International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Efficient ID-Based Password Authenticated Key Exchange Using Multiple Server

Gopiga. P[1], Hemalatha. A[2] J. Haripriya[3], Muthukumarasamy.S[4]
[1, 2, 3] *U.G. Student Computer Science and Engineering, S.A. Engineering College, Chennai*
[4] *Assistant Professor, Computer Science and Engineering, S. A. Engineering College, Chennai*

Abstract: ***Password Authenticated Key Agreement is a relational method for two or more entities to establish cryptographic key exchange based on one or more entity's ability of the password. PAKE protocol that are designed to be safe even session key based on shared human memorable password. The main objective of these protocols is security against password dictionary attacks. A exact answer of this protocol involves segmenting the password between the multiple servers. If a single server is accord by an attacker, the password is required to remain secure. If a two servers are accord by an attacker, the secure password is not obtained. To avoid this problem, It introduce identity based multiple server password authentication key exchange protocol. By the authority, It can generate id based multiple server PAKE protocols which achieve fixed authentication. As far as the elemental two-party PAKE protocol and identity based signature scheme have confirmable security without arbitrary oracles.***

Keywords: Password-authenticated key exchange, identity based signature, Diffiee -Hellman key exchange, dictionary attacks.

I. INTRODUCTION

In today's technology, security is one of the main challenges in the networking field. Passwords are the first line of protection against cyber scandalous. Passwords are frequently accessed by user during a login process that force access to guaranteed computer operating system, mobile phones, tablet, cable TV adapter, ATM(automated teller machine),applications and so on. In two server authentication PAKE protocol if one server is compromised by an attacker, the password of the user is required to remain secure. But if two servers are accord by an attacker the password is not secure. To solve this problem, to establish ID based multi-server password authentication key exchange protocol. In this system, present two compiler that transform any two party PAKE protocol to a multi-server PAKE protocol on the basis of identity based cryptography, called ID based multi-server PAKE protocol. In this protocol, to achieve implicit authentication by the user. ID based PAKE protocol can be thought as exchange of between watchword just and PKI-based PAKE. In the single server setting every one of the password is essential to confirm customer are put away in a solitary server. In multi-server PAKE protocol, many server are present so the password will be more secure than the two server PAKE protocol. For example, In multi- server PAKE protocol ,the password is segmented for a various server to protect secure communication between the users. In Diffie-Hellman key[1], the principal viable technique for two clients to set up a common mystery key over an unprotected correspondences channel. Despite the fact that it is a non-authenticated key trade convention, it gives the reason for an assortment of verified conventions. Diffie-Hellman key trade convention was taken after in the blink of an eye a while later by RSA , the primary useful open key cryptosystem. Alice and Bob agree on a cyclic group GG of large Clearly k1 ¼ k2 and therefore Alice and Bob have conceded to a similar mystery key, by which the consequent interchanges between them can be ensured. Diffie-Hellman key trade convention is secure against any detached enemy, who can't associate with Alice and Weave, endeavoring to decide the mystery key exclusively based upon watched information .Diffie-Hellman key understanding did not depend on encryption and decoding, yet rather depends on numerical capacities that empower two gatherings to produce a mutual mystery key for trading data privately on the web. Basically, each gathering concurs on an open esteem g and a vast prime number p . Next, one gathering picks a mystery esteem x and the other party picks a mystery esteem y . The two gatherings utilize their mystery esteems to infer open esteems, g x mod p and g y mod p, and they trade the general population esteems. Each gathering at that point utilizes the other party's open an incentive to compute the mutual mystery key that is utilized by the two gatherings for private interchanges. An outsider can't determine the mutual mystery key since they don't know both of the mystery esteems, x or y .

