iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4528

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

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 IV, April 2018- Available at www.ijraset.com

Secure Two Factor Authentication of Protocol using Key Exchange Method

Pasupuleti Naveen[1], Swarnava Das[2], Sunny Kumar[3], Mrs. Krishnammal[4], Dr. P. Mohamed Fathimal[5]
[1]*Srm University*

Abstract: ***In last five years of survey, around 30 billion of data have been breached. Nowadays since data can be accessed anywhere and with any network connected device, it is very necessary to provide a better security system to cloud storage. So, in order to do so a new security system is being proposed in which a new key is generated in the background during every login. Also for the shared data, a time limit is provided beyond which the access to the data will not be allowed. And for downloading of data also a unique key is generated automatically without which the data cannot be downloaded.***
Index Terms: Encryption, Key Exchange, smart id, password.

I. INTRODUCTION

The development of the high level encryption techniques will provide the authorization of key exchange problems in day to day life. To provide efficient authentication, the password authentication has to be generated randomly and securely. A person should not have any sort of access when try to actually authorize himself using wrong credentials. This means, unauthorized access may be captured by intruders when the data is ”sniffed out of the air” in various techniques without requiring wire communications and various malwares are installed .This encryption technique is used in wide range of industrial networks, rfid, sensor fusion and distributed networks. Two-Factor AKE protocols will satisfy the various characteristics such as security within high level vulnerabilities which has desynchronization attack-smart card is lost and obviously the very common dictionary attack, user anonymity, perfect secrecy. Neither of long-term public key nor of centralizing in passkey code storage, or change in user passkey code. Extended security is present only in our modified model. The scheme which is actually been already implemented has very small key length and easily managed in computations and generally depends on a very minute number of code flows. That is the reason why the protocol is manageable on pervasive applications on computer and mobile communications.

II. LITERATURE SURVEY

A. Session Password Generation

This scheme proposed complementary authentication using smart cards and passkeys within nature of computing.
This scheme provides mutual authentication of identity, verifying of the server platform and secure session key agreement. This scheme also provides much security protection for smart card users and the server, supports user identity anonymity, user password free changing and server platform trusted certificate updating. [1] Hwang and Li proposed a new remote user authentication scheme using smart cards. Smart Check Digits is used to generate a user authentication method which can be used remotely. The authors proposed authentication scheme using smart cards that is still vulnerable to the attack. This system provided the enough amount of security in the random oracle model. In fact the more analysis visualized that the proposed scheme follows all the suggested properties and deletes many security threats which are very tough to be defended at the same time in previous methods. This adverse model and criteria set an analysis for easy evaluation of future two-factor authentication generations.

B. RFID-based product information on the background of a privacy improved discovered service

The Electronic Product Code (EPC) global Networking acts as an upcoming globally accepted information architecture for major guidance to Radio-Frequency Identification (RFID) for various supplementary chains. Discovery of the services for the EPC global networking has been distributed among options. As logged in, users information will actually be in the interests of the EPC global Network, this could be used to create not only lists present in the inventory but also registrations of his physical environment and atmosphere and also different types of various intelligence required in business on the flow of different goods which can be applied and used in corporate world, protecting privacy of the client and that becomes immensely popular. A discovery which is highly enhanced for various protection and private service for RFID information can be prepared on the peer-to-peer logic to develop the confidentiality of the user’s question against registering by rehashing the search algorithms cryptographically which also includes

splitting and distribution of various service addresses of the interest. To enhance the secured proposal of one-time authentication by two factor method and passkey proposal in 2010 the complementary perfection and passkey agreement has been that is threatening to loss of attack to smart key, not getting forward security, and a securely improved proposal to eradicate these vulnerabilities. In this paper, we demonstrate that securely enhanced protocol is yet dangerous to the above attacks. Also, their proposal will not be able to eradicate attacks like session observed in parallel manner. Observing the complementary authenticating proposals using keys or cards is mostly possible for smart key lost attacks. We shall there by introduce a latest one-time authentication by two factor method and scheme for key agreement to eradicate these weaknesses. Understanding of a singular sign-On Working for Networks in distributed connected computers on a security basis. Singular sign-on (SSO) is a latest method of mechanism in an authenticated manner which will allow a legally sensed user with any singular part to be validated by various service distributors in a connected network. Chang and Le stated a new SSO proposal and provided its security in a well-organized securely based arguments. This is totally insecure because it failed to understand any sort of credential privacy and authentication in a soundless manner. To be specific, we provide two attacks which are in an impersonated manner. Firstly an attack will allow a virus infected service provider, who has already made communication with a legally sound user two times, to be able to gather the user's details and further to imitate the registrar to gain resource and service provided by others. Secondly, an outsider with no sort of any profile may able to use network services without any hassle by imitating any legally sound user or any non-existing user. This proposed method uses RSA signature for encryption.

