International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

# An Efficient Elliptic Curve Based Smart Card Authentication Scheme

**Anuj Kumar Singh, B.D.K. Patro**

***Abstract*: With the innovation and advances in technology, the usage of smart cards has grown up rapidly in a wide range of applications including the Internet of Things. Particularly, the smart card facilitates the process of authentication of a legitimate user by the server providing some services. Therefore, smart card security has been a primary concern for the researchers. This article presents an efficient smart card authentication mechanism based on the elliptic curve, which provides all the essential security properties, while simultaneously providing resistance from the threats and attacks made on to the system. Furthermore, the results show that the proposed scheme is time efficient than other related schemes.**

***Index Terms*: Authentication, elliptic curve, key agreement, smart cards.**

## I. INTRODUCTION

In a communication environment, there are different parties involved in transmitting information to each other. For secure communication, the authentication and key establishment are the two essential building blocks which ensure the verification of identities of the parties and encryption of secret information respectively. Generally, these types of communications can be modeled as the user-server model, where a user willing to access the facilities or services provided by a server, has to register with the server. The server must ensure that it is granting services to a legitimate user and a user must ensure that the server is a legal party in the communication. The three kinds of authentication approaches in a user-server environment are certificate based-approaches, identity-based approaches, and the password-based approaches [1]. Out of these three approaches, password-based approaches have been particularly attractive, since the password is easy to remember and these approaches are relatively easy to implement. In password based approaches the user has to remember a password for accessing the services of a server, at the same time the server is required to maintain a table of passwords and identities to verify the validity of passwords. However, the password based schemes are more susceptible to offline password guessing attacks. To overcome this, two-tier authentication schemes can be developed in which the password of the user along with the smart card is used in the authentication process. The two-tier approach for authentication is more secure because if any one of the two secrets i.e. either the password or the smart card is exposed to an attacker then also the scheme is secure. But, it must be ensured that both the password and the smart card must not be revealed to an opponent simultaneously.

**Manuscript published on 30 June 2019.**
* Correspondence Author (s)
**Anuj Kumar Singh***, Amity University Haryana, Gurugram, India
**B.D.K. Patro**, Rajkiya Engineering College, Kannauj, U.P., India



## II. SECURITY REQUIREMENTS AND CHALLENGES

Mutual authentication, integrity, confidentiality, and non-repudiation are the four basic security attributes which must be provided by any communication system. However, K. Markantonakis [2] have made an analysis on the security of smart card based system and figured out that except these four basic security attributes, availability and forward security must also be implemented to make these systems secure. In addition to providing the security properties, the smart card based authentication system must also counter against different attacks launched by the attackers. H. Ko and R. D. Caytiles [3] performed a detailed analysis of the security issues of smart card based systems. They explored that the attacks on the smart card can be divided into four classes – logical attacks, side channel attacks, physical attacks, and other attacks. The taxonomy of attacks on smart cards has been shown in Table I. The limitations of smart card based systems in fulfilling the security requirements includes less computational capacity, low power, and less bandwidth. Typically, a smart card possesses CPU clock rate of up to 5 MHz, RAM size up to few 100s KB, and maximum flash memory of 1 MB [4]. These limitations enforce the challenges in achieving the desired security level. Therefore efficient cryptographic mechanisms must be designed and implemented to make these systems secure in a way that all the necessary security functionalities are provided and the consumed computational cost is very reasonable.

## III. RELATED WORK

A brief discussion of the authentication schemes based on password and the smart card has been presented in this section of the paper. C.C. Chang and T.C. Wu [5] presented an authentication scheme based on smart card and password, which provides enhanced security than only password-based schemes. M.L. Das et al. [6] developed the first password and smart card based authentication approach based on dynamic identity, which overpowered the weaknesses of static identity-based schemes.

**Table I. Taxonomy of attacks on smart cards.**

| Class of Attack | Specific Attack |
|---|---|
| Logical attacks | Hidden commands |
| | Parameter poisoning |
| | File access |

| | |
|---|---|
| | Malicious Applets |
| Physical attacks | Reverse engineering |
| | Probe stations |
| | Ion beams |
| Side channel attacks | Eavesdropping |
| | Differential power analysis |
| | Simple power analysis |
| | Password cracking |
| | Denial of service |
| | Power glitching |
| Other attacks | Covert Transactions |
| | Interruption of Operations |
| | Dual modes |

I.E. Liao et al. [7] proved that the authentication approach of M.L. Das et al. [6] is susceptible to user impersonation attack. Liao et al. also suggested a dynamic identity authentication protocol for both the parties which is secure from user impersonation attack.

