International Journal of Engineering & Technology, 7 (3.34) (2018) 192-197

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enhanced Mutual Authentication System in Mobile Cloud Environments

[1]S.Shanmuga Priya, [2]Dr.A.Valarmathi, [3]M.Rizwana, [4]Dr.L.Mary Gladence

[1]Department of CSE,Assistant Professor,M.I.E.T Engg College,Trichy 620007, India
[2]Department of Computer Application, Assistant Professor & Head, Anna University BIT Campus,Trichy 62007, India
[3]Department of CSE,PG Student,M.I.E.T Engg College,Trichy 620 007,India
[4]School of computing,Assistant professor/IT,Sathyabama Institute of Science and Technology, Chennai
**Corresponding author E-mail: *shanmugapriyaraj@yahoo.com*

Abstract

Security is one of the significant worries of all associations which utilizes online methods for interchanges particularly banks. Of this, customer side is most defenseless against hacking, as the framework can't be totally shut when use over web by a typical customer is to be permitted. Most frameworks utilize a static password– based verification strategy which is anything but difficult to hack. There are different other validation strategies existing like cards, biometric recognizable proof, and so on. These strategies give better security, however are not material to online customer correspondence as these techniques require extraordinary gadgets for their usage. One conceivable technique for applying an upgraded factor of verification for online access to the framework is a dynamic secret word. In this venture we can plan the validation framework in light of key age, confirmation age and OTP based framework. The keys are created progressively utilizing Mobile IMEI number and SIM card number. The OTP age utilizes the components that are novel to the client and is introduced on a PDA in Android stage and furthermore cloud server claimed by PHP server. An OTP is legitimate for a minutes time, after which, is pointless. The framework in this way gives better customer level security – a straightforward minimal effort strategy which shields framework from hacking strategies, for example, speculating assault, answer assault, stolen and verifier assault and adjustment assault.

Keywords: *Security, Password based authentication, One time Password, Mobile Cloud communication, IMEI number*

1. Introduction

At present protection concerns are on the increasing in all zones. Most frameworks today depend on static passwords to check the client's character. Government institutions are placing benchmarks, passing laws and constraining institutions and offices to agree to these norms with resistance being met with some distance attaining effects. There are a few troubles with regards to protection issues in these diverse and converting ventures with one primary feeble connection being passwords. The fast improvement in the quantity of online administrations activates an increasing range of diverse computerized characters each purchaser desires to supervise. Yet, passwords are maybe the most widely identified sort of certification utilized these days. To stay far away from the dreary task of recollecting tough passwords, customers frequently act much less accurately via utilizing low entropy and feeble passwords. Most frameworks nowadays rely upon static passwords to check the client's person. Notwithstanding, such passwords accompany actual administration safety concerns. Clients generally tend to make use of easy to-parent passwords, make use of a similar mystery phrase in unique records or keep them on their machines, and so forth. Moreover, programmers have the selection of making use of numerous techniques to take passwords, as an instance, undergo surfing, snooping, sniffing, speculating, and so forth. Besides passwords may be composed down, left out and stolen, speculated intentionally being suggested to different individuals. Now protection things are on the scale in all zones. The majority of the frameworks today depend on static passwords to validate the client's personality. Clients encompass the predilection to develop clear passwords, basic secret key, efficiently guessable watchword and same secret key for different report, and even invent their passwords, accumulate them on their framework or approaching the sites for recalling their secret key and so on. Procedure of fixed passwords in this extensive reliance on access to IT frameworks continuously introduces themselves to Hackers, ID Thieves and Fraudsters. What's additional, programmers have the preference of utilizing different procedures/assaults, for example, speculating assault, bear surfing assault, word suggestion assault, beast compel assault, snooping assault, social building assault and so forth to take passwords in order to access their login accounts. Many methods, methodologies for utilizing passwords have been planned however some of which are particularly difficult to utilize and rehearse. To take care of the secret word issue in saving money divisions and in addition for online exchange two factor confirmations utilizing OTP and ATM stick/cards have been actualized. An approval segment is a touch of information and moves toward used to validate or check the character of an individual or other component requesting right to use under protection goals. Multifaceted check is a defense system in which in excess of one watchword of confirmation is executed to affirm the validness of a trade. In two-factor authentication, the client gives double methods for identifiable testimony, one of which is generally a physical token, for example, a card, and the other of which is

commonly impressive remembered, for example, a security code. Authentication structure is shown in fig 1.