For instance, Alice picks mystery esteem x and sends the general population esteem g x mod p to Bob. Sway picks mystery esteem y and sends people in general esteem g y mod p to Alice. Alice utilizes the esteem g xy mod p as her mystery key for classified correspondences with Bob. Bounce utilizes the esteem g yx mod p as his mystery key. Since g xy mod p parallels g yx mod p , Alice

and Bob can utilize their mystery keys with a symmetric key calculation to lead classified online correspondences. The utilization of the modulo work guarantees that the two gatherings can figure a similar mystery key esteem, yet a meddler can't. A spy can catch the estimations of g and p , but since of the to a great degree troublesome numerical issue made by the utilization of a substantial prime number in mod p, the spy can't practically compute either mystery esteem x or mystery esteem y . The mystery key is known just to each gathering and is never obvious on the system. Its requirement for haphazardness, and its slower speed(especially to sign). The potential inconvenience of the ElGamal framework is that message extension by a factor of two happens amid encryption(implies the ciphertext is twice the length of the plaintext.). The proposed the different PAKE convention a two kinds of servers are likewise clarified that are symmetric and deviated. Diffie-Hellman and Elagamal encryption calculations are fundamental building squares of the clarified convention. Here it is vital to consider that in the event that one server shutdown due to some reason at that point there is office to the servers to take intermittent reinforcement. By utilizing intermittent reinforcement procedure the repetition in the information a be stayed away from. Security recommend that it is critical an productive convention. Mostly this convention utilizes people in general key encryption so that correspondence is done through secure channel as opposed to broadcasting from customer to the servers. After security investigation it is come to realize that this convention secure against dynamic and uninvolved assault. In cryptography, the ElGamal encryption framework is an unbalanced key encryption calculation for open key cryptography which depends on the Diffie– Hellman key trade. The framework gives an extra layer of security by lopsidedly encoding keys already utilized for symmetric message encryption. It was portrayed by Taher Elgamal. ElGamal encryption is utilized as a part of the free GNU Privacy Guard programming, late forms of PGP, and different cryptosystems. The Digital Signature Algorithm (DSA) is a variation of the ElGamal signature conspire, which ought not be mistaken for ElGamal encryption. Generally, secure encoded correspondence between two gatherings required that they first trade keys by some protected physical channel, for example, paper key records transported by a put stock in dispatch. The Diffie– Hellman key trade technique permits two gatherings that have no earlier information of each other to together build up a common mystery key over a shaky channel. This key would then be able to be utilized to encode ensuing interchanges utilizing a symmetric key . The focal points incorporate a RSA calculation is sheltered and secure for its clients using complex arithmetic. RSA calculation is difficult to split since it includes factorization of prime numbers which are hard to factorize. In addition, RSA calculation utilizes people in general key to encode information and the key is known to everybody, in this way, it is anything but difficult to share the general population key. The drawbacks incorporate; RSA calculation can be moderate in situations where vast information should be encoded by a similar PC. It requires an outsider to confirm the unwavering quality of open keys. Information exchanged through RSA calculation could be bargained through go between who may temper with people in general key framework. Taking everything into account, both the symmetric encryption system and the unbalanced encryption method are essential in encryption of delicate information.

