Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review Encryption/Decryption in SWiFi Network

Er. Gurleen Kaur, Er. Gurvinder Kaur
GGSCMT Kharar, Punjab,
India

Abstract— The Internet has emerged collectively of the foremost convenient and wide used media for exchanging info. The Internet of nowadays is Janus-faced with several challenges. one in every of the foremost discouraging challenges is to make sure security. Pursuing authentication through applicable mechanisms becomes a posh issue. Like different network applications, security problems became the core problems to be settled. Among different security problems, authentication and access control are the 2 main fields of security problems, that should be resolved to shield info and computing systems against unauthorized access. In this paper we have a tendency to reviewed numerous security technique that uses new coding and coding algorithms to attain authenticated communication and increased information integrity.

Keywords: SAML, WHO, HMAC, PGP

I. INTRODUCTION

Computer industry has created Associate in Nursing array of identification and authentication technologies like userID/Passwords, One Time word, Biometrics, Smartcards, Secure Socket Layer, light-weight Directory Access Protocol,
Security Assertion language (SAML), OpenID and CardSpace address variable business and security requirements [1]. every organization adopts one or a lot of these technologies to secure info against misuse and un-authorized access. during a networked setting, users area unit granted access to the network only if they provide their access info (e.g. User name
password) firmly to examine and validate their identity. If a person will prove that he's, additionally is aware of one thing that only he may is aware of, it's affordable to assume that someone is he WHO claims to be. the aim of non-public authentication is to make sure that the rendered services area unit being accessed solely by a legitimate user. All Network users aim to access info and transfer knowledge safely. To make sure secure transmission of data between the parties; a bunch of challenges should. We detain these challenges to 3 areas: knowledge Integrity, authentication and privacy. All Network users aim to access info and transfer knowledge safely. to make sure secure transmission of data between the parties; a bunch of challenges should met. we tend to confined these challenges to 3 areas: knowledge Integrity, authentication and privacy. Privacy refers to secure and valuable knowledge[2] that shouldn't be accessible unless the parties involved area unit allowed to try to thus. Several techniques is won't to maintain and improve user privacy like cryptography techniques [2], passwords and firewall. In Associate in Nursing unsecure setting, it's straightforward to interrupt through privacy in many ways in which. For example, viewing knowledge while not certificate, behavior scanning or movement [3] and eavesdropping. Recently, there's an effort to interrupt the privacy of the users on encrypted channels [4]. Integrity refers to the consistency and accuracy of information to make sure that unauthorized parties area unit prevented from modifying knowledge Authentication. As a result, the data which is received should be to be constant because the knowledge sent. protective knowledge transmission method is necessary to avoid any intentional or unintentional changes of those knowledge. Any injury or distort of knowledge can have an effect on the feasibleness of those data or information; it becomes not useful and not safe to use. Knowledge will use multiple techniques like coding, Digital signature and Checksum to avoid any injury or distort.
Authentication is that the method of supportive if a user or entity or device is WHO claims to be. In other words it's a mix of verification and Identification. Authentication falls into 3 categories [5]:

- information factors: one thing you recognize (e.g. Password, personal identification number)
- possession factors: one thing you have got (e.g. Smart Card, cell phone, ID card)
- immanence factors: one thing you're (e.g. fingerprint, signature, voice, iris, biometric).

To enhance security, differing kinds of authentication area unit combined. The client, host and transmission channel area unit the locations wherever authenticators is attacked. In this paper, we tend to propose a completely unique approach to reinforce the info integrity, authentication and privacy counting on some coding / decoding strategies by combining PGP, sWIFI and HMAC Systems. The projected system provides the protection and safety to secure knowledge transfer across network against spoofing, tampering, repudiation, security attacks and data disclosure.

