# Innovative Remote user Authentication Protocol for Multi-Server Structural Design Based on ECC

**Ms. Shirkande M.R.**
Dnyanganga College of Engineering and Research,
Narhe, Pune
*madhurishirkande106@gmail.com*

***Abstract:*** We have achieved an era where preferred web services are accessible over the networks by click of a button. In such a situation, remote user authentication performs the most part in determining the genuine users of a web service on the World Wide Web. Scientists have suggested a number of security password centered authentication techniques which depend on single server for authentication. But, with remarkable improvements in technology, it is probable to interact with several web servers in authenticating their clients to experience greater protection. In this paper, we recommend an efficient security password centered authentication protocol for multiserver structure. The method provides common authentication using intelligent card and is depending on Elliptic Curve Cryptography, thus offers best protection at a low price. In 2011, Sood et al. suggested a multi-server structure protocol utilizing smart cards. In this papers, we enhance Sood et al. plan by improving its protection and decreasing the computation cost. The protocol is in accordance with the idea of powerful identification that uses a nonce centered system and has no time synchronization issue.

***Keywords:*** *Authentication, Elliptic Curve Cryptography Multi-server architecture, Smart card.*

*****

## 1. Introduction

Remote user authentication is the procedure of determining a genuine user of a specific web support on the Web. Due to their low price, performance and mobility, smart cards are widely applied in e-commerce applications for remote user authentication. Smart cards are a mess proof plastic card almost the size of an ATM cards with built in micro-processor and memory. The customer of the smart cards inserts his cards in a cards reader machine and goes into his qualifications such as identity and security password. Depending on this detail, the authentication server and the smart cards perform cryptographic functions to verify the customer of the web support. A number of security password centered verification techniques have been designed where only individual server is engaged in the verification procedure. The authentication details stored on only one server becomes highly vulnerable to various attacks such as flow of verifier, server spoofing and thieved verifier attack. These days, popular processing has become very popular where multiple web servers are engaged in authenticating their users. For that reason, multi-server authentication techniques are required to serve the requires of modern computing solutions. Over last few years, scientists have designed security password centered authentication techniques centered on multi-server structure Most of the suggested techniques are vulnerable to one or more security strikes and involve high calculations and interaction price. In this research papers, we recommend an authentication plan which is depending on two-server-architecture model. The authentication factors of the user are distributed among two web servers namely the management server and service provider server. The back-end management server is much less revealed to the clients and therefore is more protected from various protection attacks. The client directly conveys only with the service provider server which in turn conveys with the management server to verify the client of the web support.

Security passwords are the most typical and convenient way to verify the remote customer of a web application. But users tend to use easy and typical passwords for a amount of web applications. Such passwords turn into a delicate target for the online hackers which lead to bargain of the protection password based authentication plan. Such techniques flow out the limited information about the customer which again leads to bargain of the plan. On the other hand, in case of powerful identification techniques the identification of the user changes with every sign in and even if the enemy releases a replay attack by recording various interaction messages, he is not able to sign in as a genuine customer. In this document, we recommend a powerful identification centered multi-server structure protocol which is protected against various protection attacks.

Protection passwords are the most frequent and practical way to verify the remote user of a web application. But user usually utilizes simple and frequent passwords for a number of web programs. Such passwords become a delicate focus on for the online hackers which guide to bargain of the protection password centered authentication plan. Another point of vulnerability is the fixed identification of the client where the user may modify his security password but he cannot modify his identification. Such techniques flow out the limited information about the user which again leads to bargain of the plan. Alternatively, in case of powerful identification techniques the identification of the user changes with every sign in and even if the hackers release a replay attacks by documenting various interaction message, he is not able to sign in as a genuine user. In this paper, we propose a powerful identification centered multi-server architecture protocol which is protected beside different security attacks.

Cost and performance are a further two factors on which the durability of any authentication plan relies upon. Authentication techniques depending on public key cryptography are very complicated to consist of because of the natural durability of public key techniques, but these techniques are very expensive as the use of public key cryptography includes computation of rapid functions which needs a lot of processing time. Smart cards are tiny electronic cards with restricted sources and therefore public key cryptography does not create a perfect choice for them. Symmetrical cryptographic factors are inexpensive in terms of calculations price but they are easier to create as compared to public key cryptographic factors. In evaluation to other public key systems (PKS), Elliptic Curve Cryptosystem provides highest possible security per bit for a given key dimension (Borst et al., 2001). Smaller key dimension indicates faster computation even with restricted sources. Thus, ECC can very well be applied in smart credit cards without increasing its computational sources and consequently its size and price. Therefore, the most efficient way to apply security with smart cards is to use a burglar password centered authentication plan depending on ECC.