I.C. Lin et al. [8] presented an authentication approach based on ElGamal signature for theremote user in the multi-server environment.

Y. P. Liao et al. [9] developed the first dynamic identity authentication approach for multi-server settings. But, H.C. Hsiang et al.[10] explored that Y. P. Liao's approach is susceptible to impersonation attack, insider attack, and forgery. They also suggested an improved protocol which overcame these shortcomings.

S. K. Sood et al. [11] explored that Hsiang et al.'s scheme is prone to the impersonation attack, replay attack, and stolen smartcard attack.

K.H. Yeh [12] designed a security enhanced authentication approach based on the elliptic curve which is secure from man-in-the middle attack and the user or server impersonation attack.

S. Chaudhry et al. [13] presented an elliptic curve based remote user authentication mechanism. They also proved that the protocol given by B. Huang et al. [14] has correctness issued and it is also susceptible to forgery and impersonation attack.

Recently T.T. Truong et al. [15] have developed an elliptic curve user authentication scheme for multi-server settings and claimed that it is secure. This scheme is based on identity. However, Y.Zhao et al. [16] have proved that T.T. Truong et al.'s scheme is defenseless from impersonation attack and password guessing attack.

## IV. THE PROPOSED SMART CARD AUTHENTICATION SCHEME

The proposed smart card authentication scheme has four phases – the initialization phase, the registration phase, and the mutual authentication phase. There are three parties involved in the whole protocol, first is the user $U$with a smart card, second is the server$S$, and the third is the registration center$RC$. The notations and the symbols used in the protocol have been mentioned in Table II.

**Table II. Symbols and notations used.**

| Symbol | Notation |
|---|---|
| $q$ | Large prime number |
| $F_q$ | Finite field of size $q$ |
| $E$ | Elliptic curve on $F_q$ |
| $A, B$ | Elliptic curve parameters |
| $G$ | Base point of E |
| $O$ | Point on infinity |
| $H$ | Hash function |
| $P_S$ | Server's public key |
| $ID_S$ | Server's identity |
| $ID_U$ | User's identity |
| $PW_U$ | User's password |
| $T$ | Current timestamp |
| $t$ | Expected delay |

### A. The Initialization Phase

In the initialization phase, the registration center initializes the global system parameters as follows:

1) An elliptic curve $E: y^2 = x^3 + Ax + B$ on $F_q$ having curve factors $\{A, B, q, G, n\}$sustaining $4A^3 + 27B^2 \neq 0$.
2) Randomly selects$\beta \in Z_n$.
3) Also chooses the hash function$H: \{0,1\}^* \rightarrow \{0,1\}^l$.
4) Parameters $\{A, B, qG, n, F_q, E(F_q), G, H, P_S\}$ are published by the registration center and β iskept secret. Where, $P_S$ is the server's public key.

### B. Registration Phase.

In the registration phase, the user and the server register themselves with the registration center$RC$. This phase has been divided into parts, first is the registration of the server with the $RC$and second is the registration of the user with the $RC$.

1) The steps carried out in the registration of a server with the registration center $RC$are:

- The server $S$ selects its identity $ID_S$, and sends the message $\{ID_S\}$ to the $RC$using a secure channel. The server also computes its public key $P_S = ID_S G$.
- Upon receiving the message of registration request from the server, the $RC$first selects $\beta \in Z_n$ and computes
$$A_S = H(ID_S \oplus \beta)$$
- The registration center$RC$transmits the message $\{A_S\}$ to the server.

The process of server registration with the registration center has been shown in Figure 1.

