_i = h(h(b \oplus PW_i) \| h(x \| y))$ |
| | | $H_i = h(T_i)$ |
| | $SC[V_i, B_i, h(y), h(.)]$ | |
| | Enter $b$ into the Smart Card | |

| User($U_i$) | [Authentication Phase] | Server($S_j$) |
|---|---|---|
| | | Compute $N_i = M_2 \oplus h(SID_j \| h(y))$ |
| | | $T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j))$ |
| | | $h(b \oplus PW_i) = CID_i \oplus h(T_i \| h(y) \| N_i)$ |
| | | $B_i = h(h(b \oplus PW_i) \| h(x \| y))$ |
| | | Check if $M_1 \stackrel{?}{=} h(P_{ij} \| CID_i \| h(y) \| N_i)$ |
| | | Generate a random number $N_j$ |
| | | Compute $M_3 = h(B_i \| N_j \| SID_j)$ |
| | | $M_4 = h(B_i \| SID_j) \oplus N_i \oplus N_j$ |
| | | Else reject login request |
| | $\xleftarrow{M_3, M_4}$ | |
| Compute $N_j = M_4 \oplus h(B_i \| SID_j) \oplus N_i$ | | |
| Verify if $M_3 \stackrel{?}{=} h(B_i \| N_j \| SID_j)$ | | |
| Compute $M_5 = h(B_i \| N_i \| SID_j)$ | $\xrightarrow{M_5}$ | Check if $M_5 \stackrel{?}{=} h(B_i \| N_i \| SID_j)$ |
| Else authentication failure | | authentication successful |
| | | Else authentication failure |

| User($U_i$) | [Session Key generation Phase] | Server($S_j$) |
|---|---|---|
| $SK = h(CID_i \| N_i \| N_i \| SID_i \| B_i)$ | | $SK = h(CID_i \| N_i \| N_i \| SID_i \| B_i)$ |

| User ($U_i$) | [Password Change Phase] | Registration Center ($RC$) |
|---|---|---|
| Insert smart card $SC$ | Smart Card ($SC$) | |
| Input $ID_i, PW_i, PW_i^{new}$ | Compute $T_i = V_i \oplus h(ID_i \| h(b \oplus PW_i) \| h(y))$ | |
| | $H_i^* = h(T_i)$ | |
| | Verify if $H_i^* \stackrel{?}{=} H_i$ | |
| | Choose a new random number $b_{new}$ | |
| | Compute $h(b_{new} \oplus PW_i^{new})$ | |
| | $V_i^{new} = T_i \oplus h(ID_i \| h(b_{new} \oplus PW_i^{new}) \| h(y))$ | |
| | | $ID_i, h(b_{new} \oplus PW_i^{new})$ |
| | | $B_i^{new} = h(h(b_{new} \oplus PW_i^{new}) \| h(x \| y))$ |
| | Replace $B_i, V_i$ with $B_i^{new}, V_i^{new}$ | |