In this document, we recommend a protocol by enhancing the protocol suggested by Sood et al. (2011) which is centered on multi-server structure. We recommend a remote user password authenticated protocol depending on ECC for multi-server architecture. We have decreased the interaction and computation price significantly and also improved the security of the protocol. The significant advantages of our method are 1) Asymmetric cryptographic primitives offer highest possible security against brute force attacks as in evaluation to symmetric primitives. ECC is in accordance with the difficult issue of ECDLP (Elliptic Curve Discrete Logarithm Problem) and there is no polynomial time algorithm available to fix it. Therefore, the use of ECC (public key cryptography) significantly increases the protection of any authentication plan. Hence, our protocol depending on Elliptic Curve Cryptography provides common verification and session key contract at a low calculations price. 2) The communication price of our plan is significantly low as compared to the techniques depending on symmetrical primitives and other techniques in accordance with the public key cryptography. With a short interaction price and improved performance our protocol can very well be applied for smart cards which are constrained gadgets with restricted computational sources.

3) This protocol is a nonce centered method and the identification of the user modifications dynamically whenever when the user is authenticated by the server. The user's identification is forever secreted to the attacker in a vulnerable interaction way. This gives an additional stage of protection and stops many well known attacks possible otherwise. 4) It is depending on two server- architecture and therefore provides much greater security than protocols depending on individual server structure. 5) Our protocol provides multi-factor verification where the authority of a user is confirmed on several aspects. The protocol authenticates the user on the reasons for security password, smart card and two-server-architecture. Therefore, the protocol is extremely effective and cannot be made. 6) It accomplishes mutual authentication and session key contract. 7) It is a dynamic identity centered verification plan where the idea of dynamic identification is applied using a nonce centered system so there is little time synchronization issue. 8) The protocol is secure against all the well recognized attacks. 9) The security password can be selected easily by the user. 10) The security password modify phase of the protocol is much easier and effective in evaluation to all the other protocol.

## 2. RESEARCH REVIEW

Brainard J, Juel A, Kaliski B, Szydlo M. [1], Security passwords and PINs continue to stay the most extensive types of user authentication, despite growing attention of their security restrictions. This is because brief tricks are realistic, particularly for a more and more mobile user inhabitants. Many users are enthusiastic about utilizing a variety of computers with different types of connection and different software systems. Such users often find it realistic to verify by means of passwords and brief tricks, to restore missing passwords by responding to personal or "life" questions, and to create comparable use of relatively poor secrets. In common verification methods based on short secrets, the secrets (or related values) are saved in a main database. Often neglected is the weakness of the secrets to robbery en bloc in the event of server bargain. With this in mind, Ford and Kaminski and others have suggested a variety of security password "hardening" techniques including several web servers, with security password comfort confident given that some web servers stay uncompromised. In this paper, we explain a new, two-server secure roaming system that benefits from an especially light and portable new set of methods. Contrary to past concepts, ours can be applied so as to require basically no intense cryptographic calculations by user. This and other style features provide the system, in our view, the most realistic offer to date in this area. We explain in this document the protocol and execution difficulties and the style options actual the system.

In paper [2], since the number of server offering the features for the customer is usually more than one; the authentication protocols for multi-server environment are required for realistic programs. Most of security password verification techniques for multi-server atmosphere are depending on static ID, so the attacker can use this information to monitor and recognize the customer's demands. It is undesirable to be used to special programs, such as e-commerce. In this paper, we create a protected dynamic ID centered distant user authentication plan to accomplish customer's privacy. The proposed scheme only uses hashing features to apply a effective authentication plan for the multi-server atmosphere. It provides a protected method to update security password without the help of third reliable party. The suggested plan does not only fulfill all specifications for multi-server environment but also accomplish efficient calculations. Furthermore, our plan provides complete performance to match with the real applications.

In paper [3], in most password-authenticated key exchange techniques there is a individual server saving security password confirmation information. To present some strength against server bargain, this information will get the form of a one-way function of the security password (and possibly a salt, or other community values), rather than the security password on its own. Nevertheless, if the server is affected, this password verification information can be applied to execute an off-line vocabulary attacks on the user’s security password. In this papers we recommend an effective password-authenticated key return system including a set of web servers with known public keys factors, in which a certain threshold of web servers must get involved in the verification of a user, and in which the bargain of any less than that threshold of servers does not allow an enemy to execute an off-line vocabulary strike. We confirm our program is protected in the unique oracle design under the Decision Diffie-Hellman supposition against an attacker that may eavesdrop on, insert, remove, or change information between the user and web servers, and that adjustment less than that threshold of web servers.

In paper [4], Following advances in system technologies, many systems have been provided to help network users via the Web. In sequence to authenticate the remote users, password-based protection systems have been commonly applied. They are simply executed, but these systems must shop a confirmation desk in the server. If an attacker steals the confirmation desk from the server, the attacker may masquerade as a authorized user.