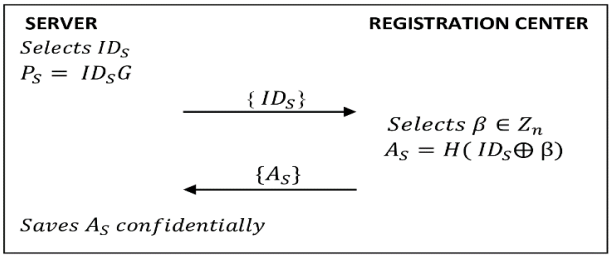


**Figure 1. Registration of the server with the registration center.**


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

2) When a user wishes to register with the registration center$RC$, the steps given below are executed:

- The user $U$ selects its identity $ID_U$ and the password $PW_U$. Furthermore, the user randomly selects a number$u \in Z_n$.
- The user computes
$$R = (PW_U \oplus u)$$
- The user then sends the message $\{ID_U, R\}$ to the $RC$, through a secure channel for issuing a smart card. Since the smart card is needed to access and use the services or facilities provided by the server.
- Upon getting the registration request form $U$, the registration center $RC$computes
$$A_{SU} = (A_S \oplus R \oplus ID_U)$$
And then the $RC$ issues the smart card to the user which contains $\{A_{SU}, H(), G\}$.
- Upon getting the smart card from $RC$,the user $U$marks the smart card with number $u$ and saves it.

The process of user registration with the registration center has been shown in Figure 2.

In this way, both the user and the server are registered with the registration center.

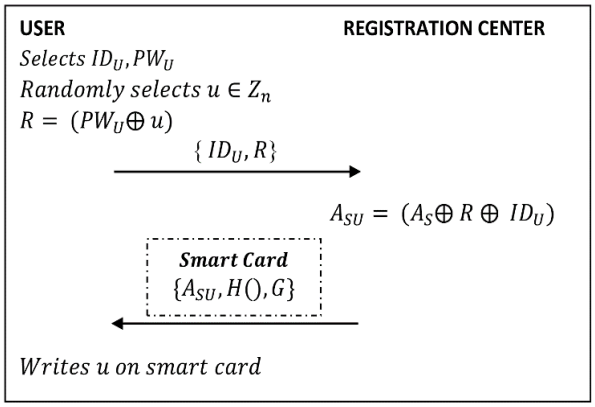


**Figure 2. Registration of the user with the registration center.**

### C. Mutual Authentication Phase

In this phase both the parties including the user $U$ and the server $S$ authenticate each other to ensure that they are communicating with the legitimate party, i.e. the user server $S$ ensures that the user $U$ is a genuine user while the user $U$ ensures that he is getting the services from a legal server. The steps in the mutual authentication are given below.

1) At the user's end following computations are made.

- The user $U$insets the issued smart card into a reader or device for authentication purpose. Moreover, he also enters the identity $ID_U$ and the password $PW_U$.
- The smart card computes
$$A' = A_{SU} \oplus ID_U \oplus PW_U \oplus u$$
- The smart card selects $v \in Z_n$ and computes $P_U = vG$.
- The Smart card also computes
the key $K = vP_S$
Produces ciphertext $c = E_K(A')$
$$r = H(c \oplus K)$$
$$Q = rG$$
- Timestamp $T_U$ is recorded, then the message $\{c, r, Q, P_U, T_U\}$ is sent to the server.

2) Upon getting the message $\{c, r, Q, P_U, T_U\}$ from $U$:

- The server $S$ first verifies whether
$$T - T_U \leq t$$
Here$T$ is the current timestamp and t is the expected delay. If it is not true then the session is terminated. After successfully verifying the timestamp, the server computes the following:
$$K' = ID_S P_U$$
$$A' = D_{K'}(c)$$
- If $A' = A_S$then the user $U$ is authenticated by the server.
- The server further computes
$$r' = H(A' \oplus K')$$
$$Q' = r'G$$
$$a_s = E_{K'}(Q' \oplus K')$$
The server records the timestamp$T_S$ and transmits the message $\{a_s, T_S\}$ to the user.
- Upon getting the message $\{a_s, T_S\}$, the user first verifies whether
$$T - T_S \leq t$$
If it is not true then the session is terminated. After successfully verifying the timestamp, the user computes
$$a_s{}' = E_{K'}(Q \oplus K)$$
If $a_s = a_s{}'$ , then the server $S$is successfully authenticated by the user$U$.

## V. PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME

The performance analysis of the presented elliptic curve smart card based authentication scheme has been done in this section with respect to two dimensions. The first is the computational cost consumed by the presented scheme and second is the security functionalities offered by the presented scheme.

### A. Computational Cost Analysis

The computational time of the proposed scheme can be evaluated by counting the most significant operations executed by the scheme. The authentication schemes proposed for the smart cards are either based on modular exponentiation or based on the elliptic curve. The modular exponentiation operation and the point multiplication on the elliptic curve are the two most time consuming operations.


