# An Improved and Efficient RSA Based Remote User Authentication Scheme using Smart Card for Telecare Medical Systems

**S. Ramesh, V. Murali Bhaskaran**

***Abstract:*** ***Password and Smart card are the authentication factors to access significant information from remote servers. Authentication schemes based on RSA which are studied intensively that are utilized in most of the telecare medical systems. Latest RSA based remote beneficiary validation scheme which does not resist against certain attacks, not satisfy functional properties and consume more computations. The existing previous schemes still have less functional strengths. However, these schemes cannot be efficient by means of performance which is measured in terms of computation and communication. The improvised scheme using smart card and hash functions remove security short comings and reduce the communication, computational cost. We compare the proposed scheme with the other current schemes, our scheme has less computational, communication cost, security attacks than other schemes and prove that it efficient one.***

***Keywords: Remote user authentication, Medical system, Cryptanalysis, Smart card.***

## I. INTRODUCTION

Most of the services use the Internet such as telecare medical information systems, online transactions, online game, online voting is done through insecure public networks. Remote user or beneficiary authentication is simpler and acceptable mechanisms which can allow only the authentic users access the remote servers may provide resources over open public common network through insecure channel such as Internet. The client-network server application offer security, which may use cryptography technique for better security. Moreover, user utilizes both identity and PIN for authentication purpose to access the significant information and services stored on the remote network server [1, 2]. Smart card or smart magnetic card is another security facility to verify the card holder has the rights for accessing the remote servers. The server does not verify the personal identification number (PIN) in the verifier table which may suffer from the risks created by the adversaries. Most of the authentication system utilizes single-way hash function and cryptography algorithms such as DES, AES, RSA, ElGamal and ECC. But these schemes cannot solve the security problems encounter at the authentication time and does not resist all kind of attacks. The main objective of our proposed scheme makes communication, storage and computation efficient by reduces the number of bits transmitted and stored between the client and the network server. The current open public network is affected by various known attacks [3-5]. The scheme uses less number of modular exponentiation and hash function. The scheme must satisfy the essential requirements but does not use PIN table and allow changing the PIN without consult the network server. Finally, the network server and client generate the sessional key together during authentication process for security and safe communication. The scheme usually meets the following requirements that are described below:

The security requirements are resisting the masquerade user attack, masquerade network server attack, parallel session, stolen verifier, PIN predicting and DOS attack. The functional requirements allow to freely choosing PIN, use timestamp, no PIN table, forward secrecy and user anonymity. The performance requirements are the cost in computation, cost involved in communication, cost in storage and execution time.

In this article, we proposed an enhanced and effective secured remote user authentication scheme that may use the one-way hash function, modular exponentiation and exclusive OR operations [6-7]. A hash function based scheme must be able to withstand all possible known attacks. The insiders attack in the in this remote user authentication scheme is removed by that all registered user's sensitive PIN cannot be easily derived.

In section II discussed the Giri's [8] remote user authentication scheme and its security weakness. Section III detailed a cryptanalysis of Giri et al. structure. The security, functionality and performance analysis of the proposed system and the other methods are discussed in sections IV, V and VI respectively. Finally, the conclusion of the article in section VII.

**Table I. Notations**

| Symbol | Descriptions |
|---|---|
| $U$ | User or beneficiary |
| $S$ | Trusted server |
| $ID$ | User Identity |
| $PW$ | Password or PIN of the user |
| $p, q$ | Too large prime numbers |
| $Z_q$ | The ring of integers modulo $q$ |
| $Z_q^*$ | The multiplicative group of $Z_q$ |

**Revised Manuscript Received on September 05, 2019.**

***** Correspondence Author

**Dr. S. Ramesh***, Department of Information Technology, Veltech Multitech Dr. Rangarajan Dr. Sagunthala Engineering College, Avadi, Chennai, India. Email: raameshs@gmail.com