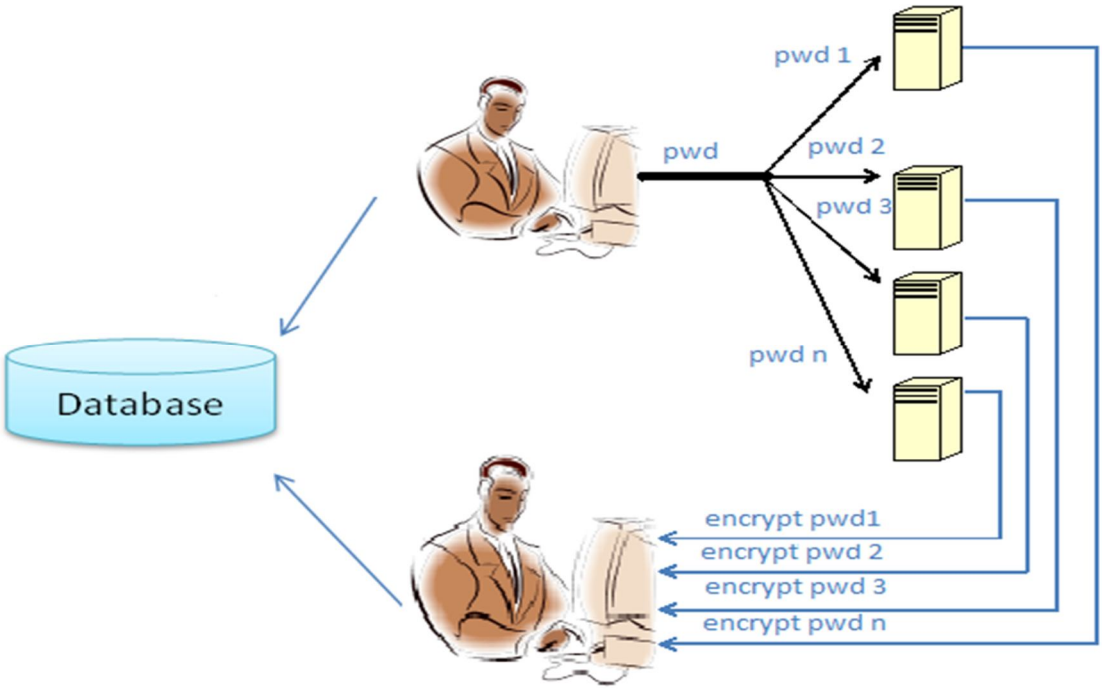

Fig: Multi-server Password Authentication Key Exchange

II. LITERATURE SURVEY

Albert Y. Zomaya[1] designed a model two-server secret word verified key trade (PAKE) convention, a customer parts its watchword and stores two offers of its secret key in the two servers, separately, and the two servers at that point coordinate to verify the customer without knowing the secret word of the customer. On the off chance that one server is traded off by a foe, the watchword of the customer is required to stay secure. In this paper, It introduce two compilers that change any two-party PAKE convention to a two-server PAKE convention based on the character based cryptography, called ID2S PAKE convention. By the compilers, It can develop ID2S PAKE conventions which accomplish certain validation. For whatever length of time that the fundamental two-party PAKE convention and character based encryption or mark conspire have provable security without arbitrary prophets, the ID2S PAKE conventions developed by the compilers can be turned out to be secure without arbitrary prophets.
Huaxiong Wang[2] developed a Secret key confirmed key trade (PAKE) is the place a customer and a server, who share a watchword, validate each other and in the interim build up a cryptographic key by trade of messages. In this setting, every one of the passwords important to validate customers are put away in a solitary server. On the off chance that the server is traded off, due to, for instance, hacking or considerably insider assault, passwords put away in the server are altogether uncovered. Current answers for two-server PAKE are either symmetric as in two associate servers similarly add to the confirmation or awry as in one server validates the customer with the assistance of another server. This paper presents a symmetric answer for two-server PAKE, where the customer can set up various cryptographic keys with the two servers, separately. Our convention keeps running in parallel and is more productive than existing symmetric two-server PAKE convention, and much more proficient than existing hilter kilter two-server PAKE conventions as far as parallel calculation.
Zhenfeng Zhang[3] developed a two-server watchword validated key trade enables the customer to part a low-entropy watchword into two pieces what's more, store them in two servers, individually, and two servers to cooperatively verify the customer and set up session keys with him. Despite the fact that both of servers has been adulterated, it ensures that the watchword still stays secure Additionally, it is asserted that the plan is provably secure in an important formal model. In this letter, It call attention to a current related-key assault to their plan with the goal that when one server is ruined, the foe can unpretentiously infer the crisp key shared by the staying two genuine gatherings. Also, It propose a straightforward fix to evade this worry.
David P. Jablon[4] designed a Safe long haul stockpiling of client private keys is an issue in customer/server frameworks. The issue can be tended to with a wandering framework that recovers keys on request from remote certification servers, utilizing secret key validation conventions that forestall watchword speculating assaults from the system. Their techniques utilize a formerly validated channel which requires customer put away keys and authentications, and might be helpless against disconnected speculating in server parodying assaults when individuals must decidedly distinguish servers, however don't. It exhibit a multi-server wandering convention in a less difficult model without this requirement for an earlier secure channel. This framework requires less security presumptions, enhances execution with equivalent cryptographic suspicions, and better handles human mistakes in secret key section.
Kenneth G. Paterson[5] developed a To decrease the harm of phishing and spyware assaults, banks, governments, and other security-touchy businesses are sending one- time secret word frameworks, where clients have numerous passwords and utilize each secret word just once. In the event that a solitary secret word is traded off, it can be just be used to mimic the client once, restricting the harm caused. Be that as it may, existing down to earth ways to deal with one-time passwords have been powerless to modern phishing assaults. The utilization of one-time passwords in the unique situation of secret key confirmed key trade (PAKE), which takes into account common validation, session key assertion, and protection from phishing assaults. It depict a security display for the utilization of one-time passwords, unequivocally considering the bargain of past (and future) one-time passwords, and demonstrate a general procedure for building a secure one-time-PAKE convention from any safe PAKE convention.
Elisa Bertino[6] developed a In two-server secret word verified key trade (PAKE) convention, a customer parts its secret word and stores two offers of its watchword in the two servers, individually, and the two servers at that point collaborate to authenticate the customer without knowing the secret key of the customer. In the event that one server is traded off by an enemy, the secret key of the customer is required to stay secure. In this paper, It display a compiler that changes any two-party PAKE convention to a two-server PAKE protocol. This compiler is essentially based on two-party PAKE and character based encryption (IBE), where the personalities of the two servers are utilized as their open keys. By our compiler, It can develop a two-server PAKE protocol which accomplishes certain confirmation with just two correspondences between the customer and the servers.
Michael Szydlo[7] developed a Customary watchword based validation and key-exchange conventions experience the ill effects of the basic actuality that a solitary server stores the delicate client watchword. By and by, when such a server is traded off, an expansive number of client passwords, (for the most part secret key hashes) are uncovered on the double. A characteristic