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

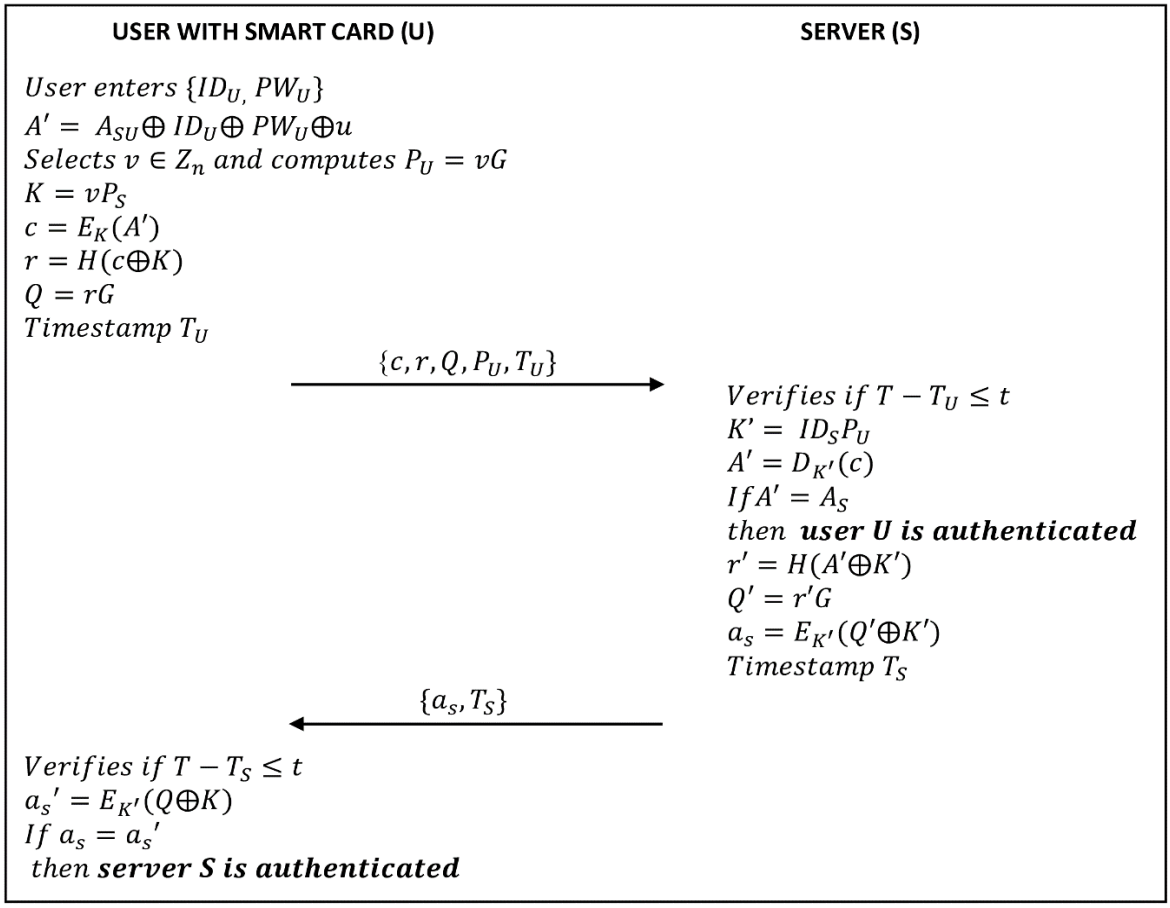


**Figure 3. Mutual authentication phase of the proposed scheme.**

**Table III. Comparison of computational time of different schemes.**

| Protocol | No. of operations performed | | | | | | Time (ms) | | |
|---|---|---|---|---|---|---|---|---|---|
| | User | | Server | | Total | | User | Server | Total |
| | *p* | *e* | *p* | *e* | *p* | *e* | | | |
| Yeh et al. [12] | 0 | 2 | 0 | 4 | 0 | 6 | 6.086 | 12.172 | 18.258 |
| Wang et al. [16] | 0 | 2 | 0 | 1 | 0 | 3 | 6.086 | 3.043 | 9.129 |
| Chaudhry et al. [13] | 3 | 0 | 3 | 0 | 6 | 0 | 7.503 | 7.503 | 15.006 |
| Xie et al. [17] | 3 | 0 | 3 | 0 | 6 | 0 | 7.503 | 7.503 | 15.006 |
| Truong et al. [15] | 2 | 0 | 2 | 0 | 4 | 0 | 5.002 | 5.002 | 10.004 |
| ***Proposed Scheme*** | ***3*** | ***0*** | ***2*** | ***0*** | ***5*** | ***0*** | ***7.503*** | ***5.002*** | ***12.505*** |

