ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Enhanced Security through Token's

Rahil Amin Bhurani[1], Dr. K.P.Adhiya[2], Prof. Dr.Girish K. Patnaik[3]

M.E. Student, Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon(M.S.), India[1,]

Associate Professor, Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon(M.S.), India[2,]

Professor and Head, Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon(M.S.), India[3,]

ABSTRACT: Previously, computer applications was not designed with security in mind, but because of the increasing frequency and sophistication of malicious attacks against information systems, modern software design methodologies include security as a primary objective. With Server Computing to meet multiple objectives such as cost, performance, reliability, maintainability, and security, trade-offs have to be made. Any server is vulnerable to an attacker with unlimited time and physical access to the server. Additionally, physical problems could cause the server to have down time.The increasing network bandwidth and reliable flexible network connections make even possible for users to obtain high quality services from data and software that completely resides on data centers. The main goal is to ensure the data integrity and security. To maintain the data securely in distributed environment, Token Generation algorithm in a distributed environment for data files checking is as a secure and dependable Server storage service. A new token generation scheme is suggested to encrypt the user with specified key parameters to make the resource more robust. Token generation scheme will add security for not only authentication but also authorization.

KEYWORDS: Attacks; Security; Threats; Authentication; Token GenerationAlgorithm

I. Introduction

Every person in the world has a trust on web based applications. The world is now-a-days turning digital and the people started storing and sharing their personal data on internet assuming that information is more secured on internet as compared to the handwritten documents. With the increase in popularity of the Internet the number of frauds and abuses is literally exploding. But the information stored in digital form on web is easily accessible to anyone. Man in Middle attack is a kind of eavesdropper attack [13]. The protection of digital identities is getting more and more crucial.The rapid growth in the number of online services leads to an increasing number of different digital identities each user needs to manage. But passwords are perhaps the most common type of credential used today. To avoid the tedious task of remembering difficult passwords, users often behave less securely by using weak passwords. The systems today completely rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use passwords which are easy to guess and using the same password in multiple accounts or store them on their systems, etc. Moreover passwords can be written down, forgotten and stolen, guessed deliberately being told to other people.

Large amount of data is generated due to applicationsare needed to be stored which requires large amount of storage space. Data generation is currently outpacing storage availability, hence, there will be more and more need to outsource data. Server computing provides the storage and supports for outsourcing of data without having the local copy of data or files. However an important problem is to prevent unauthorized modifications [12]. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary.Various strategies for usingpasswords have been proposed by researchers out of which are very difficult to use and others might not meet the security concerns. Some solutions have been developed to eliminate the need for users to create and manage passwords.

To maintain the data integrity and data availability researcher's proposed several algorithms and methods, Thereby servers are not only used to store data like a warehouse, it also provides frequent updates on data by the users.Strong authentication solutions requires two identification factors, in addition to first factor is as follows "something you

DOI: 10.15680/IJIRCCE.2016. 0412028

know" represented by password it is introduced a second factor which is as follows"something you have" in the form of security token. The main purpose of token generation algorithm is to ensure the data integrity and security. The suggested scheme of Token generation algorithm which is simple and secure method and less overhead due to few parameters that has to be considered.Challenge verification scheme designed in easy and efficient way to prevent data from Man in middle attacks and data dependability detection or detect data errors on blocks.Servers ensure that the tokens were saved successfully without block modifications. This can be achieved by two way token checking and verification which results more robust and ensure that data will not be modified.

Section 2 describes Literature Survey based on token generation algorithm used in various domains. The solution based on LiteratureReview and analysis of problems in token generation algorithms is given in Section 3. Section 4 gives the conclusion implicating benefits ofsolution.