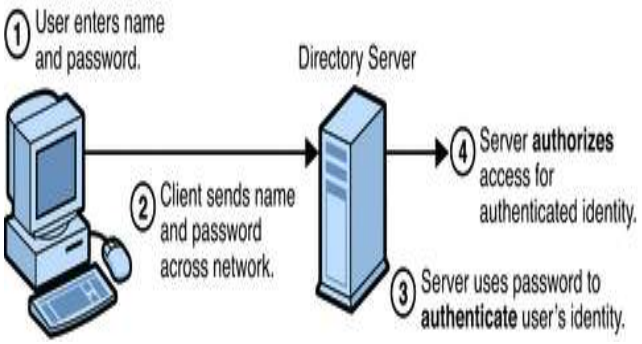

Fig 1: Authentication Structure

The goal of MFA is to create a layered safeguard and make it more complicated for an unauthorized individual to access a target corresponding to a physical place, computing device, community or database. If one aspect is compromised or damaged, the attacker nonetheless has at least one other barrier to breach before effectively breaking into the goal. Multifactor authentication is a method where in two or extra distinct explanations are used in conjunction to authenticate. Utilizing multiple aspects is often known as "strong authentication". The method that solicits multiple answers to project questions as good as retrieves 'something you might have' or 'anything you are' is regarded multifactor. Multifactor affirmation is a safety structure in which multiple appearance of affirmation is achieved to verify the validness of an exchange. In two-component affirmation, the patron gives twofold procedure for conspicuous verification, one of which is as a rule a physical token, for illustration, a card, and the other of which is generally anything held, for example, a security code. The goal of MFA is to make a layered trouble and make it more difficult for an unapproved man or woman to get to a focus, for example, a physical zone, figuring contraption, framework or database. In case one part is exchanged off or broken, the attacker nonetheless has no wanting what a further obstacle to interrupt before viably breaking into the target. Multifactor approval is a process the place in two or more targeted elements are used as a section of conjunction to approve. Using multiple segments is every so quite often called "powerful affirmation". Most of the time the multifactor approach needs more than a few reactions to test request and recoups 'similar to whatever you've got' or 'something you are'. Two-components or multi-element verification is precisely what it looks like. As opposed to utilizing one and only sort of confirmation element, for instance, simply matters a patron is aware of (Login Ids, passwords, mystery snap shots, imparted privileged insights, requested school information, and so on), two-component verification requires the growth of a 2d element, the expansion of something the consumer HAS or something the person IS. Two factor confirmations encompass restrictions which integrate the cost of buying, issuing, and commerce through the tokens or cards. Observance this innovative method has been planned, Authentication with two well-known factors such as Alphanumeric and graphical password. The basic step is shown in fig 2.

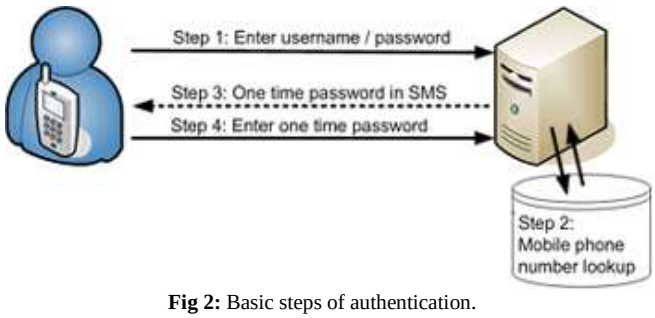

Fig 2: Basic steps of authentication.

2. Related Work

Al-Riyami,et.al,… [1] Proposed recognizable proof focused open key cryptography (personality PKC) which handles the hindrance of validity of keys unmistakably to customary PKI. In distinguishing proof PKC, a viewpoint's open key's gotten direct from unmistakable elements of its character, for example, an IP furnish having a circumstance with a procedure have, or an email manage related with a client. Elite keys are made for materials by a trusted pariah called a select key generator (PKG). The prevalent altogether rational and loose character based open key encryption plan used to be shown. From that factor forward, an expedient development of character %has happened. There now exist character based key interchange traditions, signature designs, a considerable amount of leveled plans and a noteworthy group of various locals. It has besides been portrayed, how personality percent can be used as a gadget to approve what is likewise named "cryptographic work techniques", that's, arrangements of occasions (e.g. Checks) that must be done with the guide of a substance in order to achieve a natty gritty reason. The prompt choice of open keys in ID %takes out the prerequisite for confirmations and a piece of the scatters related with them. Of course, the dependence on a PKG who uses a system wide pro key to make private keys clearly familiarizes key escrow with id-percent frameworks.