© 2015, IJARCSSE All Rights Reserved

II. BACKGROUND

According to American Bankers, the HMAC could be a technique that uses cryptographic hash functions for message authentication. This system combines any iterative science with a shared secret key. The HMAC has 2 parameters, the message and a shared secret key that is thought solely to the sender and receiver. The sender uses HMAC to supply a worth that is represents the mix of the key

key and therefore the message input, the new price is named raincoat the sender appends the raincoat message and sends all to the receiver. The receiver uses HMAC and a shared secret key, that the sender used before, by applying the raincoat algorithmic rule to the received message and compares the result with the received raincoat. We are able to insure that the message has been correctly received if the 2 values match. This method conjointly provides assurance that the message comes from sender United Nations agency shares the key[6]. In their paper mentioned that solely the sender and receiver understand the hash operate which is employed by sender to hash message and manufacture the hash price, then the sender encrypts the resulting hash price by mistreatment science operate to form a message tag that is shipped to receiver with the message. On the receiver's aspect, the user has to verify that the receiver's tag is valid for the receiver message supported the hash operate and science key that are known solely to the sender and receiver. There are several steps to use sWIFI : initial, the sWIFI is split into 2 halfs: the primary part is that the plain text for key functions, the second half is split into four pieces; to get and write in code the key mistreatment logical OR-ing and bit shifting of the information during a sure pattern within the four parts. In order to get the key, write in code the primary half and disrupt the probabilistic phenomena of the letters within the language. Finally, at intervals the blocks the encrypted knowledge is shuffled to form certain that there is no similarity with original knowledge. Pretty sensible Privacy, is one of the most necessary secret writing and security applications that use economical and confidential algorithms to secure knowledge transmission. The PGP as a secret writing program supported by Phil Zimmerman on 1991 provides complete verification and secret writing for message files.

The PGP is taken into account the foremost key science employed by the general public with PGP during a secure manner therefore there's no would like for any specific infrastructure.The security of PGP Model is trusty since it's AN open supply therefore skilled individuals will close any weaknesses if found, it's supported symmetric-key cryptography and use combination of data compression, hashing and public-key cryptography. The PGP is that the initial successful try of a free science model that is accessible for the general public. The sender United Nations agency has the non-public key is able to produce a digital signature for corresponding public key. Digitally, PGP offers alternative users the power to sign certificates that they assume it's authentic, that the owner of the general public secret's an owner of the certificate. To verify a public key, the user has to check if there are any digital signatures that ar signed by the trusty users.

PGP compresses the message and creates a public key and a non-public key for the sender through cryptography computer code. once the plain text is encrypted, the general public secret's encrypted to the receiver's non-public key which might be employed by the receiver to decode the message[4].

Although the PGP is taken into account together of the simplest secret writing techniques, it will have some disadvantages. The PGP method is taken into account a posh method to use on an everyday basis since it is very troublesome for several individuals to know the which means of Cryptography. Also, The PGP could be a two way street that the sender and therefore the recipient should use it, otherwise the recipient won't be able to view the encrypted data. Managing keys for a brand new user mistreatment PGP are a challenge. Lost or corrupted keys cause high risk and can not permit users to look at encrypted data.

III. AUTHENTICATION TECHNIQUES

Cryptography provides a straightforward approach for the transmitter and receiver to outline a set of valid messages that the transmitter will construct and therefore the receiver will verify [10]. Two kinds of cryptosystems square measure available:-

i) personal key cryptosystems
ii) Public key cryptosystems: A a lot of ancient technique that enhances the 2 cryptologic methods is
iii) Biometric Systems

Private Key cryptosystems: rhombohedral secret writing (also known as private-key secret writing or secret-key encryption) involves victimisation constant key for secret writing and cryptography. secret writing involves applying Associate in Nursing operation (an algorithm) to the information to be encrypted victimisation the personal key to form them unintelligible. The slightest algorithmic program (such as Associate in Nursing exclusive OR) will create the system nearly tamper proof (there being therefore such issue as absolute security).

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. rhombohedral secret writing is based on the exchange of a secret (keys).