II. Literature Survey

To enhance security using token generation algorithm in domains such as Privacy, Secure Data De-Duplication, are described below in literature survey represented as a structure in fig: 1. Privacy enhancing attribute-based credentials allows users to obtain credentials from an issuer, by which the issuer assigns a list of certified attribute values to the user. Users can then use these credentials to authenticate to verifiers, but have the option to disclose only a subset of the attributes; all non-disclosed attributes remain hidden from the verifier. In next domain, to make data management scalable in cloud computing, data de-duplication is one of the important compression techniques for eliminating duplicate copies of repeating data. In previous encryption systems, identical data copies will lead to cipher texts after encryption, making de-duplication impossible. New de-duplication algorithms supporting authorized duplicate check in hybrid cloud using token number and privilege key.

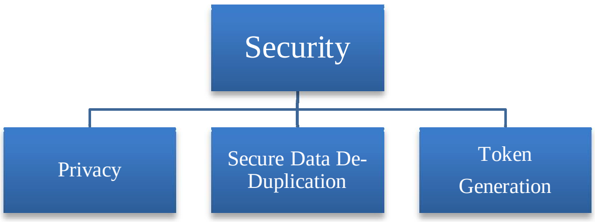

Fig.1: Structure of Literature Survey

Jan Camenischetal.,in [1], proposed a practical scheme to apply the data minimization principle, when the verifiers' authentication logs are subjected to external audits and extended PABC scheme in which verifier further remove attributes from presentation tokens before handing them to an auditor.The Advantage of this scheme is Audited tokens can be linked to the presentation from which they were derived which can be used as a feature when the verifier must be unable to initiate the number of presentations that it performed, and it also is a privacy drawback.

Sohil Sharma etal.,in [2], proposed a concept of Two Layer Encryption techniques in which the user performs the coarse grained encryption which reduces the costs on user side while the Server provides fine grained encryption techniques which ensures the confidentiality of the system as well as also reduces costs on user side.The proposed system is to provide user with a safe and secure environment in public clouds to ensure that user receives benefits incurring costs. Using the proposed system the confidentiality of the data will be totally ensured. Hence using the proposed system there is decentralization of attributes and no interference of roles as there was in previous kinds of algorithms. Because encrypting data on user side incurs high computational costs but load increases on server side result in a drawback.

Twinkle Graf.F and Prema.P,in [3],proposed a privacy preserving symmetric key block algorithm for the Server database to enhance the security in Server environment where data is shared and stored and transferred through which collaborative learning is performed. Authenticated users whose pre computed code will be equal to the signature value generated by the server is allowed to view data on the server.The author proposes a novel public verifying mechanism for the integrity of shared data with efficient user identification. By utilizing signatures, it allows the cloud to re-sign blocks on behalf of existing users during user revocation and a public verifier is able to verify the integrity of shared data without retrieving the entire data from the cloud. Thereby lacks a solution of security because it allows two or more parties to collaboratively conduct the updating on data which is arbitrarily partitioned between them.

HimikaParmar et al., in [4], proposed an image based authentication scheme on the base of pre-chosen categories of grid of pictures to eliminate the need of text passwords and to generate OTP Token for authorized user after image authentication using Hash Message Authentication Code HMAC based technique.A hash-based OTP starts with the input parameters as synchronization value, username, password, and encrypt them through the cryptographic hash function, which produces the fixed-length password, in the form of OTP. The OTP operates in two modes of delivery text messaging as well as Email services, also has a drawback of spam in the form of email. The Proposed algorithm uses the Time Synchronized OTP Values to generate the token, and has drawback of expiring the token if the session is expired.

Deepali C. Ghosalkar,in [5], proposed convergent encryption technique to enforce data confidentiality while making deduplication feasible because data deduplication at server storage reduces the amount of storage space and saves bandwidth.The proposed system encrypts as well as decrypts a data with a convergent key, is obtained by encrypting the hash value of the content of the data. After key generation and data encryption, users retain the keys and send the ciphertext to the cloud. The proposed Encryption scheme is deterministic which is derived from data content has a drawback of data modification.