Au, Man Ho, et al,… [2] Proposed certificateless plans, it is always expected that the malicious KGC starts pushing strikes (claimed Type II ambushes) basically after it has made a pro open/riddle key join genuinely. In this paper, we propose new security models that remove this doubt for both certificateless check and encryption designs. Under the new models, we exhibit that a class of certificateless encryption and stamp designs proposed already is questionable. These designs still experience the evil impacts of the key escrow issue. In a certificateless cryptosystem, a Key Generation Center (KGC) is related with issuing customer partial key to customer whose identity is believed to be excellent in the system. The customer in like manner uninhibitedly makes an additional customer open/riddle key join. Cryptographic exercises would then have the capacity to be performed viably exactly when both the customer fragmentary key and the customer riddle key are known. Knowing only a solitary of them should not have the ability to copy the customer that is, finishing any cryptographic errands as the customer paying little respect to whether the KGC is toxic, the KGC should not have the ability to play out any cryptographic action as the customer, gave that the KGC can't supplant the customer open key or find the customer riddle key, however the KGC knows the customer deficient key.

Blaze,et.al, [3] Present another approach for fine-grained control over customers' security benefits (brisk revocation of accreditations) spun around the possibility of an on-line semi-place stock in mediator (SEM). The use of a SEM in conjunction with a direct utmost variety of the RSA cryptosystem (mediated RSA) offers different convenient central focuses over current denial systems. The focal points consolidate enhanced endorsement of modernized imprints, capable support revocation for legacy structures and snappy denial of check and translating limits. This paper looks at both the building and the utilization of our approach and furthermore its execution and closeness with the present system. Test comes to fruition show its sensible points of view. We acknowledge that a Public Key Infrastructure (PKI) is available and all customers have modernized mark, and furthermore en/unscrambling, capacities. Over the traverse of performing routine normal errands, customers abuse secure applications, for instance, email, record trade, remote sign in and web examining. By and by accept that a place stock in customer (Alice) achieves something that warrants provoke repudiation of her security benefits. For example, Alice might be ended, or she may theorize that her private key has been exchanged off. Ideally, quickly following disavowal, the key holder, either Alice herself or an assailant, should be not capable play out any security

exercises or use any ensured applications.
Boneh,et.al,[4] Shown another approach for fine-grained control over customers' security benefits (snappy repudiation of capabilities) in light of the possibility of an on-line semi-place stock in referee (SEM). The use of a SEM in conjunction with a direct cutoff variety of the RSA cryptosystem (mediated RSA) offers different down to business purposes of enthusiasm over current disavowal frameworks. The focal points fuse streamlined endorsement of mechanized imprints, powerful validation renouncement for legacy structures and brisk denial of stamp and unscrambling limits. This paper discusses both the building and the use of our approach and moreover its execution and closeness with the present establishment. The results show its rational perspectives. We acknowledge that a Public Key Infrastructure (PKI) is available and all customers have modernized mark, and what's more en/disentangling, capacities. Over the traverse of performing routine standard assignments, customers misuse secure applications, for instance, email, report trade, remote sign in and web examining.
Matt Franklin,et.al,… [5] Picked figure security in the sporadic prophet demonstrates tolerating a variety of the computational Diffe Hellman issue. The structure relies upon bilinear maps between social events. The Weil mixing on elliptic twists is an instance of such a guide. We give correct definitions for secure identity based encryption designs and give a couple of utilizations for such structures. To fight about the security of our IBE structure we describe picked figure security for identity based encryption. Our model gives the enemy more power than the standard model for picked figure security. To begin with, we empower the aggressor to ambush a self-confident open key ID of her choice. Second, while mounting a picked figure ambush on ID we empower the assailant to secure from the PKG the private key for any open key of her choice, other than the private key for ID. This models an attacker who gains different private keys contrasting with a couple of characters of her choice and after that tries to strike some other open key ID of her choice. To be sure, even with the help of such inquiries the attacker should have insignificant good position in vanquishing the semantic security of the system. The straggling leftovers of the paper are dealt with as takes after. A couple of employments of character based encryption are analyzed. By then give correct definitions and security models.