Public-key cryptosystems: Public-key cryptosystems also called uneven cryptography may be a category of cryptographic algorithms which needs 2 separate keys, one in every of that is secret (or private) and one in every of that is public. though completely different, the 2 elements of this key combine are mathematically coupled. the general public key's wont to encrypt plaintext or to verify a digital signature; whereas the personal key's wont to decipher cipher text or to make a digital signature. The term "asymmetric‖ from the utilization of different keys to perform these opposite functions, each the inverse of the opposite – as contrasted with standard ("symmetric") cryptography that depends on constant key to perform each.

© 2015, IJARCSSE All Rights Reserved

- Digital signatures: Digital signatures within which a message is signed with the sender's personal key and may be verified by anyone UN agency has access to the sender's public key. This verification proves that the sender had access to the personal key, and so is probably going to be the person associated with the general public key. This additionally ensures that the message has not been tampered with, as any manipulation of the message can lead to changes to the encoded message digest, that otherwise remains unchanged between the sender and receiver.
- Hash Functions: A cryptologic hash perform is a hash perform that is taken into account much impossible to invert, that is, to recreate the input file from its hash price alone. These unidirectional hash functions have been known as "the workhorses of contemporary cryptography". The input file square measure typically known as the message, and therefore the hash value is usually known as the message digest or just the digest. The ideal cryptologic hash perform has four main properties:
  - it's simple to figure the hash price for any given message
  - it's impossible to come up with a message that incorporates a given hash
  - it's impossible to change a message while not changing the hash
  - it's impossible to search out 2 completely different messages with constant hash.

Cryptographic hash functions have several info security applications, notably in digital signatures, message authentication codes (MACs), and alternative kinds of authentication. they'll even be used as standard hash functions, to index knowledge in hash tables, for procedure, to notice duplicate knowledge or unambiguously establish files, and as checksums to notice accidental knowledge corruption. Indeed, in information security contexts, cryptologic hash values are generally known as (digital) fingerprints, checksums, or just hash values, although of these terms symbolize more general functions with rather completely different properties and purposes.

IV. CURRENT SECURITY SOLUTIONS FOR DATA SECURITY AND PRIVACY PROTECTION

IBM developed a totally similarity encoding theme in June 2009. This theme permits knowledge to be processed while not being decrypted [12].Roy I and Ramada applied localised info flow management (DIFC) and differential privacy protection technology into knowledge generation and calculation stages in cloud and place forth a privacy protection system referred to as air vat [13]. this technique will forestall privacy escape without authorization in Map scale back computing method. A key downside for encryption solutions is key management. On the one hand, the users haven't enough experience to manage their keys. On the opposite hand, the cloud service suppliers have to be compelled to maintain an oversized range of user keys. The OASIS and Key Management ability Protocol (KMIP) is making an attempt to retort such problems [14]. concerning knowledge integrity confirmation, the information communication, transfer fees and time price, the users cannot 1st transfer knowledge to verify its correctness then transfer the information. And because the knowledge is dynamic in cloud storage, ancient knowledge integrity solutions aren't any longer appropriate.NEC Lab's demonstrable knowledge integrity (PDI) resolution will support public data integrity verification.Cong Wang planned associate arithmetic methodology to evidence the integrity of the information dynamically store within the cloud. Within the knowledge storage and use stages, Mow bray planned a client-based privacy management tool. It provides a user central trust model to assist users to manage the storage and use of their sensitive info within the cloud. Munts-Mulero mentioned the issues that existing privacy protection technologies like K anonymous, Graph Anonymization, and knowledge preprocessing methods long-faced once applied to massive knowledge and analyzed current solutions. The challenge of information privacy is sharing knowledge whereas protective personal privacy info. It planned privacy protection framework supported info responsibility (IA) parts [19]. The American state agent will establish the users World Health Organization square measure accessing info and therefore the sorts of info they use. once inappropriate misuse is detected, the agent defines a group of ways to carry the users answerable for misuse. About data destruction,U.S.Department of Defense (DoD) 5220.22- the National Industrial Security Program operative Manual shows 2 approved ways of information devastation protection, however it doesn't give any specific needs for a way these 2 ways square measure to be achieved [20].The National Institute of Standards and Technology (NIST) Special journal [21], 800-88,gives a "Guidelines for Media Sanitization" .