To solve the confirmation desk thieved issue, several individual server authentication techniques without confirmation tables have been suggested. These individual authentication techniques suffer from a limitation. If a remote user wishes to use several system services, they must register their identity and protection password in these web servers. In response to this issue, several related studies recently have been suggested. These authentication techniques enable remote user to obtain service from multiple web servers without separately registering with each server. This research proposes an alternative multi-server authentication plan using smart cards. The suggested plan is in accordance with the nonce, uses one-way hash function, and does not need to shop any confirmation desk in the server and registration facility. The suggested plan can withstand seven well known network protection attacks.

## 3. Proposed Methodology

In this section, we recommend an ECC based protocol for multi-server structure applying smart cards. The protocol is protected against all well known protection attacks. The user Ui records in to the server by placing his smarts cards in the cards reader machine by posting his IDi and protection password Pi. The method consists of 5 stages

### 3.1. Registration phase

In order to register with the control server CS, the customer Ui transmits his identification IDi via a protected interaction route. The CS determines the verification factors and stores them on the smart cards. The user triggers his smart cards by coming into his protection password and the protection factors are saved on the smart cards.

### *3.2.* Precomputation phase

Before the system starts the smart cards determines an ECC point and stores it in its memory for further interaction.

### 3.3. Sign in phase

The user Ui in order to login with the support agency server Sk inserts his smart cards into a cards reader machine and gives up his IDi, password Pi and the identity SIDk of support agency Sk. The validity of the user is verified by the smart cards which then deliver the confirmation and login information to the desired destination server Sk.

### 3. 4. Authentication and period key agreement phase

The confirmation information of user and server Sk is passed to the control server CS by the support provider server Sk. The server Sk and the control server CS mutually authenticate each other and the user Ui. Once authenticated, the user Ui, support provider server Sk and management server CS agree on a common session key for additional interaction.

### 3.5. Password change phase

The user can easily modify his password without the disturbance of the control server CS. Before the program starts, the control server CS chooses a large prime number p and two integer components a and b where p is of great purchase such that p > $2^{160}$ and a and b fulfill the formula ($4a^3$ + $27b^2$) mod p ≠ 0. Then the server chooses an elliptic curve formula Ep over the limited area

p : $y^2$ = ($x^3$ + ax + b) mod p. The server chooses a creator point G of order n, where n is a huge divisor such that n × G = O. The server also chooses X as its private key and posts (Ep, G, n, p).

## 4. Conclusion

Modern network technological innovation has prepared the use of e-commerce applications extremely. A lot of delicate information moves over the networks these days. In such a situation, user authentication becomes vital for cooperate networks to succeed. Security password centered authentication techniques using smart cards create a perfect choice for e-commerce programs over work networks as they provide multi-factor verification between the client and server.

Researchers have suggested various multi-server authentication protocols to eliminate the major factor of vulnerability of a single verification server. We have suggested an efficient multiple server authentication method using smart cards depending on Elliptic Curve Cryptography (ECC). The requirement of ECC offers all the advantage of utilizing an asymmetric cryptosystem even for a restricted environment of common smart cards. With a low computational and interaction cost it stops all well known attacks by the harmful users of the technique.

## References

[1] Brainard J, Juel A, Kaliski B, Szydlo M.A new two-server approach for authentication with short secrets. In: Proceeding of the USENIX security symposium August 2003. p. 201-14.

[2] Liao YP, Wang SS.A secure dynamic id-based remote user authentication scheme for multi-server environment. Computer Standard & Interface 2009; 31 (1):24-9.

[3] Mackenzie P, Shrimptom T, Jakobsson M. Threshold password authenticated key exchange. Journal of Cryptography 2006; 19(1):27-66.

[4] Tsai JL.Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers & Security 2008; 27 (3e4):115-21.

[5] Yang YJ, Bao F, Deng RH.A new architecture for authentication and key exchange using password for federated enterprises. In: Proceedings of 12th international federation for information proceeding information security conference (SEC ’05) March 2005. p. 95-112.

[6] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Proceedings CRYPTO 99 1999. p. 388-97.

[7] Borst J, Bart P, Rijmen V. Cryptography on smart cards. Elsevier. Journal of Computer Networks 2001; 36:423e35.

[8] Sood SK, Sarje AK, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Application 2011; 34:609-18.

## .AUTHOR

**Madhuri Ramchandra Shirkande** received the Bachelor’s degree (B.E) in Computer Science in 2012 BMIT Solapur,.She is now pursuing Master’s degree in Computer Engineering at ZES’s Dantanganga College of Engineering, Pune. Her current research interests include information security.