**Dr. V. Murali Bhaskaran**, Department of Computer Science and Engineering, Rajalakshmi Engineering College, Thandalam, Chennai, India. Email: murali66@gmail.com

| | |
|---|---|
| $h(.)$ | One way hash function |
| $e$ | Server's public key |
| $d$ | Server's private key |
| $N_u$ | Pseudo random Nonce used by $U$ |
| $N_s$ | Pseudo random Nonce used by $S$ |
| $\oplus$ | XOR operation |
| $\|\|$ | Concatenation operation |

## II. REVIEW OF GIRI ET AL. SCHEME

### A. Initialization phase

The trusted authority Signing up Center $RC$, provides the public, private parameters and smart magnetic card to the beneficiary $U$.

Step 1: RC selects dual primes such as p, q and calculates n= p*q

Step 2: RC publishes p, q as private and 'n' as public and select a prime e as public key and compute an d which is a private key

### B. Signing up phase

When the remote user or beneficiary $U$ needs to Sign in the network server $S$, the beneficiary initially registered with network server and performs the below activities [9-11].

Step 1: Beneficiary $U$ selects identity $ID_i$, PIN $pw_i$ and a pseudo random number $b_i$. beneficiary $U$ calculates the masked PIN $PW_i = h(b_i \| pw_i)$

Step 2: $U$ send their $ID_i$, masked PIN $PW_i$ to the network server $S$ via a protected channel for Signing up.

Step 3: Next $S$ perform the below computation

$$A_i = h(ID_i \| d)$$
$$B_i = A_i \oplus PW_i$$
$$C_i = (A_i \| PW_i)^e$$
$$D_i = h(A_i \| PW_i)$$

Step 4: $S$ store $h(.), ID_i, B_i, C_i, D_i, p, q$ on the beneficiary smart magnetic card $SC$. The data in the $SC$ directs to the beneficiary $U$ through a protected channel. Later getting $SC$ securely $U$ stores random number $b_i$ into the smart magnetic card $SC$.

### C. Sign in phase

When the beneficiary $U$ needs to Sign in to remote network server $S$, the subsequent operations will be performed by $S$

Step 1: Beneficiary $U$ keep their smart magnetic card into smart magnetic card reader and input their identity $ID_i$, and PIN $pw_i$

Step 2: Smart magnetic card makes computation as

$$PW_i = h(b_i \| pw_i)$$
$$A_i^{'} = B_i \oplus PW_i$$
$$D_i^{'} = h(A_i^{'} \| PW_i)$$

The $D_i$ in the smart magnetic card has been compared with $D_i^{'}$. If they are unequal, beneficiary enters incorrect PIN and terminate the session.

Step 3: Otherwise the beneficiary $U$ choose a pseudo random number $N_u$ and the smart magnetic card does the subsequent computations.

$$E_i = h(PW_i \| N_u \| A_i^{'})$$
$$F_i = PW_i \oplus N_u$$

Step 4: The smart magnetic card demands the Sign in information $ID_i, C_i, E_i, F_i$ to the network server $S$.

### D. D. Authentication phase

The authenticated Sign in seeks information $ID_i, C_i, E_i, F_i$ that is received by the remote network server $S$.

Step 1: Network server $S$ validate the $ID_i$, if it is invalid $S$ reject's beneficiary $U$'s Sign in request. Otherwise, network server $S$ calculates $A_i^* = h(ID_i \| d)$, $PW_i \| A_i^* = C_i^d \bmod n$ and compares $A_i^*$ with $A_i$. If both of them i.e. $A_i^* = A_i$ are equal, $S$ accept $U$'s Sign in call, otherwise it is rejected.

Step 2: Network server $S$ calculates $N_u^* = F_i \oplus PW_i$, $E_i^* = h(PW_i \| N_u^* \| A_i)$. The network server $S$ compare the calculated value $E_i^*$ with the received value $E_i$. If both are equal $U$ is a valid beneficiary and continues for subsequent step.