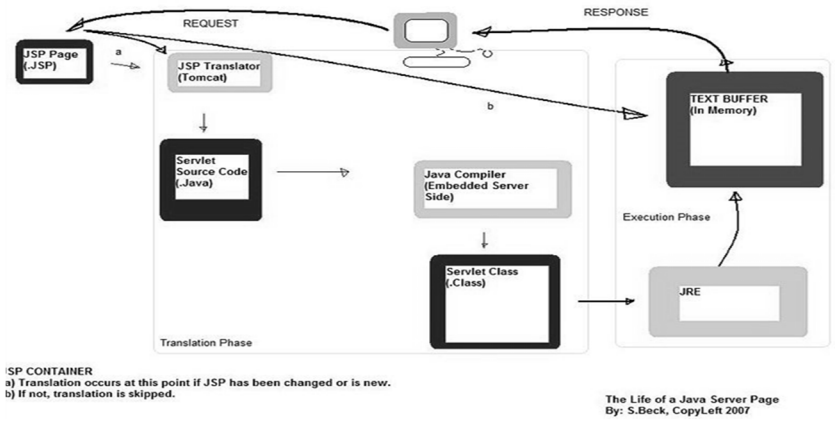
C. A platform based on P2P to provide distribution, collaboration and ubiquitous computation JXTA-OVERLAY.

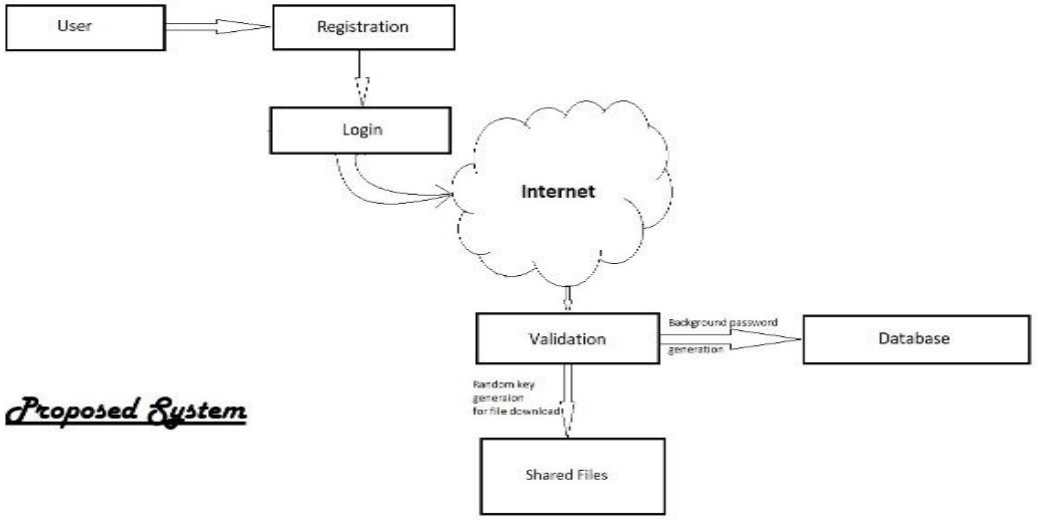
With rapid growth of Internet architectures and usage of huge-sized complicated applications in global industries, transportations, government organizations, health departments, and business industries there will be an increase in need to design and provide multi featured network applications. Various features of applications shall be inclusive of capability to be self-organized, decentralized, and to be able to use various types of assets like laptops, mobile devices, and also shall give us globally transparent, and security to resources. Also, applications shall be able to provide old forms of distributing computation and optimize various resources and also many forms of mutual activities, like learning, social networking in a secured atmosphere. In this journal, we shall provide the Overlay which is named as Juxtapose that is a JXTA- (P2P) platform manufactured for purpose to hold the possibilities in P2P technologies to provide distributions in systems. The architecture can be used in high enhanced computers and also in mutual activities by integration of the platform end device. This user interface and security problems will also to be tackled. We shall test the system by studying it in an experimental manner and visualize its useful part for high level processing in computations.