3. Existing Methodologies

In the current sophisticated day with striking development in Computer division, Single factor confirmation, e.g. passwords, is no further consider as protected in the World Wide Web. It has never been less troublesome in Securing the construction and isolated access. Basic, apparent and easy to-figure passwords, for example, names and age, are effortlessly revealed by means of programmed unknown key social instance programs. The protection and defense dangers all the way through malware are consistently forever fetching mutually in amount and quality. Extensive access to records builds inadequacy to hacking, breaking of passwords and online fakes. In this attachment the habitual login/watchword confirmation is measured defectively protected for a few security-basic applications, for example, login to Mailing Accounts, Social Networks, Gadgets, Financial records, official secured systems, and business sites online and so forth. Obliging in excess of one autonomous factor expands the trouble of giving false certifications

3.1. Passwordless Login System Using CAPTCHA

One of the plans which are proposed to customers to crush these strikes is picking exceptional passwords which contain characters, numbers, and pictures and don't have any importance. The customers furthermore encouraged to change their passwords frequently. However, the rule impediment of this system is that customers ignore these passwords, in light of the way that these passwords don't have any centrality and holding them is troublesome. What's more every customer as a general rule has various passwords in different destinations and troublesome, especially if they are changed a significant part of the time. This structure relies upon IMEI code and uses a CAPTCHA technique. CAPTCHA (Completely Automatic Public Turing Test to Tell Computer and Human Apart) are structures which are used to recognize human and machine one from the other therefore. These systems rely upon Artificial Intelligence (AI) focuses. They resemble Turing test, yet they differentiate in that the judge is a PC. The target of these structures is to make request which human customers can without quite a bit of an extend reply, while current PCs can't. In the accompanying fragment, we will discuss these structures in more inconspicuous components. The IMEI (International Mobile Equipment Identity) number is a 15-digit number which is extraordinary for every wireless and it is used to see the GSM/DCS/PCS PDAs in sort out organizations. In this technique, a photo of a number is appeared to the customer and he/she should type it. The customer response is coded with his/her mobile phone IMEI and sent to the server. The server checks customer's response as demonstrated by customer's IMEI and if it is correct, let the customer to enter the site, so there is no convincing motivation to enter any mystery word. In like manner, the customer's PDA IMEI never sent. In like manner the customer does not require entering the IMEI code in light of the way that the program gets it from phone thusly.

3.2 Two Factor Authentication Using SMART CARD

In this structure, begin the examination of twin specific or particular or especially security risks (techniques for explanation of an objective or an affirmation to convey hurt on another) on quick card based watchword affirmation (or endorsement planning) in scattered systems. Sharp card based mystery word affirmation is one among the boss for the most part used security instruments to see the identity of an evacuated purchaser, who should hold a genuine canny card and moreover the contrasting watchword with hold out a flourishing approval with the server. The approval is ordinarily planned with a key establishment tradition and yields smartcard-based mystery scratch affirmed scratch assertion. Swindle two starting late orchestrated traditions as logical examinations; we tend to display two new kinds of foes with sensible card: Adversaries with pre-figured information hold tight inside the insightful card, and Adversaries with extremely shocking or absolutely interesting information (with association with different opening) hold tight inside the sagacious card. These risks, but down to earth in scattered systems, haven't been considered inside the written work. In addition, to construe the vulnerabilities, we tend to propose the countermeasures to agitate the prosperity perils and secure the traditions. Canny cards can be either contact or contactless insightful card. Splendid cards can give singular ID, affirmation, data storing, and application dealing with. Astute cards may give strong security approval to single sign-on (SSO) inside significant affiliations. This proposition came back to the assurance of 2-factor PAKA (Password Authenticate Key Agreement) traditions through sensible (keen) cards. While they were believed to be secure, we showed that these traditions are defective under their own specific doubts separately. In particular, we considered a couple of sorts of foes which were not considered in their frameworks or approach, e.g., challengers with pre-discovered data saved like (enlistment information, and other related information of record and customer recognizing evidence) in the sensible-card and challengers with different information (concerning dynamic opening) saved in the sensible (sharp) card. These challengers address the potential risks (strategies for a confirmation to correct harm on another) in coursed structures and are unmistakable which thought from both the academic group and the business.