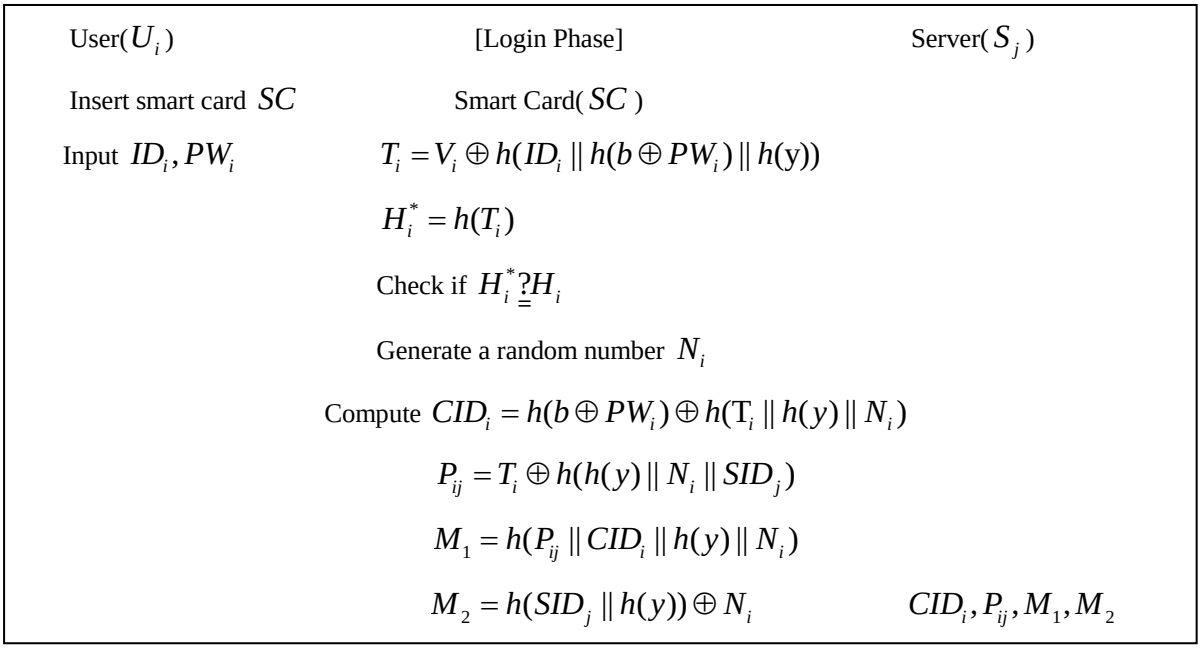


FIGURE 2. PROPOSED SCHEME

## VI. SECURITY ANALYSIS

In this section we analyze the security of the proposed scheme and discuss the security features involved in it. The proposed scheme provides several security characteristics and resist against various known attacks. TABLE III describe the security characteristics involved in our scheme and other related schemes.

### *A. Resist replay attack*

An attacker $A$ eavesdrops the login message between the user $U_i$ and the server $S_j$ and try to imitate $U_i$ to login to the server by replaying the intercepted messages. In our proposed scheme, two random numbers $N_i, N_j$ are generated by the user and the server respectively for verification that make all messages dynamic and valid for the session only. After eavesdropping the previous login request $CID_i, P_{ij}, M_1, M_2$ from the user, the intruder may replay the message to $S_j$. $A$ will receive the acknowledge message $M_3, M_4$ from $S_j$ and cannot compute the mutual message $M_5$ to respond to $S_j$ without knowing $B_i, N_i$. $A$ replies a previous message $M_3, M_4$ to $U_i$ in this session, because each session have its own $N_i$, the computed random number $N_j$ will not equal to the random number $N_j$ of this session that was chosen by $S_j$ $h(B_i \| N_j \| SID_j)$ will not equal to $M_3$ and the authentication will fail. Therefore there is no chance of replay attack.

### *B. Resist forgery attack/Masquerade attack*

An attacker $A$ act as like the legal user to login the remote server, he must be able to forge a valid login request $CID_i, P_{ij}, M_1, M_2$ to fool $S_j$. The adversary cannot compute a valid login request message without knowing $T_i, N_i$. In addition, if the adversary is a legal user of the system, he/she also cannot masquerade as another legal user to login to the remote server, since he/she cannot compute $T_i$ from his/her smart card and intercepted login request $CID_i, P_{ij}, M_1, M_2$ without knowing $x, h(x \| y), b, PW_i$ .Suppose an adversary steals user smart card and extract the parameters $b, V_i, B_i, H_i, h(y), h(.)$ in some way , he/she cannot forge the login request. Because it is difficult to find the $T_i$ without knowing the password $PW_i$. Our proposed scheme is withstand forgery attack.

### *C. Resist server spoofing attack*

If the attacker is a legal user of the system, he/she must be able to forge a valid response message $M_3, M_4$ to the user. However, the attacker cannot compute $T_i$ and $h(b \oplus PW_i)$ from his smart card and

intercepted login request $CID_i, P_{ij}, M_1, M_2$ without the knowledge of $h(x \| y)$, therefore the attacker cannot compute the valid response message $M_3, M_4$. If the attacker is a legal server of the system, he/she cannot masquerade as another server to fool any legal user since he does not have the other secret information $h(SID_j \| h(y))$ to check the login request and cannot compute the valid response message $M_3, M_4$. Our proposed scheme is withstand server spoofing attack.