D. Implementation of RFID Mutual Authentication Protocol

Many research scholars have made us realize where (EPC) (C1G2) has major security issues. To eradicate such problems, some publishers have planned a design pad generator (PadGen) that will enhance security. The PadGen shall be able to provide a cover coded pad that shall cover the tag's passkey. In this the radio-frequency identification (RFID) tag–reader has been used for mutual authentication. The architecture of RFID protocols shall conform to the Standards based on International Protocols, named as EPC C1G2 RFID protocol and shall be provided. The usability of the strong agreements was successful in using an Altera DE3 board that shall comprise of an Altera Cyclone III field-programmable gate array.

III. SYSTEM ARCHITECTURE





A. RSA algorithm

It is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

1) Generating Public Key

Select two prime no's.
Suppose P = 53 and Q = 59.
First part of the Public key: n = P*Q = 3127.
Exponent say 'e' .
But e must be an integer.
Not be a factor of n.
$1 < e < \Phi(n)$

2) Generating Private Key

To calculate $\Phi(n)$:
Such that $\Phi(n) = (P-1)(Q-1)$
so, $\Phi(n) = 3016$
Calculate Private Key,
$d = (k*\Phi(n) + 1) / e$ for some integer k
For k = 2, value of d is 2011.
Hence the Public Key (n = 3127 and e = 3) and Private Key(d = 2011) are generated.

B. Proposed Method

The proposed method has

1) Session Grid algorithm
2) File upload and Encryption
3) Session based data sharing
4) File Decryption and Download

C. Session Grid algorithm

The session password is generated randomly based on the randomly generated grid. The grid is used as a medium for password generation. While registration the user must normally enter his username and password while registering into the system. Now the system stores this password and uses it to generate a unique session password while user logs in the next time. This session based authentication system uses the user password and compares alphabets contained alongside a 6*6 grid with letters a-z and numbers 0-9. The user needs to know the original password and the generation scheme to enter the exact password.

D. File upload and Encryption

Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

E. Session based data sharing

The users can view the files which are uploaded by them, then the users can share the files to the receiver by giving the time limit to accessing the data. Based on the time limit, the session key is generated for that file access. The key is only valid for that user given time, after the time limit the receiver have no access for that file.

F. File Decryption and Download

User requests the file by providing details and in response system replies with encrypted file. Before that the system will check the role and signature of the users whether the receiver have the same role as the sender mentioned. It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has correct role and signature, if it's correct, the original file gets decrypted for the receiver. This allows them to access information without authorization and thus poses a risk to information privacy.

G. Future Enhancement

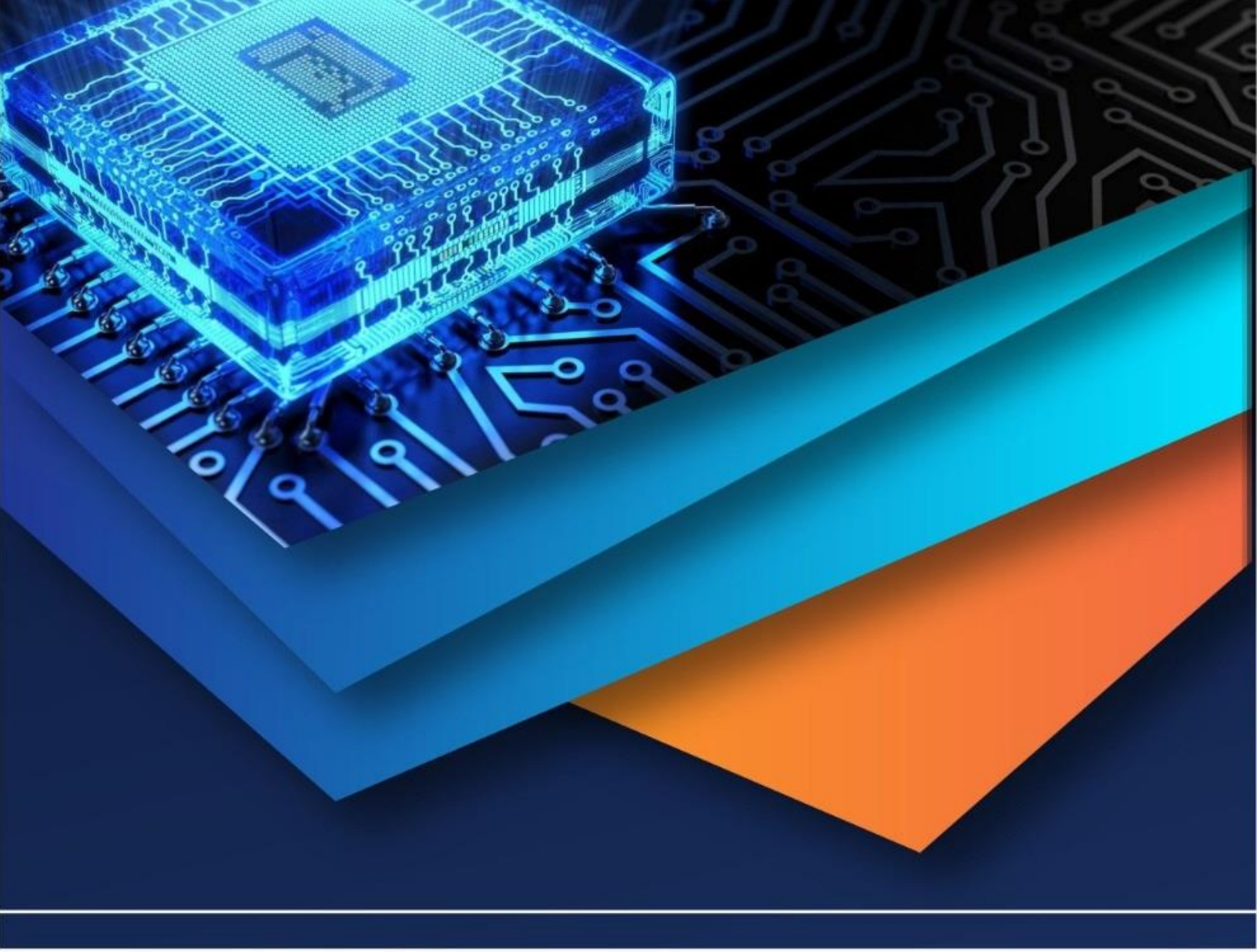
1) Optimal Algorithms for Complex Data Structures
2) Different Fusion Operators
3) Concurrent Updates on Backup Structures