*p-elliptic curve point multiplication, e-modular exponentiation*

Q.Xie et al. [17] have mentioned that using Intel i5 processor having 8 GB RAM and clock rate of 2.5 GHz, it consumes 3.043 ms in executing one modular exponentiation and 2.501 ms in a single elliptic curve point multiplication operation.The time consumed by the other operations is very small in comparison to modular exponentiation operation and the point multiplication on the elliptic curve, and therefore has been ignored in the analysis. On the basis of these facts, a comparison of computational time consumed by different smart card authentication schemes has been made and shown in Table III.

From Table III, it can be understood that in the presented scheme, the user takes three point multiplication operations and the server takes two point multiplication operations. Therefore, the time consumed by the user is 7.503 ms and the time consumed by the server is 5.002 ms.

### B. Analysis of Security Functionalities

The analysis of security functionalities can be performed in two phases, first is the analysis of security properties satisfied by the presented scheme, and second is the analysis of defense capability from attacks on smart card based systems.The proposed smart card authentication scheme satisfies mutual authentication, secure key agreement, anonymity, forward security, two-factor authentication, and availability.

A comparative analysis of security attributes of the presented scheme with the related schemes in [12, 13, 15, 16, 17] have been performed and shown in Table IV.

**Table IV. Comparison of security properties of different schemes.**

| Protocol | Security attributes | | | | | |
|---|---|---|---|---|---|---|
| | MUA | SKE | FWS | ANO | TFA | AVA |
| Yeh et al. [12] | × | × | ✓ | × | × | ✓ |
| Wang et al. [16] | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| Chaudhry et al. [13] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Xie et al. [17] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Truong et al. [15] | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| ***Proposed Protocol*** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

*MUA-Mutual authentication, SKA-Secure key exchange, FWS-Forward security, ANO- Anonymity, TFA-Two factor authentication, AVA-Availability, ✓- Satisfied, × - Not Satisfied.*

Furthermore, the proposed scheme successfully provides resistance against replay attack, known key attack, user impersonation, server impersonation, insider attack, and password guessing attack.The defense capability of the proposed scheme against different attacks has been compared with the related schemes in [12, 13, 15, 16, 17] and publicized in Table V.

**Table V. Comparison of resistance capability of different schemes from the attacks.**

| Protocol | Resistance against attacks | | | | | |
|---|---|---|---|---|---|---|
| | RPA | KNA | UIM | SIM | INS | PWG |
| Yeh et al. [12] | ✓ | ✓ | × | ✓ | ✓ | × |
| Wang et al. [16] | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| Chaudhry et al. [13] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Xie et al. [17] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Truong et al. [15] | ✓ | ✓ | × | × | ✓ | × |
| ***Proposed Protocol*** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

*RPA-Replay attack, KNA-Known key attack, UIM-Impersonation, SIM-Server impersonation, INS-Insider attack, PWG-Password guessing attack, ✓-Satisfied, × - Not Satisfied.*

## VI. DISCUSSION

The comparison of computational costs publicized in Table III and the security functionalities shown in Table IV and Table V shows that our presented scheme is better than the other related schemes. From Table IV and Table V it is verified that our presented scheme is the only scheme which satisfies all the security attributes and only it can counter different attacks. None of the other schemes provides all the security functionalities. Although schemes mentioned in [12, 15, 16] consumes less total time, these schemes fail to provide one or more security attributes. Therefore, the proposed scheme performs best among the schemes discussed in [12, 13, 15, 16, 17].

## VII. CONCLUSION

Smart cards are utilized in a wide range of critical applications including banking, e-commerce, secure payments, securing physical access, attendance management and many more. The major advantages of using smart cards are longer life and high security. However, due to the less computational capability of smart cards, security is a major concern. Elliptic curve based solutions have been found suitable for securing resource-constrained environments. Therefore, this paper has presented an efficient elliptic curve based security solution for smart cards. It has been revealed from the results that the proposed scheme provides availability, secure key exchange, anonymity, two-factor authentication, and forward security. Moreover, it can counter password guessing attack, insider attack, impersonation attack, known key attack, and replay attack. Additionally, the proposed scheme takes a reasonable amount of computational time. Therefore, the proposed scheme is suitable to be used for smart cards. The work explained in this paper is worth for the researchers, teachers, and professionals working in the area of security of smart cards.