3.3 Multi Factor Authentications:

Biometric Based Authentication Biometric confirmation system uses physiological or behavioral characteristics of a man for approval. It relies upon "Something You Are". A segment of the biometric affirmation systems use one of a kind check affirmation, face affirmation, iris affirmation or voice affirmation to confirm the customers. Biometric recognizing verification depends upon PC estimations to settle on a yes or no decision. This method enhances customer advantage by giving quick and straightforward conspicuous confirmation. Keeping up security is winding up being all the all the more testing with time. A level of the difficulties can be anticipated; for example, moves in estimation that are making it continually less asking for to word reference attack a riddle key database. Various difficulties are harder to assume, for example, the exposure of new "day-zero" vulnerabilities in working programming. In this manner, security prerequisites are not balanced, yet rather expand with time. Multifaceted certification is reliably being utilized to work around the principal inadequacies in riddle key association. While three-segment affirmation improves security, it develops client pounding, a specific issue for online associations that are not in a circumstance to charge 3FA. Combined 3FA gives the best ease of use to better security, so a three-fragment check headway that can be moved to mastermind the three factors all the more nearly has the best capacity to make as requirements change and furthermore to help client take-up of discretionary 3FA. After the client gives their username, three procedures for movement are accessible for the clients in light of their slant and requirements. The major is a stay singular approach that is unquestionably not hard to utilize and secure and is regular. The second approach is picture-based logic that is in like way simple to utilize and secure yet requires structure plots and the third approach is biometric affirmation which is something the client has like exceptional finger impression, palm print, and retinal yield, yet turns costly.

3.4 Knowledge based Authentication

The data based systems are the most frequently used affirmation structures. They are of two sorts: Text based passwords and picture based passwords. Regardless of the way that there are unmistakable sorts of approval methodologies available alphanumeric passwords are the extensively used in light of the fact that they are versatile and it is definitely not hard to execute and use. The based passwords need to satisfy two clashing necessities. That is it should be easily recalled by the customer and it should be hard to figure by an aggressor. So these passwords are feeble against word reference ambushes and savage power strikes. Learning based confirmation can be used close by other approval methodology to ensure security. Picture based passwords uses pictures for making passwords

4. Proposed Work

In proposed work, we can beat the examination situations, for example, the passwords or check tables are not put away inside the PC. The secret key can be picked and changed openly by the proprietor. The secret key can't be uncovered by the chairman of the server. The passwords are not transmitted in plain content on organize. Nobody can imitate a lawful client to login the server. The plan must oppose the replay assault, speculating assault, adjustment assault, and stolen-verifier assault. The length of a secret key must be suitable for remembrance. The plan must be productive and reasonable. The plan can accomplish shared confirmation. Can server check the legitimate clients, as well as clients can confirm the lawful server. The secret key can't be broken by speculating assault regardless of whether the savvy card is lost. The proposed framework engineering give enhanced structure. The proposed work includes the following steps:

4.1 User Registration:

The fast development in the quantity of online administrations prompts an expanding number of various advanced personalities every client needs to oversee. Be that as it may, passwords are maybe the most well-known kind of certification utilized today. In this module, client enrolls their subtle elements, for example, name, portable number, email id et cetera. What's more, send the administration demand to cloud server.

4.2 Certificate Generation:

In cryptography, an open key authentication, otherwise called an advanced declaration or personality testament, is an electronic record used to demonstrate the responsibility for open key. The endorsement incorporates data about the key, data about the personality of its proprietor (called the subject), and the advanced mark of a substance that has checked the authentication's substance (called the backer). In cryptography, a nonce is a subjective number that may just be utilized once. It is comparative in soul to a nonce word, thus the name. It is regularly an irregular or pseudo-arbitrary number issued in a verification convention to guarantee that old correspondences can't be reused in replay assaults. They can likewise be valuable as instatement vectors and in cryptographic hash capacities. The hash capacities can be created utilizing secure hash calculation. In this module, create the match of keys, for example, private and open key utilizing Asymmetric calculation. Open key cryptography, or topsy-turvy cryptography, is any cryptographic framework that utilizations set of keys: open keys which might be scattered broadly, and private keys which are known just to the proprietor. The quality of an open key cryptography framework depends on the level of trouble (computational difficulty) for a legitimately produced private key to be resolved from its comparing open key. Security at that point depends just on keeping the private key private, and the general population key might be distributed without trading off security. At that point create authentication in view of Nonce, Public key