V. DATA SECURITY AND PRIVACY PROTECTION ISSUES

The substance knowledge|of knowledge|of information} security and privacy safety in cloud is analogous thereto of standard data security and privacy protection. it's additionally concerned in each stage of the information life cycle. however due to directness and multi-tenant characteristic of the cloud computing, the substance of knowledge security and privacy protection in cloud has its particularities.

The which means adopt by Organization for Economic Cooperation and Development (OECD) [11] is any info regarding associate known or distinctive individual information subject. Another accepted definition offer by the yankee Institute of Certified Public Accountants (AICPA) and therefore the Canadian Institute of leased Accountants (CICA) within the usually Accepted Privacy Principles (GAPP) standard is "The rights and obligations of people and organizations with relevance the cluster, use, and disclosure of individual information".

Data Life Cycle

Data life cycle refers to the complete method from generation to destruction of the information. the information life cycle is divided into seven stages. See the figure below:

© 2015, IJARCSSE All Rights Reserved

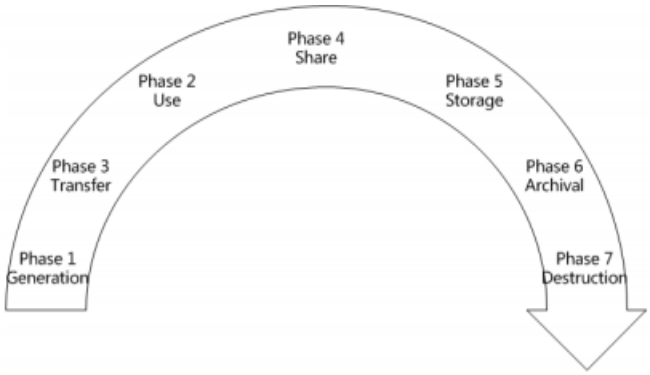

Figure 1: Data life cycle

A. information Generation

Data generation is concerned within the information possession. within the ancient IT setting, sometimes users or organizations own and manage the info. however if information is to be migrated into cloud, it ought to be thought of that how to maintain the info possession. non-public} private data, information homeowners are entitled to grasp what personal data being collected, and in some cases, to prevent the gathering and use of private data.

B. Transfer

Within the venture boundaries, information broadcast sometimes doesn't need encoding, or simply have a simple encryption quantify. For information broadcast across enterprise borders, each information privacy and integrity ought to be ensured so as to forestall information from being broached and tampered with by unauthorized users. In alternative words, solely the info encoding isn't enough.

Data integrity is additionally required to be ensured. th7us it ought to make sure that transport protocols offer both confidentiality and integrity. Confidentiality and integrity of information transmission got to guarantee not solely between enterprise storage and cloud storage however additionally between totally different cloud storage services. In other words, privacy and integrity of the full transfer procedure of information ought to be ensured.

C. Use

For the static information employing a easy storage service, like Amazon S3, encryption is possible. However, for the static information utilized by cloud primarily based applications in PaaS or SaaS model, encryption in several cases isn't possible as a result of encryption can cause issues of compartmentalization and question, the static information used by Cloud-based applications is mostly not encrypted. Not solely in cloud, however additionally in typical IT environment, the info being treated is sort of not encrypted for any program to arrangement with. Due to the multi-tenant feature of cloud computing models, the info being processed by cloud- primarily based applications is stored in conjunction with the info of alternative users. Unencrypted information within the methodology may be a grave threat to information security.