Step 3: Network server $S$ generates a pseudo random number $N_s$ and calculates $N_r = N_u^* \oplus N_s$ and $G_i = h(A_i \| N_s)$. $S$ sends the reply information $G_i, N_s$ to the beneficiary $U$.

Step 4: $U$ receive the reply information and derive $N_s^{'} = N_r \oplus N_i$ and calculates $G_i^{'} = h(A_i \| N_s^{'})$. The beneficiary $U$ matches the calculated value $G_i^{'}$ with the received value $G_i$. If it matched $S$ authenticates $U$. Otherwise terminate the session. Next both the beneficiary $U$ and the network server $S$ agree common secret session key

$SK_u = h(ID_i \| PW_i \| N_u \| N_s^{'})$ or $SK_s = h(ID_i \| PW_i \| N_s \| N_u^{'})$ for further secure communication in the same session.

**PIN change phase**

Whenever beneficiary $U$ wish to modify their PIN $pw_i$ with a new PIN $pw_i^{new}$, the forthcoming process will be executed

Step 1: Beneficiary $U$ keeps their smart magnetic card $SC$ into the smart magnetic card reader and enters their $ID_i$, $pw_i$ and new PIN $pw_i^{new}$.

Step 2: Beneficiary smart magnetic card $SC$ calculates $PW_i^{'} = h(b_i \| pw_i)$, $A_i^{'} = B_i \oplus PW_i = h(ID_i \| d)$ and $D_i^{'} = h(A_i^{'} \| PW_i)$ compares $D_i^{'}$ with $D_i$. If both are not equal, reject PIN modification request, otherwise the smart magnetic card calculates. $PW_i^{new} = h(\mathrm{pw}_i^{new} \| b_i)$, $B_i^{new} = A_i^{'} \oplus PW_i^{new}$ $C_i^{new} = (A_i^{'} \| PW_i^{new})^e$ and $D_i^{new} = h(A_i^{'} \| PW_i^{new})$

Step 3: At last $U$ 's smart magnetic card $SC$ replace $B_i$ with $B_i^{new}$, $C_i$ with $C_i^{new}$ and $D_i$ with $D_i^{new}$.

## III. CRYPTANALYSIS OF GIRI ET AL. SCHEME

### A. Impersonation attack

In the authentication phase any third party / attacker act as like the original beneficiary, he extracts the information stored on the smart magnetic card. By knowing the PIN he obtain $h(ID)^x$, he then choose the random number, set the timestamp with the current time, calculates $B = h(ID)^{PW} \bmod p$ and $D = h(ID)^{N_u} \bmod p$ .he sends $ID, D, M_1, T_u$ to the network server.

### B. Server spoofing attack

Any third party / attacker intercept the Sign in information $ID, D, M_1, T_u$ send to the network server and try to know the value of $B$, the random number .Next he act as like the network server and create the fake information $ID, V, M_2, T_s$ and send to the beneficiary. The beneficiary accepts authenticated information from the third party / attacker and communicates to the third party / attacker as like the original network server.

### C. PIN predicting attack

The beneficiary's PIN and secret key can be guessed or extracted using the secret values from the smart magnetic card and information exchanged between beneficiary and network server. Thus the system is not safe and infected by the PIN guessing attack.

### D. Beneficiary anonymity

Beneficiary identity $ID_i$ is transmitted in plain text form; any third party can eave Sign in information $ID, D, M_1, T_u$. Static *ID* is utilized during Sign in request information of enrolment, validation and session key creation stage. Any third party / attacker easily track the various Sign in request information belongs to the same beneficiary and attempt to derive some related to the beneficiary $U$.

## IV. PROPOSED SCHEME

### A. Initialization phase

The trusted authority Signing up Center $RC$, it provides the public , private parameters and smart magnetic card to the beneficiary $U$.

Step 1: $RC$ chooses two large primes $p, q$ and calculates $n = pq$.