## REFERENCES

1. Y. Zhao,S.Li, L. Jiang,"Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment," *Security and Communication Networks*, Vol. 2018, 2018, pp. 1-13.
2. K. Markantonakis, K. Mayes, M. Tunstall, D. Sauveron, F. Piper,"Smart Card Security," in Studies *in Computational Intelligence (SCI). Vol. 57*, J. Kacprzyk, Ed., Springer, Berlin, 2007, pp. 201-234.
3. H. KO, R. D. Caytiles, "A Review of Smart Card Security Issues," *Journal of Security Engineering*, Vol. 8, No. 3, 2011, pp. 359-370.
4. A.K. Singh, B.D.K.Patro, "Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions", *Cybernetics and Information Technologies*, Vol. 19, No. 1, 2019, pp. 133-164.
5. C.C. Chang, T.C. Wu, "Remote password authentication with smart cards," *IEEEProceedingsPart E Computers andDigital Techniques*, Vol. 138, No. 3, 1991, pp. 165–168.
6. M. L. Das, A. Saxena, V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, 2004, pp. 629–631.
7. I.E. Liao, C.C. Lee, M.S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme," in *Proceedings of the International Conference on Next Generation Web Services Practices, NWeSP 2005*, 2005, pp. 437–440.
8. I. C. Lin, M. S. Hwang, L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, Vol. 19, No. 1, 2003, pp. 13–22.
9. Y. P. Liao, S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, Vol. 31, No. 1, 2009, pp. 24–29.
10. H.C. Hsiang, W.K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme formultiserver environment," *Computer Standards & Interfaces*, Vol. 31, No. 6, 2009, pp. 1118–1123.
11. S. K. Sood, A. K. Sarje, K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, Vol. 34, No. 2, 2011, pp. 609–618.
12. K.H. Yeh, "A Provably Secure Multi-server Based Authentication Scheme,"*Wireless Personal Communications*, Vol. 79, No. 3, 2014, pp. 1621–1634.

13. S. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, M. K. Khan, "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography", *Wireless Personal Communications*, DOI 10.1007/s11277-016-3745-3, 2016.
14. B.Huang, Muhammad KhurramKhan,LibingWu,Fahad T. Muhaya, D. He, "An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography,"*Wireless Personal Communications: An International Journal*, Vol.85, No.1, 2005, pp.225-240.
15. T.T. Truong, M.T. Tran, A.D. Duong, I. Echizen, "Provable Identity Based User Authentication Scheme on ECC in Multi-server Environment,"*Wireless Personal Communications*, Vol. 95, No. 3, 2017, pp. 2785–2801, 2017.
16. D. Wang, N. Wang, P. Wang , S. Qing, "Preserving privacy for free Efficient and provably secure two-factor authentication scheme with user anonymity," *Information Sciences*, Vol. 321, 2015, 162-178.
17. Q. Xie, D.S.Wong, G.Wang, X.Tan, K.Chen, L.Fang, "Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol With Extended Security Model," *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 6, 2017, pp. 1382-1392.

## AUTHORS PROFILE

**Anuj Kumar Singh** is pursuing Ph.D in Computer Science and Engineering from Dr. A.P.J. Abdul Kalam Technical University, Lucknow (India). He is also working as Assistant Professor in Department of Computer Science & Engineering at Amity University Haryana, Gurgaon (India). He passed M.Tech degree with honours from Panjab University, Chandigarh. He has more than 14 years of teaching experience in technical education. He has published 23 research papers in journals and conferences

**Dr. B.D.K. Patro** earned Ph.D degree in Computer Science from Institute of Computer and Information Sciences, Dr.B.R.Ambedkar University, Agra. He is an Associate Professor of Computer Science & Engineering in RajkiyaEngineeirng College, Kannauj (India). He has more than 24 years of experience to teach the undergraduate and postgraduate courses. He has guided 02 Ph.d, guiding 03 Ph.d candidates and he supervised 12 M.Tech and many Undergraduate projects. He has published more than 30 research papers in journals and conferences.