International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Incorporated Approach for Multiserver Inaccessible User Authentication

Madhuri R. Shirkande

Zeal College of Engineering and Research, Narhe, Pune-411041, India

Abstract: ***Multi server remote client verification assumes essential part in distinguishing the aggressors of web administrations. In existing methods we utilized single server for identify remote user & security. In Multiserver remote user authentication people obtain their services by using mobile devices. Which require minimum computation and communication energy. Important goal of system is enhance security using ECC (Eliptic curve cryptography), OTP (one time password), And ATM Matrix card validation. Which withstand with offline Dictionary attacks, MIME attacks, malicious server attacks. Praposed scheme enhance security with mutual authentication between servers with minimum computation and communication energy. Multi server strategy is utilized for confirmation & security. The one server is used to give administration to the client & other server is utilized for enrolling the clients as a part of multi client server procedure. On the off chance that client has enrolled to the registration server than just he/she can get to the administration server. User can login in on administration client in the wake of getting the user ID, secret key in their database. With most reduced sum count overhead & littler keys ecliptic bend cryptography gives better security. So design such type of protocol which reduces the cost and computatation speed with enhanced security is main goal of system.***

Keywords: Multiserver, Authentication, ECC, OTP, Matrix Validation

1. Introduction

In ubiquitous computing multiserver remote user authentication plays important role in finding authorised user on web application. multiple server are involving to authenticate remote user. This security must be secure with possible attack. In this system we used OTP and ATM Matrix card validation Technique with ECC Asymmetric key algorithms purpose is to enhance security and minimise the Computation and communication energy.ECC based on ECDLP problems which cannot break in given polynomial time. In logically keen cards are utilized for remote client validation on web. It's truly a mind boggling assignment to recognize the remote client in e-trade. Distinguishing the remote client is truly an unpredictable undertaking in e-business application .The classified data is needed for confirmation, for example, personality & client secret key by entering his brilliant card in card reader. The assaults like hole of verifier, server caricaturing stolen verifier assault ought to be more secure by administration supplier server. Client regularly picks simple secret key as it is most normal system for verification

So they recollect that it. Another weakness client's personality of anticipating assailants effectively which recognizes the secret key so that client need to change their confirmation in every login. Regarding the cost & fitness of the framework is another component on which make of check framework depends. In any case, it is extreme & complex to gauge additionally hard to calculate, lot of handling time is required. With littler key size with per bit the most extreme assurance is given by the circular bend cryptography .This framework diminishes the correspondence value & amplifies the security & insurance Benefits of this convention are:-

1) Asymmetric key primitives give greatest security contrary to the numerous attacks.
2) There is no polynomial time calculation accessible to illuminate ECC which is relied on hard issue of ECDLP (Elliptic Curve Discrete Logarithm Problem) and the utilization of ECC (open key cryptography) build the insurance of check. Plan. Thus, this framework is rely on upon Elliptic Curve Cryptography which gives shared confirmation and most minimal sum estimation overhead. The correspondence cost is sensibly close to the ground in light of deviated key cryptography. Framework actualized extremely well for the savvy cards due to less declaration cost and more adequacies.
3) Two server architectures give more security than single server structural planning.
4) Multifactor approval is principle objective of development in that muscle client is affirmed by different components.
5) It accomplishes normal affirmation and gathering key understanding.
6) It accomplishes security contrary to all understood assaults.
7) Password can pick liberally by client.
8) The secret word change stage is much less demanding and able in assessment to the various conventions.

2. Related Work

1) ManikLalDas, VedP.Gulati: Planned organism dynamic identity based Remote: through this system we allow user to change the password freely.ID verifier tale is not maintained. This mechanism protects the ID thief also resists reply attack, guessing attacks stolen verifier.

2) Liao YP, Wang SS. [4] protected active unique based verification rules for the multi server structure. It keeps their stationary uniqueness variant in connection in channel. It includes two servers for registering & password verification.
3) Two server based authentication password scheme is used to verify user. The service which is front end is

controlled by service provider & back end is control by enter prise head quarter each

4) Tsai JL. [6] An competence multi server password verified solution using smart card: Itmaintains the encrypted solution table to decrease load of each registered server. User& server shared private key while it is based on hash faction.
5) Lee WB, Chang CC. [9] User authentication Scheme with privacy preservation for Multiserver Environment.
6) Chang CC, Lee JS. [1] Competence multi server password verification agreement key using smart cards: in suggestion multi user authentication rules using cards which were based on symmetric formula.
7) M.L.Das, A.Saxena, V.P.Gulati,[15] A Dynamic ID based Remote User Authentication Scheme used to choose and change their password freely. It uses input data like ID based authentication scheme and Hash function for the enhancing security. Not require to maintain ID verifier. But drawback is only that Multiserver system but affected by reply and password guessing attack.
8) Dynamic identity based authentication protocol for smartcards based on multi-server used to two server based password authentication scheme. Also use backend control server is controlled by an enterprise head quarter and a frontend external server is operated by each affiliating organization.

1) Implementation Details

Phase I:- Registration phase-To access the service server user need to register it on registrationserver. The user UI submits his identity ID through a secure communication channel. The control server estimates the verification parameters and Store in memory. From users credentials system calculate ATM Matrix card validation and store for further authentication .

Phase 2:- Pre estimation phase in pre calculation stage to access the system smart card calculates ECC points for further connection.

Phase 3: Login phase user enters his users ID, password. after login service provider server calculate ATM matrix card and match with Control servers ATM Matrix card. After Matching Service Server Send OTP to users mobile no.user submit OTP and sends login message to Control server to authenticate & verify the user.

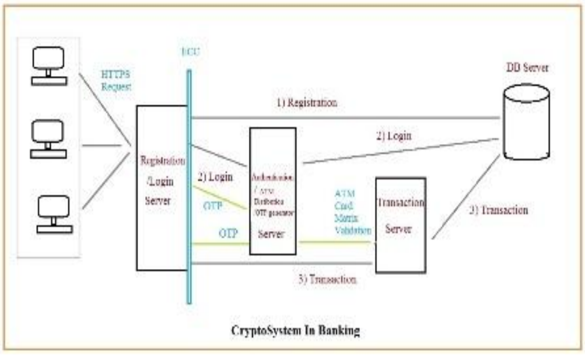
Phase 4: OTP production phase after successful completion of login OTP originators OTP by genetic algorithm & sends it to user for verification.

Phase V:-ATM Matrix Validate-After using OTP verification of user will be done. We create matrix which store users credentional at the time of registration that matrix verify after completion of OTP phase.

Phase 5: ATM matrix validate after using OTP verification of user will be done.We create matrix which stores

Phase 6: Verification &assembly key agreement phase verification message is send to control server to authentication. Control server manually checks service provider & user control server agree for session.

Phase VII:-Password change phase:-Before scheme begins, the direct server selects a large prime number p and two integer elements a and b where p is of high order Then the server selects an elliptic curve equation Ep over the finite field p. And then change password generate newly. OTP: One time password technique A one-time password (OTP) is a password that is valid for only one login session or operation. OTPs avoid a number of restrictions that are associated with Static Password based authentication; a number of implementations also incorporate two factor authentications by ensuring that the one-time password requires access to something a person has well as something a person knows. The most important short coming that is addressed by OTPs is that, in contrast to static passwords, they are not susceptible to replay attacks. This shows a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A Second major benefit is that a user, who uses the same password for multiple systems, is not made Vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reduce the attack.