*D. Resist stolen smart card attack*

The attacker steals or user lost the smart card can extract the significant information $b, V_i, B_i, H_i, h(y), h(.)$ stored in the smart card. Even after collecting this information in order to change the password or login into the system by using the lost smart card, the attacker submit the real identity and password correctly at the same time, but it is not possible to guess these parameters correctly at the same time in real polynomial time since they are protected by a one way hash function and attackers does not have the knowledge of the master secret key $x$ .Therefore, the proposed scheme is secure against stolen smart card attacks.

*E. Resist leak of verifier attack*

The proposed scheme, the server or the registration center does not store any verifier information, so even any malicious legitimate user cannot retrieve any useful information from them, and cannot impersonate a legal user to login to the server. Thus, the proposed scheme can resist the leak of verifier attack.

TABLE III

Security Comparison

| Security Factors | Lee et. al [2011] | X.Li et. al [2012] | X.Li et.al [2013] | Leu-Hsieh [2014] | Proposed Scheme |
|---|---|---|---|---|---|
| Replay attack | No | No | No | Yes | Yes |
| Forgery /Masquerade user attack | Yes | No | Yes | Yes | Yes |
| Server spoofing attack | Yes | Yes | No | Yes | Yes |
| Stolen smart card attack | No | No | No | Yes | Yes |
| Leak of verifier attack | No | No | No | Yes | Yes |

## VII. PERFORMANCE AND FUNCTIONAL ANALYSIS

In this section we compare our proposed scheme with other related schemes, our scheme achieve more functionality features that are required to implement the real time identity and password authentication using smart cards is described in TABLE IV.

*A. Proper mutual authentication*

The proposed scheme can provide proper mutual authentication, the user sends $CID_i, P_{ij}, M_1, M_2$ to $S_j$ to access the service in it. After receiving the message $S_j$ computes $T_i, B_i, h(b \oplus PW_i)$ and then checks $M_1 \stackrel{?}{=} h(P_{ij} \| CID_i \| h(y) \| N_i)$ .If it holds $U_i$ is a valid user and login request was accepted by the server. Otherwise $S_j$ rejects the login request. The authentication equation is fully depending on the one way hash function, any fabricated message $CID_i^{'}, P_{ij}^{'}, M_1^{'}, M_2^{'}$ cannot pass verification. Then $S_j$ compute $M_3, M_4$ and send to the user. Next user compute $N_j = M_4 \oplus h(B_i \| SID_j) \oplus N_i$ and verify $M_3 \stackrel{?}{=} h(B_i \| N_j \| SID_j)$ .If they are not equal user terminate the session. Otherwise server is authenticated by user. The fabricated message $M_3^{'}, M_4^{'}$ cannot pass the authentication. With the same reason any fabricated mutual authentication message $M_5^{'}$ cannot pass the mutual authentication. Therefore, the proposed scheme can provide proper mutual authentication.

*B. User anonymity*

In the registration phase, the user's identity is well protected by a secure communication channel among the user and the registration center. Our proposed scheme, the login phase generate the dynamic identity $CID_i$ is

used for the real identity $ID_i$ for its authentication to the service of the server. When the user wants to login to the server the dynamic $CID_i$ is different for each session. Besides, instead of the real identity, the attacker cannot distinguish between different sessions corresponding to a certain user and cannot obtain any idea about the real identity. Our scheme can provide user anonymity.

*C. Session key agreement*

The user and server can agree on a shared common session key for further communication. An attacker guess the the random secrets $N_i, N_j$ it is difficult to derive the session key without knowing the value of $B_i$ .Even if an adversary know the values of $b, PW_i, y$ , it is impossible to find the session key.

*D. Forward secrecy*

The master key of the system is compromised; the secrecy of the previously established session keys should not be affected. If the master secret key $x$ is compromised for some reason, the attacker cannot compute any previous session key without knowing $b, PW_i, y$ .Our proposed scheme can ensure forward secrecy.