Regarding the utilization of private information, things ar a lot of problematical. The homeowners of personal information got to specialise in and guarantee whether or not the utilization of private data is consistent with the needs {of data|of data|of knowledge} assortment and whether or not personal information is being shared with third parties, for instance, cloud service suppliers.

D. Share

Data sharing is obtaining larger the utilization vary of {the information|the info|the information} and render data permissions extra complex. the info homeowners will allow the info admittance to at least one party, and successively the party will a lot of portion the data to a different party while not the consent of the info owner. Therefore, throughout information sharing, especially when information shared with 3rd party, the info owner need to think about whether or not the third party continues to take care of the initial protection measures and usage restrictions. Allotment of individual data, additionally to authorization of information, sharing coarseness all {the information|the info|the information} or partial information and data transformation are also got to be troubled regarding. The sharing coarseness depends on the sharing policy and therefore the division granularity of content. {the information|the info|the data} transformation refers to analytic sensitive information from the initial data. This procedure makes the info isn't relevant with the facts owner.

E. Storage

The data within the cloud could also be divided into:

(1) the info in IaaS setting, like Amazon's easy cupboard space Service;
(2) the info in PaaS or SaaS setting interconnected to cloud- primarily based applications.

The data hold on within the cloud storages is expounded with those hold on in alternative living-room and desires to mirror on 3 aspects of knowledge security: confidentiality, integrity and handiness. The acquainted clarification for information privacy is encryption. So as to make sure the effective of encoding, there must consider the utilization of

© 2015, IJARCSSE All Rights Reserved

along encoding algorithmic program and key strength. because the cloud computing setting involving giant amounts of information communication, cupboard space and usage, there additionally must take into account processing speed and procedure potency of encrypting great amount of information.

In this case, for instance, regular encoding algorithmic program is a lot of appropriate than uneven encoding algorithm .one more key crisis regarding encryption is essential oversight. Is United Nations agency accountable for key management? Ideally, it's the facts owner. aside from at here, as a result of the shoppers haven't adequate capability to supervise the keys, they often fork up the key administration to the cloud suppliers. Cloud providers got to carry on keys for an oversized variety of users; key managing can become harder and difficult. additionally to information privacy additionally must be anxious regarding information integrity. once the users place many GB or a lot of information into the cloud storage, they the way to check the responsibleness of the data? As swift smoothness characteristic of cloud computing property, the users don't grasp wherever their information is being hold on. To move around out of or into the cloud storage can consume the user's network utilization (bandwidth) associated an amount of your time. Some cloud supplier like Amazon need users to pay transmit quantity the way to brazenly verify the integrity of information in cloud storage room while not having to initial transfer the info then transfer the info is a nice challenge. the info is active in cloud storage room, the normal technologies to ensure information integrity may not be effective. within the ancient IT setting, the most threat of the info handiness comes from external attacks. within the cloud, however, additionally to external attacks, there are many alternative areas which will threat the info availability:

(1) the provision of cloud computing services;
(2) whether or not the cloud suppliers would still operate within the future?
(3) whether or not the cloud storage services offer backup?

F. Archival

Archiving for information focuses on the storage media, whether or not to supply offsite storage and storage period. If the data is store on convenient media then the media is out of management, the info are probably to require the risk of outflow. If the cloud service supplier don't offer offsite archiving, the provision of the data are vulnerable. Again, whether or not storage period is in keeping with repository requirements? Otherwise, this may lead to the provision or privacy threats.[15]

G. Destruction

When the info isn't any longer needed, whether or not it's been fully destroyed? because of the physical characteristics of data-storage medium, the info deleted should still exist and may be improved. this could lead to inadvertently disclose of sensitive data.[16]

VI. CONCLUSION

In this paper, we have a tendency to given the authentication techniques. This system may be a pattern recognition system within which someone is recognized supported options derived from specific psychological or behavioural characteristics that the person possesses, that are tougher to be felony or purloined. In the future, we have a tendency to planned to explore literature and implement the authentication technique.