Step 2: $RC$ publishes $p, q$ as private and $n$ as public and select a prime number $e$ which is public key and calculate $d$ that is private key.

### B. Signing up phase

The remote beneficiary $U$ needs to Sign in the network server $S$, the beneficiary initially registered with network server and performs the below activities.

Step 1: $U$ choose identity $ID_i$, PIN $pw_i$ and a pseudo random number $b_i$. $U$ calculates the masked PIN $PW_i = h(b_i \oplus pw_i)$

Step 2: $U$ send their $ID_i$, masked PIN $PW_i$ to the network server $S$ through a protected channel.

Step 2: Next $S$ perform the below computation

$$A_i = h(ID_i \| d)$$
$$B_i = A_i \oplus PW_i$$

Step 3: $S$ store $h(.), ID_i, B_i, n, e$ on the beneficiary smart magnetic card and directs it to the beneficiary $U$ through a protected channel. $U$ stores random number $b_i$ into the smart magnetic card $SC$.

### C. Login phase

When the beneficiary $U$ needs to login to the remote network server $S$, the succeeding operations will be done by $S$

Step 1: Beneficiary $U$ inserts their smart magnetic card $SC$ into smart magnetic card reader and input identity $ID_i$, and PIN $pw_i$

Step 2: Beneficiary's $U$ smart magnetic card $SC$ performs below computations

$$PW_i = h(b_i \oplus pw_i)$$

$A_i^{'} = B_i \oplus PW_i$

$C_i = (A_i \oplus N_u)^e$

$D_i = h(N_u)$, where $N_u$ is the beneficiary $U$ 's pseudo random number and $D_i$ is beneficiaries information authentication code.

Step 3: The smart magnetic card directs the requested Sign in information $ID_i, C_i, D_i$ to the network server $S$ over the protected channel.

### D. Authentication phase

The authenticated Sign in request information $ID_i, C_i, D_i$ is received by the remote network server $S$ .

Step 1: Network server $S$ validate the $ID_i$, if it is invalid $S$ reject's beneficiary $U$ 's Sign in request.

Step 2: Otherwise Network server $S$ calculates

$A_i^* = h(ID_i \| d)$

$N_u^{'} = (C_i)^d \oplus A_i^*$

$D_i^* = h(N_u^{'})$.

The network server $S$ relates the calculated value $D_i^*$ with the received $D_i$. If both are identical $U$ is a valid beneficiary and proceeds for next step.

Step 3: Server $S$ creates a pseudo random number $N_s$ and calculates $E_i = (A_i^* \oplus N_s \oplus N_u^{'})$ and $F_i = h(N_s)$. $S$ sends reply information $E_i, F_i$ to the beneficiary $U$ .

Step 4: $U$ receive reply information and derive $N_s^{'} = E_i \oplus N_u \oplus A_i$ and calculates $F_i^{'} = h(N_s^{'})$. The beneficiary $U$ compares the calculated value $F_i^{'}$ with the received $F_i$. If it matches $S$ authenticates $U$ . Otherwise terminate the session.

### E. Session key generation phase

Step 1: Both the beneficiary $U$ and the network server $S$ calculate the session key $h(ID_i \| PW_i \| F_i \| D_i)$ for protected communication.

### F. PIN change phase

Whenever beneficiary $U$ wants to change their PIN $pw_i$ with a new PIN $pw_i^{new}$, the below process will be performed.

Step 1: Beneficiary $U$ inserts their smart magnetic card $SC$ into the smart magnetic card reader and enters their $ID_i$, $pw_i$ and fresh PIN $pw_i^{new}$ .

Step 2: Beneficiary smart magnetic card $SC$ calculates $PW_i^{'} = h(b_i \oplus pw_i)$, $A_i^{'} = B_i \oplus PW_i$ and compares $A_i^{'}$ with $A_i$. If both are not equal, reject PIN modification request, else the smart magnetic card computes. $PW_i^{new} = h(pw_i^{new} \oplus b_i)$, $B_i^{new} = A_i^{'} \oplus PW_i^{new}$

Step 3: At last $U$ 's smart magnetic card $SC$ replace $B_i$ with $B_i^{new}$.

## V. RESULTS

By conducting experiments, we have evaluated the performance of our newly designed scheme. We compared the proposed system with other associated schemes by using parameters of computational cost, communication cost and security. We have conducted the experiments by using client machine configuration of Core 2 Duo PC with 2.33 GHz CPU speed and 1 GB memory and server machine configuration of Xeon processor with 2.66 GHz CPU speed and 1 GB memory similar with [12-14]. The test program is coded in Java, compiled to run in Java native code. Our protocol use SHA256 for hash function. The computation cost is total time taken by the protocol including client and network server execution time. The schemes that use modular exponentiation take more computational cost. Our proposed protocol has revealed that it is time intense due to less modular exponentiation accomplished and less hash functions calculated. The proposed protocol has less communication and computation that is described in Table III and Table IV.

## VI. DISCUSSION

### A. Security Analysis

TABLE II shows that comparison of the proposed method with other associated methods based on the security requirements. With the outcome of security analysis, the proposed scheme satisfies more security criteria as compared with other validation methods using non-tamper smart magnetic card.

**a. *Resist server impersonation attack***

By intercepting the Sign in information $ID_i, C_i, D_i$ send to the network server, however an intruder is very hard to find the value of $A_i$ . An attacker by knowing the value of $N_u^{'}$ and $N_s$ cannot compute $M_3 = (A_i^* \oplus N_s \oplus N_u^{'})$ who can pretend like the network server $S_i$. Hence, there is no chance of impersonation attack.

**b. Resist forgery attack**

In the proposed method a valid request information of login phase can be generated by the legitimate beneficiary. An intruder $A$ cannot find the individual values b, d from the sign in request information $ID_i, C_i, D_i$ . Hence there is no way of forgery attack in the proposed scheme. Illegitimate persons do not forge any false information of all phases in the scheme while the communication taken between the parties.

**c. Resist modification attack**

The information is exchanged between beneficiary and network server in all phases of the system is highly protected by hash value and random nonce. The intruder captures the information and modifying the information is impossible due to one-way variable length hash function and random property. In this scheme, each information is flow in either direction along with authentication code such that there is no possibility of modifying the information

**d. Resist replay attack**

An attacker interrupts the Sign in information $ID_i, C_i, D_i$ of the beneficiary $C_i$ and replay information to the network server $S_i$. The network server immediately replies the information $E_i, F_i$ to the beneficiary. In each and every session of the proposed scheme beneficiary and network server produce different random nonce. The information passes between the beneficiary and network server during interaction session uses random nonce.

**e. Resist parallel session attack**

Suppose an intruder intercept the Sign in information when Sign in takes place and wants to initiate the parallel session attack. The network server computes the value of $D_i^*$ and verifies the value with $D_i$. Thus the attacker does not start the parallel session attack due to the value which is hold by the beneficiary. There is no such possibility of parallel session attack in this scheme.

**Table II. Security analysis**

| *Security Parameters* | *Awasthi et al.* | *Shi & Chen* | *Khan & Kumari* | *Giri et al.* | *Proposed* |
|---|---|---|---|---|---|
| Resist Offline dictionary attack | No | No | No | Yes | Yes |
| Resist Server impersonation attack | No | No | No | No | Yes |
| Resist Forgery attack | No | No | Yes | No | Yes |
| Resist Modification attack | No | No | No | Yes | Yes |
| Resist Replay attack | No | No | No | Yes | Yes |
| Resist Parallel session attack | No | No | Yes | Yes | Yes |
| PIN Provision of non-repudiation | Yes | Yes | No | Yes | |

## B. Performance and Functional Analysis

**Table III. Functional analysis**

| *Functional Parameters* | *Shi & Chen* | *Khan & Kumari* | *Giri et al.* | *Proposed* |
|---|---|---|---|---|
| Strong mutual authentication | No | No | No | Yes |
| User anonymity | No | No | No | Yes |
| Perfect forward secrecy | No | Yes | Yes | Yes |
| Freely change | Yes | Yes | Yes | Yes |

**Table IV. Performance Analysis**

| *Phases* | *Schemes* | | | |
|---|---|---|---|---|
| | **Shi and Chen** | **Khan & Kumari** | **Giri et al.** | **Proposed** |
| **RP** | $2T_h+3T_x$ | $4T_h+1T_m+2T_o$ | $3T_h+1T_m+4T_o$ | $2T_h+2T_x+1T_o$ |
| **LP** | $2T_h+1T_m+2T_x+3T_o$ | $3T_h+1T_m+4T_o$ | $3T_h+2T_x+4T_o$ | $1T_h+1T_m+2T_x$ |
| **AP** | $4T_h+1T_m+1T_x+3T_o$ | $2T_h+3T_m+6T_o$ | $3T_h+1T_m+3T_x+11T_o$ | $4T_h+1T_m+3T_x+3T_o$ |
| **PWCP** | $2T_h+3T_x$ | $6T_h+5T_o$ | $4T_h+1T_m+2T_x+5T_o$ | $2T_h+4T_x$ |
| **TOTAL** | $10T_h+2T_m+9T_x+6T_o$ | $15T_h+5T_m+17T_o$ | $13T_h+3T_m+7T_x+24T_o$ | $9T_h+2T_m+11T_x+4T_o$ |

In this part we ascertain that our proposed method consumes low cost by analyzing of various other schemes. To design a scheme that should have less communication bits, low computational cost that use minimal number of modular exponentiation. In this scheme uses the computational factors such as modular exponentiation, hash function, pseudo random number and symmetric en/decryption. These operations are the most common operations for the construction of the scheme except XOR operation due to expeditious execution.

Table III shows the functional analysis and Table IV shows the performance comparison of our scheme with other schemes. In Table IV, the term $T_h$ is used for time complexity of hash function, $T_x$ for XOR function, $T_m$ for modular exponentiation, $T_o$ for OR function.

## VII. CONCLUSION

In this paper, we have recently proposed an improved communication efficient new beneficiary authentication scheme for remote accessing remedy the security flaws and weakness. We crypt-analysis of Giri et al. scheme in which does not defend against replay attack, leakage verifier attack. Moreover, current scheme cannot provide the functional parameters such as strong mutual authentication, exact forward secrecy and anonymity preserving. Compared the new proposed scheme with other related authentication schemes, analysis the functional parameters and evaluate the performance which shows our scheme uses less modular exponentiations and more protected. The proposed scheme was strong against the vulnerabilities were present in the past public key based remote beneficiary authentication schemes even though they use the cryptographic functions and smart magnetic cards. With the help of formal and informal security analysis our scheme defended against all possible attacks were present in Giri's scheme. Furthermore, by analyzing the functional abilities the new scheme has strong mutual authentication, preserving anonymity and PFS.

According to the performance wise the improved scheme have less computational cost in terms of modular exponentiation operation than others.