TABLE IV

Functional Analysis

| Functional Factors | Lee et. al [2011] | X.Li et. al [2012] | X.Li et.al [2013] | Leu-Hsieh [2014] | Proposed Scheme |
|---|---|---|---|---|---|
| Strong mutual authentication | No | No | No | No | Yes |
| User anonymity | Yes | No | Yes | Yes | Yes |
| Session key agreement | Yes | Yes | No | Yes | Yes |
| Forward secrecy | No | No | No | Yes | Yes |
| Two factor security | Yes | No | No | No | Yes |
| Single registration | Yes | Yes | Yes | Yes | Yes |

In order to evaluate the performance of the proposed scheme, we compare it with other schemes. TABLE V gives a brief review of their performance. To analyze the computational complexity that involves time complexity of hash function. Because exclusive-OR operation requires very few computations, it is usually negligible considering its computational cost. Therefore our improved scheme is more secure and efficient than other schemes.

TABLE V

Performance Analysis

| Phases | Lee et. al [2011] | X.Li et. al [2012] | X.Li et.al [2013] | Leu-Hsieh [2014] | Proposed Scheme |
|---|---|---|---|---|---|
| Registration Phase | 7 | 7 | 7 | 8 | 7 |
| Login Phase | 7 | 7 | 8 | 8 | 6 |
| Authentication Phase | 8 | 21 | 8 | 9 | 7 |
| Password Change Phase | 6 | 6 | 4 | 6 | 6 |
| Total | 28 | 41 | 27 | 31 | 26 |

## VIII. CONCLUSION

In this paper, we have shown that the Leu-Shieh[10] scheme's dynamic ID based remote user authentication for distributed environment using smart cards is insecure against impersonation attack, smart card stolen attack, leak verifier attack and does not provide strong mutual authentication and anonymity. We proposed an improved scheme remedy the security flaws and weakness and satisfy all of the security features needed for achieving secured authentication in multi-server environment using smart cards. Compared with all other related schemes, the functional and performance analysis shows our improved scheme use less hash operation and more secure. The computational cost has been reduced by 10% approximately and it is efficient than others.

## REFERENCES


[1] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transaction on Consumer Electronics ,vol. 50(1), 2004.

[2] L. Lamport, "Password authentication with insecure communication", Communication of ACM, vol. 24(11), pp. 770-772, 1981.

[3] W. B. Lee and C. C. Chang, "User Identification and key distribution maintaining anonymity for distributed computer network," Intl J. of Computer Systems Science and Engineering, vol. 15(4), pp. 271–350, 2000.

[4] Y.Y.Wang, J.Y.Liu,F.X.Xiao,J.Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communication, vol. 4(32), pp. 583-585, 2009.

[5] J. L.Tsai , " Efficient multi-server authentication scheme based on one-way hash function without verificationtable," Computers & Security, vol.27, pp.115-121, 2008.

[6] M.K. Khan,S.K.Kim,K.Alghathbar, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme," Computer Communication, vol. 34, pp. 305–309, 2011.

[7] R. Madhusudhan, R.C.Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," Journal of Network Security & its applications , vol.35,pp. 1235-1248, 2012.

[8] X.Li,Y.P.Xiong, J.Ma,W.D.Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards", Journal of Network and Computer Applications, vol. 35(2),pp. 763-769, 2012.

[9] X.Li, J.Ma,W.D.Wang, Y.Xiong, J.Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments", Journal of Network and Computer Applications, vol. 58(2),pp. 85-95, 2013.

[10] J.S. Leu and W.B. Hsieh, "Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards,"IET Information Security , vol. 8(2) Feb , pp.104-113,2014.

[11] C.C.Lee,T.H. Lin, R.X.Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards", Expert System and Applications, vol. 38, pp. 13863-13870, 2011.

[12] M.Kim, N.Park,D.Won, "Security improvement on a dynamic ID-based remote user authentication scheme with session key agreement for multi-server environment", Communicationsin Computer and Information Science, Springer-Verlag, vol. 339, pp.112-127, 2012.