REFERENCES

[1] Payal P. Kilor, Pravin.D.Soni, "Quantum Cryptography: Realizing next generation information security", International Journal of Application or Innovation in Engineering & Management(IJAIEM), ISSN 2319-4847, Vol. 3, Issue 2, February 2014

[2] Shadi R. Masadeh, Ahmad Azzazi, Bassam A. Y. Alqaralleh, Ali Mousa.Al Sbou, "A NOVEL PARADIGM IN AUTHENTICATION SYSTEM USING SWIFI ENCRYPTION/DECRYPTION APPROACH", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[3] Amandeep kaur, Shailja Kumari, "Secure Database Encryption in Web Applications", International Journal of Advanced Research in Computer and Communication Engineering,ISSN (Online): 2278-1021, ISSN (Print): 2319-5940, Vol. 3, Issue 7, July 2014

[4] Snehlata V. Gadge, "Analysis and Security based on Attribute based Encryption for data Sharing", International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359, Vol. 3, Issue-3, March 2014

[5] Vinh Hoa LA, Ana CAVALLI, "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY", International Journal on AdHoc Networking Systems (IJANS), Vol. 4, No. 2, April 2014

[6] Sweety R. Lodha, S. Dhande, "Web Database Security Techniques", International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, Issue 3, March 2014

[7] Li Chen, Xingming Sun, Zhihua Xia, Qi Liu, "An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data", International Journal of Security and Its Applications, Vol. 8, No. 2, 2014, pp. 323-332

[8] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Mohsin Iftikha, "A Survey about the Latest Trends and Research Issues of Cryptographic Elements", International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 8, Issue 3, No. 2, May 2011

© 2015, IJARCSSE All Rights Reserved

[9] Annapoorna Shetty, Shravya Shetty K, Krithika K, "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm", International Journal of Innovative Research in Computer, ISSN (Print): 2320-9798, Vol.2, Special Issue 5, October 2014

[10] Mupnesh Kumari, Priyanka Sharma, "Privacy Preserving using Homomorphic Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 4, Issue 7, July 2014

[11] Alok Kumar Shukla, V. Kapoor, "Data Encryption and Decryption using Modified RSA Cryptography Based on Multiple Public Keys and 'n' Prime Number", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Vol. 3, Issue: 6, June 2014

[12] T. Sivasakthi, N Prabakaran, "Algorithm of User Authentication for Data Security in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): 2320-9798, Vol. 2, Issue 2, February 2014

[13] Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap, "AES Algorithm Using 512 Bit Key Implementation for Secure Communication", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): 2320-9798, Vol. 2, Issue 3, March 2014

[14] Ritu Pahal, Vikas kumar, "Efficient Implementation of AES", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 7, July 2013

[15] Saranaya K, MOHANAPRIYA R, UDHAYAN J, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 3, Issue 3, March 2014

[16] Srinivas B.L, Anish Shanbhag, Austin Solomon D'Souza, "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): 2320-9798, Vol.2, Special Issue 5, October 2014

[17] Prabhat Kumar Singh, Gajendra Singh Chandel, "A Modified Technique For Performing Data Encryption & Data Decryption", ISSN : 2248-9622, Vol. 4, Issue 7(Version 5), July 2014, pp.149-152

[18] Bonny B Raj, Panchami V, "DNA Based Cryptography Using Permutation and Random Key Generation Method", International Journal of Innovative Research in Science, Engineering and Technology, ISSN(Print): 2347-6710, Vol. 3, Special Issue 5, July 2014

[19] Neha Garg, Partibha Yadav, "Comparison of Asymmetric Algorithms in Cryptography", IJCSMC, ISSN 2320–088X, Vol. 3, Issue. 4, April 2014, pg.1190–1196

© 2015, IJARCSSE All Rights Reserved