## REFERENCES


1. S.Ramesh,V. Murali Bhaskaran, "A secured and Improved Dynamic ID based Remote User Authentication Scheme using Smart Card and Hash Function for Distributed Systems", International Journal of Computer Science and Engineering, vol 6(8), 2014,pp. 305-320.
2. S.Ramesh,V. Murali Bhaskaran, "An Improved Remote User Authentication Scheme with Elliptic Curve Cryptography and Smart Card without bilinear pairings", International Journal of Computer Science and Engineering, vol 5(6), 2013,pp. 5140-5154.
3. R.C.Wang,W.S. Juang, C.L.Lei, , "Provably secure and efficient identification and key agreement protocol with user anonymity", *J. Computer Systems. Sci.* vol. 77(4), 2011, pp.790–798.
4. D.He, J.Chen, Y.Chen, "A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography". J. *Security of. Communication. Network.* vol. 5(12), 2012, pp.1423–1429.
5. D. He, J. Chen, R.Zhang, "A more secure authentication scheme for telecare medicine information systems", J. Med. Syst. vol. 36(3), 2012, pp. 1989-1995.
6. Z.Zhu, "an efficient authentication scheme for telecare medicine systems", J. Med. Syst. vol. 36(6), 2012, pp. 3833-38383..
7. Preeti chandrasekar, Hari Ohm, "RSA based two factor remote user authentication scheme with user anonymity", Elsevier Procedia Computer Science, vol. 70, 2015, pp. 318-324.
8. D.Giri, T.Maitra, R.Amin, P.D.Srivastava, "An efficient and robust RSA based remote user authentication scheme for telecare medical information systems", J. Med. Syst. vol. 39(145), 2015, pp. 3833-38383.
9. A.K.Das,A.Goswami, "A secure and efficient uniqueness and anonymity preserving remote user authentication scheme for connected health care",J. Med System, vol. 37(3), 2013, pp; 1-16.
10. M.Karuppiah, R.Saravanan, "A secure remote user mutual authentication scheme using smart cards", vol. 19(4), 2014, pp. 282-294.
11. Karthick, K & Kavaskar, S 2019, 'Text detection and Recognition in Raw Image Dataset of Seven Segment Digital Energy Meter Display', Energy Reports, Elsevier. Vol. 5, November 2019, pp. 842-852, (ISSN 2352-4847).
12. Karthick, K & Chitra, S 2017, 'Novel Method for Energy Consumption Billing Using Optical Character Recognition', Energy Engineering: Journal of Association of Energy Engineers, Taylor & Francis, vol. 114, no. 3, pp. 64-76, ISSN:1998595
13. Karthick, K & Chitra, S 2016, 'Review of Optical Character Recognition and Its Applications', ARPN Journal of Engineering and Applied Sciences, Asian Research Publishing Network (ARPN), vol. 11, no. 5, pp. 3441-3444, ISSN 1819-6608
14. Karthick, K, Premkumar, M, Manikandan, R & Cristin, R 2018, 'Study on Diverse Automatic Identification Techniques', International Journal of Engineering & Technology (UAE), Science Publishing Corporation Inc., Vol.7 No.4, pp. 2895-2898.
15. M.K.Khan, S. Kumari, "Authentication scheme for secure access to healthcare services", J. Med. Syst. vol. 37(4), 2013, pp. 1-12.


## AUTHORS PROFILE

**Dr. S. Ramesh** is working as professor in Information Technology department at Veltech Multitech Dr. Rangarajan Dr. Saguntaha Engineering college, Chennai. He received his B.E. Degree in CSE from University of Madras in the year 1991, M.E. and PhD degrees in Computer Science and Engineering from Anna University, Chennai in the year 2006 and 2015 respectively. He completed his M.S degree at BITS, pilani in the year of 1997.He has published more than 15 papers in Journals and Conferences in National and International level. . His areas of interest include Network Security, Information Security, Big Data and Data Analytics, etc. He is the member in societies like ISTE and CSI.

**Dr. V. Murali Bhaskaran** is working as a professor in CSE, Rajalakshmi Engineering College, Chennai and having more than 25 years of academic career in teaching, research and administration in various Engineering institutions. He obtained his B.E. Degree in CSE from Bharathidasan University, Trichy in the year 1989, and completed M.E. and PhD degrees in CSE from Bharathiar University, Coimbatore in the year 2000 and 2008 respectively. He has guided 19 PhD scholars and published more than 35 papers in various journals and conferences in national and international level. He is the member in societies like ISTE, CSI, ACS and NCSSS.