arrangement includes part secret key between two or more servers. This work formally models the fundamental security prerequisite for two-server secret key confirmation conventions, and in this structure gives solid security confirmations to two conventions. For this convention, It give a solid lessening to the computational Diffie-Hellman issue in the irregular prophet demonstrate. Next It introduce a second convention, in light of the same difficult issue, however which is easier, what's more, has a less demanding, more tightly diminishment verification.

Philip MacKenzie[8] designed a In most secret key confirmed key trade frameworks there is a solitary server putting away watchword confirmation information. To give some flexibility against server trade off, this information normally appears as a restricted capacity of the watchword instead of the watchword itself. Be that as it may, if the server is traded off, this watchword check information can be utilized to play out an disconnected lexicon assault on the client's watchword. In this paper It propose a productive secret word confirmed key trade framework including an arrangement of servers with known open keys, in which a specific limit of servers must take an interest in the confirmation of a client, and in which the bargain of any less than that edge of servers does not enable an aggressor to play out a disconnected word reference assault. It demonstrate our framework is secure in the irregular prophet show under the Decision Diffie– Hellman presumption against an assailant that may listen in on, embed, erase, or change messages between the client and servers, and that bargains less than that edge of servers.

Ruijie Zhang[9] developed a Two-factor confirmed key trade (TFAKE) conventions are broadly utilized as a part of remote sensor systems (WSNs) to give client validation what's more, information classification. Be that as it may, numerous current TFAKE conventions are found to be unreliable against various assaults. In this paper, It examine how to configuration provably secure TFAKE conventions utilizing awry cryptology components. Our primary strategy device is strong verified encryption plans and fluffy verifiers. It first present a formal security demonstrate for TFAKE convention in WSNs and after that propose a novel TFAKE convention in view of confirmed encryption plans. It demonstrates the security of the proposed convention in the arbitrary prophet show. The execution examination result appears that our convention appreciates provable security as well as has high productivity.

Chien-Ming Chen[10] in this paper ,Confirmed Key Exchange (AKE) is an essential cryptographic instrument to build up a secret channel between at least two substances over an open system. Different AKE conventions use shrewd cards to store delicate substance which are ordinarily utilized for verification or session key age. It expected that shrewd cards accompany an alter safe property, however touchy substance put away in it can even now be extricated by side channel assaults. It implies that if a foe takes some ones keen card, he may have opportunity to mimic this casualty or further dispatch another assaults. This sort of assault is called Stolen Smart Card Assault. In this paper, It propose a three-party secret key verification key trade convention. Our outline is secure against the stolen brilliant card assault. It additionally gives a security investigation to demonstrate our convention is still secure if touchy data which is put away in a keen card is removed by an aggressor.

Phillip H. Griffin[11] this paper depicts biometric-based cryptographic strategies that utilize powerless privileged insights to give solid, multi-factor and shared validation, and set up secure channels for consequent interchanges. These methods depend on lightweight cryptographic calculations for classified data trade. Lightweight calculations are reasonable for use in asset obliged situations for example, the Internet of Things where usage require effective execution, constrained access to memory and little code measure. Secret word Authenticated Key Trade, and Biometric Authenticated Key Exchange conventions in light of client information extricated from biometric sensor information, both depend on feeble mysteries. These insider facts are shared between a customer and an entrance controlled server, and utilized as contributions to Diffie-Hellman key foundation plans. Diffie-Hellman gives forward mystery, keeps client accreditations from being uncovered amid character confirmation endeavors, and ruins man-in-the-center and phishing assaults.

Marten van Dijk[12] this paper depicts a system that adventures the statistical defer varieties of wires and transistors crosswise over ICs to fabricate a mystery key one of a kind to every IC. To investigate its practicality, It manufactured a hopeful circuit to produce a reaction in view of its defer qualities. It demonstrate that there exists enough postpone variety crosswise over ICs executing the proposed circuit to recognize singular ICs. Hide there, the circuit capacities dependably finished a down to earth scope of ecological variety, for example, temperature and voltage.

Hung-Min Sun[13] In view of the discrete logarithm issue, proposed a remote client validation conspire utilizing savvy cards. In this paper, It further propose a productive and reasonable remote client validation conspire utilizing keen cards. The proposed conspire not just gives an indistinguishable favorable circumstances from that of Hwang and Li's plan, yet in addition essentially lessens the correspondence and calculation costs.

Jonathan Katz[14] developed a normal conventions for secret word based validation accept a solitary server which stores all the data (e.g., the watchword) necessary to confirm a client. Sadly, an innate impediment of this approach (expecting low-entropy passwords are utilized) is that the client's watchword is uncovered if this server is ever traded off. To address this issue, various plans have been proposed in which a client's pass- word data is shared among various servers, and these servers coordinate in an edge way when the client needs to confirm. Our own is the main provably-secure two-server convention for the essential secret key just setting (in which the client require recall just a watchword, furthermore, not the servers' open keys), and is the initial two-server convention (in any setting) with a proof of security in the standard model.

Tsu-Yang Wu[15] designed a the personality (ID)- based open key framework utilizing bilinear pairings characterized on elliptic bends offers a adaptable way to deal with improve the declaration administration. This panel has characterized the ID-based open key framework with bilinear pairings as one of open key cryptography principles. In this, a validated key assertion (AKE) convention is one imperative issue that gives common verification and key trade between two gatherings. Attributable to the quick development of versatile systems, the computational cost on the customer favor low-control processing gadgets is a basic factor in outlining an AKA convention suited for versatile systems. In this paper, it show a proficient and secure ID-based common confirmation and key trade convention utilizing bilinear pairings. In examination with the as of late proposed ID-based conventions, our convention has the best execution on the customer side.

III. CONCLUSION

In this paper, the proposed system it fragment the passwords and sent to the multiple servers. Each server encrypts the received fragmented passwords and client will combine the encrypted password and sent to the source client. In addition it affords a meticulous proof of security for our compilers without random oracle. So, ID based multi-server PAKE protocol is more secured than two server AKE protocol.