4.3 Key Generation:

Server can be produced PU (Nonce1) and forward to client. At long last Secret key produced in light of IMEI number and SIM number. The IMEI number is utilized by a GSM system to distinguish legitimate gadgets and in this way can be utilized for preventing a stolen telephone from getting to that system. For instance, if a cell phone is stolen, the proprietor can call their system supplier and educate them to boycott the telephone utilizing its IMEI number. This renders the telephone pointless on that system and some of the time different systems as well, regardless of whether the telephone's endorser personality module (SIM) is changed. The IMEI is utilized for distinguishing the gadget and has no changeless or semi-lasting connection to the endorser. Rather, the endorser is distinguished by transmission of an International versatile supporter character (IMSI) number, which is put away on a SIM card that can in principle be exchanged to any handset. Be that as it may, numerous system and security highlights are empowered by knowing the present gadget being utilized by an endorser.

4.4 OTP Generation and Login:

One time password can be produced utilizing SHA-3 calculation. Hash calculations are fundament to numerous cryptographic applications. Albeit broadly connected with computerized signature innovation, the hash calculation has a scope of different employments. A safe hash calculation, regularly referred to just as a "SHA," is a hashing calculation that is considered cryptographically secure. By and large, hashing capacities are utilized to sort and compose advanced information into littler, more classified parcels for secret word. Also, exchange the OTP to

Server. Server can be contrast OTP and Allow access with the framework. A one-time secret key (OTP) is a password that is substantial for just a single login session or exchange, on a PC framework or other computerized gadget. OTPs keep away from various deficiencies that are related with conventional (static) password based confirmation; various executions likewise consolidate multi factor verifications by guaranteeing that the one-time secret word expects access to something a man has and in addition something a man knows. In the wake of getting password, the individual effectively goes into the framework. The proposed system framework is shown in fig 3.

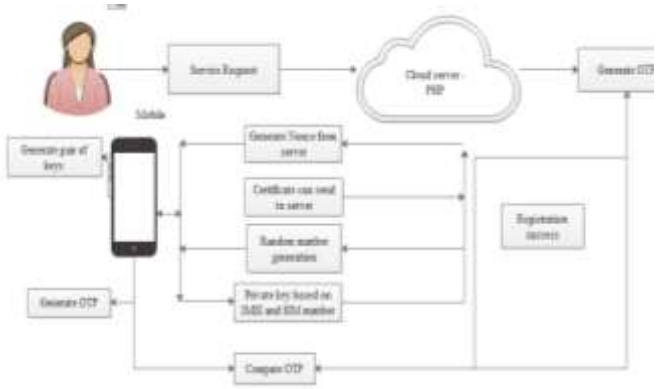

Fig 3: Proposed architecture

5 Experimental Results

We can implement this system in real time android based PHP system for provide improved authentication. The registration page is shown in fig 4.

Fig 4: Home page

The login page is shown in fig 5.

Fig 5: Login page

The key generation and random number generation is stored in fig 6.

Fig 6: Key generation and Random number

The OTP verification can be implemented in android mobile and verified with PHP server can be shown in fig 7.

Fig 7: OTP verification

In user side, we can read the IMEI and SIM card number automatically as shown in fig 8.

Fig 8: Key, IMEI and SIM card details

The performance result of response time is shown in fig 9.

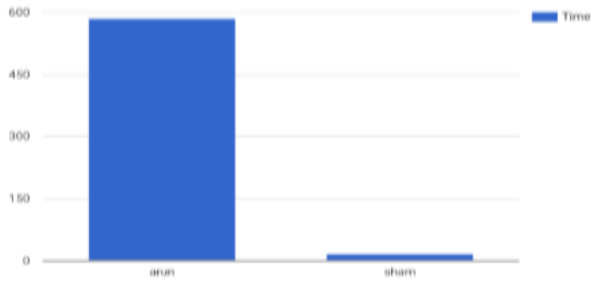

Fig 9: Response time

6 Conclusion

Today, single factor approval, e.g. passwords, is never again seen as secure in the web and keeping cash world. Easy to-figure passwords, for instance, names and age, are successfully discovered by means of automated mystery key social affair programs. Enhanced check has starting late been familiar with