AparnaAjitPatil and DhanahreeKulkarni,in [6], proposed a concept of token generation using convergent key for block level data duplication in hybrid cloud systems which uses authorized duplicate check which gives confidentiality of data incurring minimum overhead but with non-web interface. The proposed system encrypts data with a convergent key, the content of the data obtained by computing the cryptographic hash value. After the data encryption and key generation process user retain the keys and send the cipher text to the cloud. The encryption operation is determinative and derived from the data contents, same data copies will generate the same convergent key and hence the same cipher text. A secure proof of ownership protocol is provided to prevent the unauthorized access.

Xin Jin etal., in [7], proposed of Attribute based access control where access requests are evaluated based on the attributes of cloud users and those of objects such as virtual machines, storage volumes, networks, due to lack of flexible model to accommodate diverse policy requirements, the CSP needs a flexible model to accommodate diverse policy requirements, though the scheme proposed is suitable for server model not for administration model.

S.B.Patil et al., in [8], proposed a de-duplication system by using the concept of hybrid cloud which is a combination of public and private cloud. In this paper to perform duplicate check user request token from private server. Tokens are generated for each file and every file. If user wants to upload a file an authorized duplicate check is performed by public cloud. If user uploads the file having same name and same contents then such file gets delete from the storage. The drawback of this scheme is that for uploading every file user has to generate token that means multiple tokens are generated for multiple files , hence storing multiple token on the cloud increases he storage.

MadhuriGhodke etal., in [9], proposed a concept of token Generation of token for sharing with other users with privileges for avoiding duplication of data at server side. According to authorexisting system shows that each user will be issued by private keys for their corresponding privileges andthese private keys can be used to generate file token for duplicate checking. However, during file uploading, the user needs to use generated file tokens to share with other users with privileges. To compute these file tokens, the user needs to know the private keys. This restriction leads the authorized de-duplication system unable to be widely used and limited. According to author this failure can be overcome by implementing block level de-duplication which eliminates duplicate blocks of data that occur in non-identical files.Eliminating duplicate copies of repeating data to save storage can be managed by data de-duplication which is a specialized data compression technique.The proposed scheme Removes duplication and gives secured access control but taking user privileges lacks security and generated token can be cracked.

P.Srinivas and K. Rajesh Kumar, in [10], proposed a concept of Secure Data transfer in Cloud Storage Systems using Dynamic Tokens. Users access the cloud based applications with the help of the web browsers with internetconnection. Data stored at clouds are maintained by Cloud service providers with various incentives at different levels of services. Though it eliminates the responsibility of local machines to maintain data, there are chances to lost data or it effects from external or internal attacks. Due to Increased bandwidth and less reliable network connections in cloud authors proposed a scheme of Flexible distributed scheme with token generation algorithm for data stored in cloud which is highly efficient against data modification attack and gives Secure and dependable server storage service but no block storage implemented because block storage on clouds will give better results easily distribute the blocks to different cloud servers for more availability of data.

BhagyashreeAlhat and Amar Buchade, in [11], proposed a concept of token generation and replacing the token by hash value. In cloud storage data is stored in a distributed manner at different servers. Users can remotely store their data in cloud storage without having physical possession of the outsourced data, which encounters security risks in integrity, correctness and availability of the data in the storage system. In distributed storage, data is divided into blocks and these blocks are kept at different servers. These blocks are assigned with token to achieve security. In this paper, author proposed a system which replaces these tokens with hash values. While storing a data in cloud with unique identification is divided into blocks. These tokens are used in detection of error and recovery of data. After token generation and replacing token by hash value using Secured Hash Algorithm (SHA1) is better for achieving more security which is efficient against server crash attacks. But every time token changes due to rapidly changing data.

BhartiDhote and A.M.Kanthe, in [12], proposed a scheme is to build efficient data security model which supports for Data Integrity, to ensure the user’s data is correct and stored in cloud server, effectively locate the server on which data has been modified by unauthorized user, support for the dynamic data like append, delete, insert, update while retaining the same storage correctness and uses token generation algorithm to pre-computes the verification tokens. Any cloud server is vulnerable to an attacker with unlimited time and physical access to the server. This would be a loss of availability. The drawback of this system is upload time and download time of token while pre computation of individual block of server.