REFERENCES

[1] Xun Yi, Fang-Yu Rao, Zahir Tari, Feng Hao, Elisa Bertino, Fellow, Ibrahim Khalil, and Albert Y. Zomaya, Fellow, “ID2S Password-Authenticated Key Exchange Protocols”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 12, DECEMBER 2016, DOI : 10.1109/TC.2016.2553031

[2] Xun Yi, San Ling, and Huaxiong Wang,” Efficient Two-Server Password-Only Authenticated Key Exchange”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013,DOI: 10.1109/TPDS.2012.282. 1045-9219

[3] Lin Zhang and Zhenfeng Zhang,” Security analysis of an ID-Based Two-Server Password-Authenticated Key Exchange”, 1089-7798 (c) 2016 IEEE Personal use is permitted, but republication/redistribution requires IEEE permission, DOI 10.1109/LCOMM.2016.259478

[4] David P. Jablon,” Password Authentication Using Multiple Servers”, D. Naccache (Ed.): CT-RSA 2001, LNCS 2020, pp. 344–360, 2001. ©Springer-Verlag Berlin Heidelberg 200

[5] Kenneth G. Paterson and Douglas Stebila,” One-Time-Password-Authenticated Key Exchange”, R. Steinfeld and P. Hawkes ©ACISP 2010, LNCS 6168, pp. 264–281, 2010. ©Springer-Verlag Berlin Heidelberg 201

[6] Xun Yi, Feng Hao, and Elisa Bertino,” ID-Based Two-Server Password-Authenticated Key Exchange “, M. Kutylowski and J. Vaidya ©ESORICS 2014, Part II, LNCS 8713, pp. 257–276, 2014. ©Springer International Publishing Switzerland 2014

[7] Michael Szydlo and Burton Kaliski,” Proofs for Two-Server Password Authentication”, A.J. Menezes (Ed.): CT-RSA 2005, LNCS 3376, pp. 227–244, 2005. © Springer-Verlag Berlin Heidelberg 2005

[8] P. MacKenzie, T. Shrimpton, and M. Jakobsson,” Threshold Password-Authenticated Key Exchange”, Communicated by Mihir Bellare Received 3 December 2002 and revised 4 January 2005 Online publication 2 August 2005, DOI: 10.1007/s00145-005-0232-

[9] Fushan Wei , Ruijie Zhang , Jian Shen,” A Provably Secure Two-Factor Authenticated Key Exchange Protocol for Wireless Sensor Networks Based on Authenticated Encryption”, © Springer International Publishing AG 2017 L. Barolli et al. (eds.), Advances on Broad-Band Wireless Computing, Communication and Applications, Lecture Notes on Data Engineering and Communications Technologies 2, DOI 10.1007/978-3-319-49106-6_8

[10] Chien-Ming Chen, Linlin Xu, Weicheng Fang, and Tsu-Yang Wu,” A Three-Party Password Authenticated Key Exchange Protocol Resistant to Stolen Smart Card Attacks”, © Springer International Publishing AG 2017 J.-S. Pan et al. (eds.), Advances in Intelligent Information Hiding and Multimedia Signal Processing, Smart Innovation, Systems and Technologies 63, DOI 10.1007/978-3-319-50209-0_40

[11] Phillip H. Griffin,” Adaptive Weak Secrets for Authenticated Key Exchange”, © Springer International Publishing AG 2018 D. Nicholson (ed.), Advances in Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing 593, DOI 10.1007/978-3-319-60585-2_

[12] Jae W. Lee, Daihyun Lim, Blaise Gassend, G. Edward Suh, Marten van Dijk, and Srinivas Devadas,” A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications”, Computation Structures Group Memo 472,The Stata Center, 32 Vassar Street, Cambridge, Massachusetts 02139,200

[13] Hung-Min Sun,” AN EFFICIENT REMOTE USE AUTHENTICATION SCHEME USING SMART CARDS”, IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, NOVEMBER 2000 may 18. 2000 0098 3063/00 $10.00 2000

[14] Jonathan Katz, Philip MacKenzie, Gelareh Taban, and Virgil Gligor,” Two-Server Password-Only Authenticated Key Exchange”, Supported by NSF CAREER award 0447075 and Trusted Computing grant 0310751. J. Ioannidis, A. Keromytis, and M.Yung (Eds.): ACNS 2005, LNCS 3531, pp. 1–16, 2005. c Springer-Verlag Berlin Heidelberg 200

[15] Tsu-Yang Wu and Yuh-Min Tseng,” An ID-Based Mutual Authentication and Key Exchange Protocol for Low-Power Mobile Devices”, © The Author 2009. Published by Oxford University Press on behalf of The British Computer Society access publication on September 6, 2009 DOI:10.1093/comjnl/bxp083