deal with the request of relationship for giving more grounded approval decisions to its customers. All things considered, a hardware token is given to each customer for each record. The extending number of passed on tokens and the cost the collecting and keeping up them is transforming into a weight on both the client and affiliation. Since various clients pass on a PDA today reliably, an alternative is to present all the item tokens on the PDA. This will help lessen the amassing costs and the amount of devices passed on by the client. The system exhibited better than anything various as of now existed structures. The OTP based affirmation structure using a connectionless age framework was found powerful than various other existing strategies when factors like storage space, time, et cetera were considered. All that is required for this aim is a propelled cell phone with a direct application presented in it. As phone is an average device used by every ordinary national today, this framework won't require much effort for its execution. The system wound up being protected from common kind of attacks, for instance, hypothesizing strikes, replay ambushes, alteration attacks and stolen and verifier attacks. The OTP made each time was intriguing with the objective that one OTP was not usable the accompanying minute. Additionally, realize this structure ceaselessly flexible cloud conditions.

References

[1] Al-Riyami, Sattam S., and Kenneth G. Paterson. "Certificateless public key cryptography." Asiacrypt.Vol. 2894. 2003.

[2] A.Groce and J. Katz, “A New Framework for Efficient Password-Based Authenticated Key Exchange,” in ACM CCS, 2010, pp. 516– 525.

[3] Au, Man Ho, et al. "Malicious KGC attacks in certificateless cryptography." Proceedings of the 2nd ACM symposium on Information, computer and communications security.ACM, 2007.

[4] Blaze, Matt, GerritBleumer, and Martin Strauss. "Divertible protocols and atomic proxy cryptography." Advances in Cryptology—EUROCRYPT'98(1998): 127-144.

[5] Boneh, Dan, Xuhua Ding, and Gene Tsudik. "Fine-grained control of security capabilities." ACM Transactions on Internet Technology (TOIT) 4.1 (2004): 60-82.

[6] Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." Advances in Cryptology—CRYPTO 2001. Springer Berlin/Heidelberg, 2001.

[7] D. Pointcheval and S. Zimmer, “Multi-Factor Authenticated Key Exchange,” in ANCS, ser. Lecture Notes in Computer Science, vol. 5037, 2008, pp. 277–295.

[8] L. Lamport, ”Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770?LC772, 1981.

[9] M. Bellare, D. Piontcheval, and P. Rogaway, “Authenticated Key Exchange Secure Against Dictionary Attacks,” in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 1087, 2000, pp. 139–155.

[10] O. Goldreich and Y. Lindell, “Session-key generation using human passwords only,” in CRYPTO, 2001, pp. 408–432.

[11] Q. Jiang, J. Ma, G. Li, and L. Yang, ”An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks,” Wireless Personal Communications, vol. 68, no. 4, pp. 1477-1491, 2013.

[12] Q. Jiang, J. Ma, G. Li, and L. Yang, ”An efficient ticket based authentication protocol with unlinkability for wireless access networks,” Wireless Personal Communications, vol. 77, no. 2, pp. 1489-1506, 2014.

[13] S. M. Bellovin and M. Merritt, “Augmented Encrypted Key Exchange: A PasswordBased Protocol Secure Against Dictionary Attacks and Password File Compromise,” in ACM CCS, 1993, pp. 244–250.

[14] V. Boyko, P. MacKenzie, and S. Patel, “Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman,” in EUROCRYPT, 2000, pp. 156–171.

[15] W. Juang and J. Wu, “Two Efficient Two-Factor Authenticated Key Exchange Protocols in Public Wireless LANs,” Computers &Electrical Engineering, vol. 35, no. 1, pp. 33–40, 2009

[16] . Wang, W. Zhang, J. Zhang, and M. K. Khan, “Cryptanalysis and Improvement on Two Efficient Remote User Authentication Scheme Using Smart Cards,” Computer Standards & Interfaces, vol. 29, no. 5, pp. 507–512, 2007.

[17] Y. M. Park and S. K. Park, “Two Factor Authenticated Key Exchange (TAKE) Protocol in Public Wireless LANs,” in IEICE Trans on Communications, vol. E87-B, no. 5, 2004, pp. 1382–1385