IV. CONCLUSION

There are many techniques which are proposed for preventing shoulder surfing attack with all proposed techniques in the session based password scheme using shuffling keyboard with Pair Based method is more effective and secure to shoulder surfing attack, as this technique is providing a particular session password for every session or transaction Also, it is easy to use and handle in near future. This technique has scope to use in many fields for the security purpose. We shall describe a Random Two-Factor AKE scheme that will preserve security for the high level various vulnerabilities that will comprise of many de-synchronization attacks, lost smart card attacks and also guessing passkeys attacks. These possibilities will support many ways that comprises of perfect secret for forwarding anonymity, the adaptability to change the passkey code. Neither any sort of total storage of passkey codes, neither any sort of public key that is present in a long time manner. Moreover, our services will maintain high level of efficiency in comparison to need for storage, cost to communicate as well as computational complexity. Our services will require mostly a minute figure of flows in message and further the messages that are transmitted will be minute in size. The proposed agenda is probably the most secure in our figured and improved security model of AKE. This is the reason why the proposal is best suited for the launch in many low-power networks and also within industries of mobile and pervasive sort of computing networks.

REFERENCES

[1] Li Yang, Jian-Feng Ma, and Qi Jiang, "Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing", IEEE, 2012.
[2] A New Remote User Authentication Scheme Using Smart Cards with Check Digits, by Amit K. Awasthi and Sunder Lal (IEEE 2013)
[3] A. C. Weaver and M. W. Condtry, "Distributing internet services to the network's edge," IEEE Trans. Ind. Electron., vol. 50, no. 3, pp. 404–411, Jun. 2003.
[4] L. Baroli and F. Shafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing," IEEE Transa. Ind. Electron, vol. 58, no. 6, pp. 2163–2172, Oct. 2010.
[5] L. Lampord, "Password authentication with insecure communication," Comun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[6] W. B. Leee and C. C. Channg, "User identification and key distribution maintaining anonymity for distributed computer networks," Comput. Syst. Sci. Eng., vol. 15, no. 4, pp. 113–116, 2000.
[7] W. Juange, S. Chenn, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551–2556, Jun. 2008.
[8] X. Li, W. Qiue, D. Zhengr, K. Chene, and J. Liu, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," IEEE Transa. Ind. Electron., vol. 57, no. 2, pp. 793–800, Feb. 2010.
[9] A privacy enhanced discovery service for RFID-based product information, B. Fabian, T. Ermakova, and C. Muller
[10] Efficient Implementation of RFID Mutual Authentication Protocol, Y. Huang, W. Lin, and H. Li



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY