Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol. 6 No. 1, 2017, pp.40-43

Dual Authentication Using Mobile Application in Cloud Computing

D. Barathi
Research Scholar
Department of Computer Science
Sri Ramakrishna College of Arts and Science for Women, Coimbatore, Tamil Nadu. India
Email: Barathi.rajaay88@gmail.com

***Abstract* - *Internet* is that the center of all style of social and monetary activities. It's enabled organizations to supply their services on-line. Customers feel easier to avail on-line services like ebanking services rather than ancient banking services. They will gain these services twenty four hours each day from their homes. It saves their time and cash and conjointly provides them a lot of open marketplace for comparison. However at same time, security is that the biggest challenge in electronic atmosphere. In past few years, electronic banking has suffered from many malicious attacks like phishing scams, man within the middle attacks and malicious computer code attacks. To beat these issues the Mobile phones square measure ordinarily employed by net servers to validate user's identification and authentication. It enhances user's trust in on-line transactions and empowers him to use his mobile network as a further layer of security. This mechanism is understood as Mobile group action Authentication system of numeration (mTAN) that is employed by e-banks and social media sites. This technique has some weakness and users square measure still susceptible to serious security risks. Unauthorized people will notice their ways that to urge unauthorized access in ancient mTAN system. During this project, we've got explored weaknesses in current mTAN system and planned an answer for reliable and secure use of 2 layer security.**

***Keywords* : mTAN, 2 Layer Security, one-time-password, Transaction Authentication Number.**

I. INTRDUCTION

Over the past few decades, text watchword has been adopted because the primary mean of user authentication for websites. Individuals choose their username and text passwords once registering accounts on an internet site. So as to log into the web site with success, users should recall the chosen passwords.[1].Generally, password-based user authentication will resist brute force and wordbook attacks[2] if users choose sturdy passwords to produce ample entropy. However, password-based user authentication encompasses a major drawback that humans aren't specialists in memorizing text strings. Thus, most users would opt for easy-to-remember passwords (i.e., weak passwords) although they recognize the passwords could be unsafe.[6] [9] Another crucial drawback is that users tend to utilize passwords across numerous websites.

II. PREVIOUS WORK

In past few years, electronic banking has suffered from many malicious attacks like phishing scams, man within the middle attacks and malicious computer code attacks.[11] Generally, users don't have enough information and skills to properly utilize security implementations for his or her safety. Scammers take advantage of these vulnerabilities and obtain access to personal or money knowledge of users. For user authentication, net servers area unit mistreatment multi issue authentication schemes to reduce authentication connected risks in net primarily based communication.[15], They're providing an additional layer of security by mistreatment user's GSM network.

III. LIMITATIONS

1. In this method has some weaknesses.
2. Layer two isn't as secure as usually thought of.
3. Attackers will monitor GSM network and use malicious phone applications to get mobile group action authentication variety.

IV. PROPOSED SYSTEM

In our projected work we have a tendency to implement with twin Security System (mTAN system) is employed by ebanks and social media sites and it appears secure and trustable as a result of it need concurrent access of each networks. Associate in Nursing improved theme named as MABS-E which mixes 2 schemes MABS-B and packet filtering mechanism in touch packet injection. Historically, Mobile group action Authentication variety (mTAN) primarily based security mechanism needs 2 networks for completion of any group action. This system implements security in 2 layers: net and GSM network. Unauthorized people got to have access on each networks for intrusion. They have to access login data from net and authentication variety from user's transportable.

A.Advantages

1. It provides an additional layer of security by mistreatment 2 networks for identification and authentication.
2. It makes one-time- countersign system additional convenient and user friendly.

3. Currently users don't got to save lists of group action Authentication Numbers (TANs).
4. Instead, they'll receive TAN through their transportable on every occasion once needed.
5. The projected modifications in existing system can enhance the protection of two layer system and create it additional trustable.

V. ARCHITECTURE DIAGRAM

A. Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol

WTLS (Wireless Transport Layer Security) is a crucial customary protocol for secure wireless access to net services.[6] WTLS employs public-key cryptosystems throughout the hand shake between mobile shopper and WAP entryway (server).Several cryptosystems at completely different key strengths may be employed in WTLS. The trade-off is security versus process and coordinated universal time. During this paper, associate degree analytical performance model for public-key cryptosystem operations in WTLS protocol is developed. Completely different handclasp protocols, completely different cryptosystems and key sizes area unit thought-about. Public-key crypto systems area unit enforced victimization state-of-the–art performance improvement techniques, yielding actual performance figures for individual cryptosystems. These figures and also the analytical model area unit won't to calculate the price of victimization public-key cryptosystems in WTLS. Results for various cryptosystems and handclasp protocols area unit relatively portrayed and understood. It's been ascertained that ECC (Elliptic Curve Cryptography) performs higher than its rival RSA cryptosystem in WTLS. Performance of some stronger ECC curves, that aren't thought-about in WTLS customary, is additionally analyzed. Results showed that a number of those curves might be employed in WTLS for prime security applications with an appropriate degradation in performance.

B. Privacy-Preserving Public Auditing for Data Storage security in Cloud Computing

Cloud Computing is that the long unreal vision of computing as a utility, wherever users will remotely store their data into the cloud thus on fancy the on-demand prime quality applications and services from a shared pool of configurable computing resources. By knowledge outsourcing, users may be mitigated from the burden of native knowledge storage and maintenance. [5] However, the fact that users not have physical possession of the probably large size of outsourced knowledge makes the information integrity protection in Cloud Computing a really difficult and probably formable task, particularly for users with strained computing resources and capabilities. Thus, sanctioning public auditability for cloud knowledge storage security is of important importance so users will resort to associate degree external audit party to ascertain the integrity of outsourced data once required. To firmly introduce an efficient third party auditor (TPA), the subsequent 2 basic needs have to be met: 1) TPA ought to be ready to expeditiously audit the cloud data storage while not exacting the native copy of knowledge, and introduce no extra on-line burden to the cloud user; 2) The third party auditing method ought to herald no new vulnerabilities towards user knowledge privacy. During this paper, we have a tendency to utilize and uniquely combine the general public key based mostly holomorphic appraiser with random masking to attain the privacy-preserving public cloud data auditing system that meets all higher than needs. To support economical handling of multiple auditing tasks, we have a tendency to further explore the technique of additive combination signature to extend our main result into a multi-user setting, wherever TPA will perform multiple auditing tasks at the same time. in depth security and performance analysis shows the projected schemes area unit provably secure and extremely economical.

C. An Improved Dynamic Provable Data Possession Model

Cloud computing is changing into more and more well-liked. Many corporations, organizations and individuals choose to source their computing demands and storage demands. so as to confirm the integrity of the knowledge within the Cloud, particularly the dynamic files which may be updated on-line, we have a tendency to propose an improved dynamic demonstrable knowledge possession model: It divides file into blocks, generates a tag for each block, computes a hash price for every tag, uses tags to confirm the integrity of the file blocks,[11] and uses hash values to confirm the integrity of the tags. Compared with previous works, it reduces the process and communication complexityfromto constant. Though shopper wants to store some secret values which can produce some additional storage expense, it solely takes up about0.02% of the first file size. Thence it is acceptable in most cases.

D. Hybrid Provable Data Possession at Untrusted Stores in Cloud Computing

In recent years, cloud computing has gradually become the thought of web services. once cloud computing environments become additional excellent, the business and user are going to be a huge quantity of information keep within the remote cloud storage devices, hoping to realize random access, data collection, scale back prices, facilitate the sharing of alternative services. However, once the info is keep within the cloud device, a long time, enterprises and users inevitably can have security concerns, fearing that the data is really keep within the cloud remains in the device or too long while not access to, has long been the cloud server removed or destroyed, resulting in businesses and users within the future can't access or restore the data files. Therefore, this theme goal to analysis and style for data storage cloud computing environments that area unit tested. Stored within the cloud for knowledge storage, analysis and

develop security and economical storage of proof protocol, can also delegate or authorize others to public verifiability whether or not the data really keep within the cloud storage devices.

E. Robust Dynamic Provable Data Possession

Remote knowledge Checking (RDC) permits shoppers to efficiently check the integrity of information keep at untrusted servers.[15] This permits knowledge homeowners to assess the chance of outsourcing detain the cloud, creating RDC a valuable tool for knowledge auditing. Robust DC theme incorporates mechanisms to mitigate arbitrary amounts of information corruption. Specifically, protection against little corruptions (i.e., bytes or perhaps bits) ensuresthatattacks that modify a number of bits don't destroy associate encrypted file or invalidate authentication info. Early RDC schemes have focused on static knowledge, whereas later schemes like DPDP support the complete vary of dynamic operations on the outsourced knowledge, including insertions, modifications, and deletions. Strengthis required for each static and dynamic RDC schemes that relyonspot checking for potency. However, underneath associate adversarial setting there's a basic tension between economical dynamic updates and therefore the encoding required to realize strength, as a result of change even a tiny low portion of the file could need retrieving the complete file. We have a tendency to determine the challenges that require to be overcome once making an attempt to feature strength to a DPDP theme. We have a tendency to propose the first DC schemes that offer strength and, at an equivalent time, support dynamic updates, whereas requiring little, constant, shopper storage. Our initial construction is economical in coding, however has high communication value for updates. Our second construction overcomes this disadvantage through a mixture of techniques that has RS codes supported Cauchy matrices, decoupling the coding for strength from the position of symbols in the file, and reducing insert/delete operations to append/modify operations once change the RS-encoded parity knowledge.

VI. MODULES

A. User Authentication

1. Online customers should have access to a laptop and a way of payment. In our system, the user interactions square measure login, registration, communication, on-line payments and group action. User details square measure handled in backend common information.
2. In laptop security, a login or logon is that the method by that individual access to a system is controlled by distinguishing and authenticating the user concerning credentials conferred by the user.
3. A user will log in to a system to get access and might then log off or log out once the access is not any longer required. To log off is to shut off one's access to a system once having antecedently logged in.

B. Email Validation & Verification

During registration method the e-mail validation and verification are going to be processes. That is, initial it checks our entered email id is valid or not. That point we tend to use validation method. Once validation we will verify that email for whether or not it's right or not. Instantly match email addresses to famous dead domain names, malicious email addresses, and customary typographic errors in email address submissions

C. Long term password generation

In our project, the long run secret created by user. That is, in registration method the long run secret given by user that keep in internet server with encrypted format.

D. Password Encryption

a. The main security for our system is just one occasion secret authentication. The just one occasion secret created in internet application and send to humanoid application.
b. One-time pad (OTP) could be a style of cryptography that has been proved to be not possible to crack if used properly. Every bit or character from the plaintext is encrypted by a standard addition with slightly or character from a secret random key (or pad) of constant length because the plaintext, leading to a cipher text. If the secret's really random, as giant as or larger than the plaintext, ne'er reused in whole or half, and unbroken secret, the cipher text are going to be not possible to decode or break while not knowing the key.
c. Using Triple DES rule for just one occasion secret cryptography. This rule not solely used for secret encryptions however conjointly used to be used details encryptions.

E. Android application login process

In humanoid application, a login is that the method by that individual access to a mobile application is controlled by distinguishing and authenticating the user concerning credentials conferred by the user.

F. OTP Decryption

The just one occasion secret coding method exhausted humanoid application exploitation same Trible DES rule and same key of cryptography.

G. OTP Validation

Once the user got a 1 time secret in humanoid application from mobile application. That secret entered to internet application. In internet application, the just one occasion secret competition is processes. That’s compare causing OTP to user enterer choose. If the competition is true then it'll visit application otherwise airt to login page. '

H. Application Maintenance

Application maintenance could be an intimidating task for enterprises. They're struggling to scale back spends on maintenance. Whereas making certain optimized performance of their IT systems and applications. Final module of our project as application maintenance. That is, to take care of our application with a lot of and a lot of security. Like PIN code analysis and PROTOCOL reification.

VII. CONCLUSION

In this paper, we have a tendency to project a user authentication protocol named Protocol that leverages cell phones and SMS to thwart secret stealing and secret apply attacks. We have a tendency to assume that every web site possesses a novel sign. We have a tendency to conjointly assume that a telecommunication service supplier participates within the registration and recovery phases. The planning principle of Protocol is to eliminate the negative influence of human factors the maximum amount as attainable. Through Protocol, every user solely has to keep in mind a semi-permanent secret that has been accustomed defend her cellular phone. Users square measure free from typewriting any passwords into untrusted computers for login on all websites. Compared with previous schemes, Protocol is that the 1st user authentication protocol to stop secret stealing (i.e., phishing, key logger, and malware) and secret apply attacks at the same time. The explanation is that Protocol adopts the one-time secret approach to confirm independence between every login. To build Protocol totally useful, secret recovery is additionally thought-about and supported once users lose their cell phones. They will recover our Protocol system with reissued SIM cards and semi-permanent passwords. A model of Protocol is additionally enforced to live its performance. The common time spent on registration and login is21.8 and 21.6 s, severally. Per the result, SMS delay occupies over four-hundredth of total execution time. The delay may well be shorter by victimization advanced devices. Besides, the performance of login of Protocol is best than graphical secret schemes, as an example, Pass faces. The login time of Pass faces is from fourteen to eighty eight s that is longer than Protocol. Therefore, we have a tendency to believe Protocol is suitable and reliable for users. Toanalyses Protocol's usability, we have a tendency to invited twenty four participants to conduct the user study. Most participants might simply operate all procedures of the Protocol system. The login success rate is over ninetieth, aside from a couple of typewriting errors. Consequently, all of them united Protocol is safer than the first login system. Certainly, a number of the participants like Protocol to the first system.

REFERENCES

[1] Singh, R.K. and Pais, A. R., "Secure Web Based Single Sign-On (SSO) framework using Identity Based Encryption System," International Conference on Advances in Recent Technologies in Communication and Computing, Kerala, 2010

[2] Zhou, Y. Zhu, X. Fang, Y., "MABS: Multicast Authentication Based on Batch Signature," IEEE transactions on mobile computing, Issue No.07 - July(2010 vol.9), 2010

[3] Jang, W. Cho, S. Lee, H. Ju, H. Kim, J., " Rooting Attack Detection Method on the Android based Smart Phone, "International Conference on Computer Science and Network Technology, 2011

[4] Hisamatsu, Pishva, D. and Nishantha, G.G.D., "Online Banking and Modem Approaches toward its Enhanced Security," The 12th International Conference on Advanced Communication Technology (ICACT), 2010

[5] Fatemi Moghaddam, F, "A scalable and efficient user authentication scheme for cloud computing Environments," IEEE Region 10 Symposium, 508 – 513, 2014

[6] Gupta, S. Sengupta, S. Bhattacharyya, M. Chattrejee, S. and Sharma, B. S. "Cellular Phone Based Web Authentication System Using 3-D Encryption Technique under Stochastic," First Asian Himalayas International Conference on internet, Kathmandu, 2009

[7] Thiyagarajan, Venkatesan, P. Aghila, G. "Anti-Phishing Technique using Automated Challenge Response Method," International Conference on Communication and Computational Intelligence (INCOCCI), Erode, 2010

[8] Avarzaman, M. M. Salahi, A., "Increasing performance of authentication in universal mobile telecommunication system," International Conference on Application of Information and Communication Technologies, Baku, 2009

[9] Al-Dala'in, T.Summons, P. and Luo, S., "A Prototype Design for Enhancing Customer Trust in Online Payments," Journal of Computer Science 5 (12): 1037- 1044, 2010

[10] Seto, J., "User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices," IEEE Transactions on Emerging Topics in Computing, 2015

[11] Rahman, N. A. B. A. Harun, K. S. B. Yusof, Y. B., "SMS Banking Transaction as an Alternative for Information, Transfer and Payment at Merchant Shops in Malaysia, 3rdInternational Conference on Information Technology and e-Services (ICITeS), Sousse," 2013

[12] Christianson, H. X. B. and Zhang, Y., "A Purchase Protocol with Live Cardholder Authentication for Online Credit Card Payment," The 12th International Conference *on Advanced Communication Technology* (ICACT), 2010

[13] Zhang, Z. Yu, M. Huang, M., "Based Mobile Agent Transaction Authentication Scheme," *International Conference on Computational Intelligence and Natural Computing* (CINC), 2009

[14] Hartung, D. Busch, C., "Biometric Transaction Authentication Protocol," *Fourth International Conference on Emerging Security Information, Systems and Technologies, 2010*

[15] Xu, J. Zhang, D. Liu, L. Li X., "Dynamic Authentication for Cross-Realm SOA-Based Business Processes," *IEEE Transactions on Computing Services*, Issue No.01 - Jan.- March (vol.5), 2012

[16] Ribalda, R. Rivera, G. G. Castro, A. Garrido, J., "A Mobile Biometric System-on-Token System for Signing Digital Transactions," *IEEE Security & Privacy, vol.8 Issue No.02, 2010*