Cryptosystem in banking

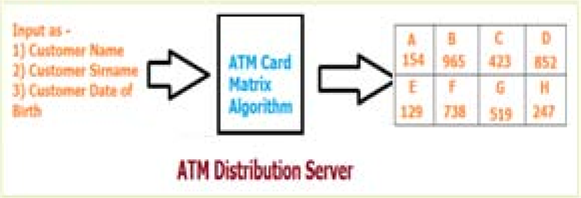
3. Algorithm Used In Proposed System

A. OTP Algoritham
INPUT:ID and Password of User
OUTPUT:Generate OTP from 8 random Password.
Step 1.Using genetic operators we create random 8 alphabets from that two alphabets and suppose it is Random key.
Step 2.We have to select 8 alphabets from encrypted output assume it as ID.
Step 3.We have two keys of 8 alphabets. One is Random key and second is Identification ID.
Step 4.Divide Identification ID and Random password into two Parts of 4 alphabets.i.e.pswdL = X1X2X3X4 pswdR = X5X6X7X8,IDL = Y1Y2Y3Y4,IDR =Y5Y6Y7Y8.
Step 5.Take random point from elliptic curve which satisfyequation of elliptic curve and convert it into binary form of8bits.
Step 6.Calculate Values KL = pswdL (OR operation) IDL KR= pswdR (OR operation)IDR Else if b[i]==1 perform KL =pswdL (OR operation) IDL KR = pswdR (OR operation)

F(IDR) Where F (IDR) = Product between the IDR and Anyrandom point in elliptic curve cryptography.
Step 7.Merge KL AND KR is equal to K.
Step 8.Merge F (IDR) and IDL = ID.
Step 9.Find the product of ID with any private key.
Steps 10.We have now 8 Random passwords which we arestore in database and newly generated identification.
Step 11.Next time when user login then that IdentificationNo. (ID) is given to OTP generator for generating password.
Matrix card validate algorithm.

B. Algorithm for ATM card Matrix creation
A = (ASCII Value of First Names 1st letter + ASCIIValue of First Names Last letter) * 2
B = (ASCII Value of First Names 2nd Letter + ASCII Valueof First Names last letter) * 2
C = (ASCII Value of First Names last letters + ASCII Valueof First Names last letter) * 2
D = (ASCII Value of Last Names 1st letter + ASCII Value ofLast Names last letter) * 2
E = (ASCII Value of Last Names 2nd letter + ASCII Valueof Last Names last letter) * 2
F = (ASCII Value of Last Names last letters + ASCII Valueof Last Names last letter) * 2
G = (ASCII Value of Day of Birth's 1st digit + ASCII Valueof Day of Birth's 2nd digit) * 2
H = (ASCII Value of Year of Birth's 3rd digit + ASCII Valueof Year of Birth's 4th digit) * 2
C] Example Customer Details are - First Name = "Madhuri";Last Name = "Shirkande";
DateOfBirth= "06-05-1989";
A = (77 + 105) * 2 = 364
B = (97 + 105) * 2 = 404
C = (105 + 105) * 2 = 420
D = (83 + 101) * 2 = 368
E = (104 + 101) * 2 = 410
F = (101 + 101) * 2 = 404
G = (48 + 54) * 2 = 204
H = (56 + 57) * 2 = 226
C. Output of ATM Card Matrix card validator
Fig. 2. Output of ATM card Matrix Validation

D. Mathematical



A	B	C	D
154	965	423	852
E	F	G	H
129	738	519	247

Figure 2: Output of ATM card Matrix Validation

D. Mathematical Model

Service provider Send sid to Control Server then verification of control server and Service provider
User Sends P1,P11 and Nonce(N1) Send To the Service Provider and Service Provider Calculate Ei,P2,P22,And Nonce(N2)
And Sends to Control Server gets The P1,P2,P11,P22 and UserId and Control Server Calculate the P3 And P33 And Compare the P'11,P'22 The P11,P22 & P'11,P'22 are equal then calculate The Di and Sends to the Service Provider

Service Provider Compare the Di & Di' Are equal Then Compute the Ti and Send the User And user Calculate the Ti' And Compare with the Ti & Ti' Are equal then user login is successfully

4. Result

Regarding the cost and efficiency of system is another factor on which strength of authentication system depends. We use public key cryptography for authentication .but it is expensive and difficult to calculation also hard to computation. System should be more Secure from varies attacks like leak of verifier, server spoofing and stolen verifier attack. Mostly password is most common way to authenticate user but normally users choose Their password easy to remember password so password predicting attacker easily identify. The password. System prevents man in middle attack, brute force attacks, impersession Attacks, Denial of service. Using ECC minimizes the computation and communication overhead .also OTP resists the stolen card attacks. OTP gives the ensures the authorized user attacks, Denial of service. Using ECC minimizes the computation and communication overhead. AlsoOTP resist the stolen card attacks.OTP gives the ensures the authorised user.