[13] F. Wen, X.Li, "An improved dynamic ID-based remote user authentication with key agreement scheme", Computers and Electrical Engineering, vol.38,pp. 381-387, 2012.

[14] Z.Z. Wang, J.K.Ding, "An improved dynamic ID-based remote user authentication with key agreement scheme for multi-server environment", Proc. Int. Conf on Computer Science and Electronics Engineering(ICCSEE) , 2012.

[15] H.C.Hsiang, W.K. Shih, "Improvement of the secure dynamic ID based remote user authenticationn scheme for nulti-server environment", Computer Standard and Interfaces", vol 31(6), pp.1118-1123, 2009.

[16] Y.P. Liao, S.S Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standard and Interfaces, vol.31(1), pp. 24-29, 2009.

[17] M.S.Hwang , S.K.Chong, T.Y.Chen, "Dos resistant ID-based paswword authentication scheme using smart cards", Systems and Software, vol. 83(1), pp. 163-172, 2010.

[18] S.K.Sood, A.K.Sarje, K.A.Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," Journal of Networks and Computer Applications, vol.34(2),pp.609-618, 2011.

[19] M.L.Das, A.Saxena,V.P.Gulati, "A dynamic ID-based remote user authentication scheme,", IEEE Transaction on Consume Electronics", vol. 50(2), pp. 629-631, 2004.

[20] W.C.Ku, S.T.Chang, "Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards", IEICE Transaction Communication, vol. 5,pp. 2165-2167, 2005.

[21] T.S.Wu, C.L.Hsu, "Efficient user identication scheme with key distribution preserving anonymity for distributed computer networks",Computers and Security, vol. 23, pp. 120-125, 2004.

[22] R.Martinez-Pelaez, F.Rico-Novella, C.Satizabal,J. Pomykala, "Efficient and secure dynamic ID-based remote user authentication scheme with session key agreement for multi-server environment", Journal of Network Security & its applications, vol.2(4), pp. 106-116,2010.

[23] M.Kim, J.Nam, D.Won, "An improved secure dynamic ID-based remote user authentication scheme with key agreement using symmetric cryptology," Intl. Jrnl of Security and Applications, vol. 7(3) May pp. 143-151, 2013.

[24] D.Guo, F.Wen, "A more secure dynamic ID based remote user authentication scheme for multiserver environment,", J. of Computational Information Systems, vol. 9(2),pp.407-414, 2013.

[25] R.R.Ahirwal, S.S.Sonwanshi, "An efficient and secure ID-based remote user authentication scheme using smart card," Intl J. of applied Information Systems., vol. 1(6) Feb, pp.35-41, 2012.

[26] S.K.Sood, "An improved and secure smart card based dynamic identity authentication protocol,", Intl Journal of Network Security, vol. 14(1) Jan , pp. 39-46, 2012.

[27] T.T.Truong, M.T.Tran, A.D.Duong, "Modified dynamic ID-based user authentication scheme resisting smart card theft attack," An Intl Journal of Applied Mathematics & Information sciences", vol. 3(8) pp. 967-976, 2014.

[28] M.Kumar,M.K.Gupta,Saru kumari, "A remote login authentication scheme with smart cards based on unit sphere," Indian Journal of Computer Science and Engineering, vol. 1(3), pp.192-198, 2010.

**AUTHORS PROFILE**

S. Ramesh received the B.E. degree in Computer Science and Engineering from Madras University in 1992, M.S. degree in Software Systems from BITS, PILANI in 1997 and M.E. degree in 2006 from Anna University, Chennai. He is a research student of Anna University, Chennai. Currently, he is an Assistant Professor at Paavai College of Engineering in Computer Science department. His interests are in Cryptography and Network security.

Dr. V. Murali Bhaskaran received the B.E. degree in Computer Science and Engineering from the Bharathidasan University, in 1990, M.S. degree in Computer Science from BITS, PILANI in 1995 and M, E. degree in 2000 from Bharathiyar University. He received the Ph.D. degree in Computer Science and Engineering from the Bharathiyar University. Currently, he is a professor in Computer Science and Engineering at Dhirajlal Gandhi College of Technology. His research interests include Network Security, Data Mining, Image Processing and Grid Computing.