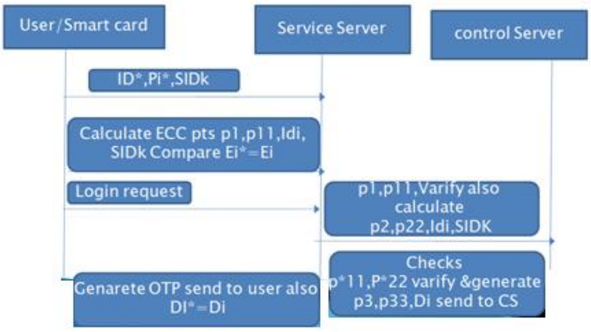

User/Smart card
Service Server
control Server
ID*,Pi*,SIDk
Calculate ECC pts p1,p11,Idi, SIDk Compare Ei*=Ei
Login request
p1,p11,Varify also calculate p2,p22,Idi,SIDK
Checks p*11,P*22 varify &generate p3,p33,Di send to CS
Genarete OTP send to user also DI*=Di

Figure 4: Mathematical Model Diagram

5. Conclusion

In ecommerce application advanced innovation is equipped so client validation is more imperative for security of server and client .remote client confirmation is discriminating pickle in ecommerce application. This paper gives multifaceted validation to security and confirmation. This paper proposed a productive multi server validation convention utilizing keen cards in light of Elliptic Curve Cryptography ECC give Public key cryptosystem which give most extreme security utilizing cell phones like savvy cards. Multi-server remote client check utilizing ECC minimizes the reckoning and correspondence cost which keeps the framework from assorted types of attack. .So benefit supplier server ought to be more secure from shifts assaults like hole of verifier, server parodying and stolen verifier assault. Mostly password is most common way to authenticate user but normally users choose their password easy to remember password so password predicting attacker easily identify the password. Another weak point of vulnerability is users identity user must have changed their identity in every login. Also it requires a lot of processing time. So elliptic curve cryptography provide maximum security.

6. Acknowledgment

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1] Chang CC, Lee JS. An efficient and secure multi-server password authentication scheme using smart cards. In: Proceedings of the international Conference on cyber worlds November 2004.

[2] Das ML,Saxena A, Gulati VP. A dynamic id-based remote user Authentication scheme. IEEE Transactions on Consumer Electronics 2004; 50(2):629e31.

[3] Juang WS. Efficient multi-server password authenticated key agreement Using smart cards. IEEE Transactions on Consumer Electronics 2004; 50(1):251e5.

[4] Wang RC,Juang WQ, Lei CL. Robust authentication and key agreement Scheme preserving the privacy of secret key. Computer Communications 2011;34:274e80.

[5] BrainardJ,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. 2014.

[6] JuangWS,Chen ST, Liaw HT. Robust and efficient password authenticated Key agreement using smart cards.

[7] Lee WB, Chang CC. User identification and key distribution maintaining Anonymity for distributed computer networks. Computer System Science 2000;15(4):211e4.

[8] 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 34 (2) (2011) 609618.

[9] C.C. Lee, T.H. Lin, R.X. Chang, A secure dynamic ID based remote user Authentication scheme for multiserver environment using smart cards, Expert Systems with Applications 38 (2011) 1386313870.Department Of Information Technology 25.

[10] C.C. Lee, T.H. Lin, R.X. Chang, A secure dynamic ID based remote User authentication scheme for multiserver environment using smart Cards, Expert Systems with Applications 38 (2011) 1386313870.Department Of Information Technology 25.

[11] W. Ku, S. Chen, Weaknesses and improvements of an efficient password Based remote user au- thantication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (1) (2004) 204207.

[12] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user Authentication scheme, IEEE Transactionson Consumer Electronics 50 (2) (2004) 629631.