The Review states that Server is responsible to protect data from threats. Once the server is compromised, the data is polluted with fraudulent data and users fails to get the original data from the Servers.Thus, all above works suggested by researchers have included auditing, token generation in many different ways. Also various works have been done on token generation, but the major problem still persists. Generation of token with high level of security is still a major concern. All previous work focus on token generation for authentication but token generation for authorization needs to be resolved and an alternative solution required to existing authentication schemes like OTP solutions which requires extra hardware and therefore put an extra burden on user and also impose cost on service providers.

III. Proposed Solution

To ensure the security and dependability for Server data storage, the aimto design a token generation algorithm for dynamic data verification and operation and achieve the following goals [17]:

(a) Storage correctness: to ensure users that their data are indeed stored appropriately and kept intact all the time at the server.

(b)Fast localization of data error: to effectively locate the malfunctioning server when data corruption has been detected.

(c) Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the server.

(d) Dependability: to enhance data availability against malicious data modification and server colluding attacks, i.e. minimizing the effect brought by data errors or server failures.

(e) Lightweight: to enable users to perform storage correctness checks with minimum overhead.

To resolve the issues of token generation for authentication as well as authorization, some schemes have to be introduced for both servers and clients.To achieve data storage correctness and data integrity, token generation takes a fewparameters in the form of question and answers given by the authenticated user and uses attribute based parameters and compute the token.Data Synchronization is allowed with token verification. Server is responsible to generate token and stores the token persistently and securely for further verification.

To achieve data storage correctness and data integrity, suggested token generation takes a few parameters in the form of question and answers and uses attribute base parameters and compute the token. As token generation is generated at server side, it is difficult to reveal the generation algorithm or scheme. After generating token, token will be ensuring correct answers from authenticated and authorized users. Every user needs to authenticate by providing correct answers. Compromised Tokens retrieved by attackers will also go through the authentication and authorization phase, so the attacks would be nullified with this.

The suggested solution of token generation algorithm generates a token by taking the input data from users in the form of question and answers. After taking input from user the token generated in the form of question of which user knows the answer. By providing the correct answer in challenge verification step by algorithm the user is authenticated with server and the starts synchronization with server which is represented in the below figure: 2.

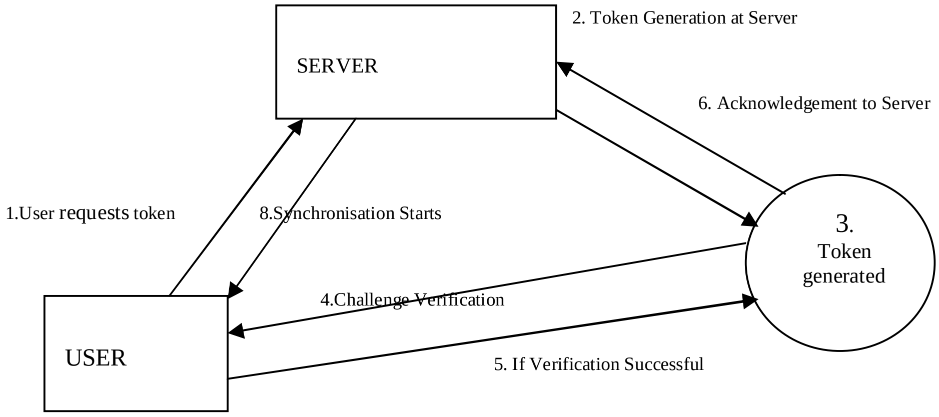

Fig. 2: Token Generation Steps

The Working of Token generation Algorithm shown above in fig.2 is as follows. Initially the user request token to server by providing input data in the form of question and answers. Taking the input token generation is processed at server side and requested token is given to user. When user accesses the token, the token request the answer followed by the question to the user. Hence the authorized user who has provided input for token generation can give the answer and the synchronization starts. Hence the user is authenticated with the server.

Various steps involved for securing client server environment using token generation observed as:

(a) Token generation algorithm using question and answers as an input to generate token with additional attribute based policies is a secure method and less overhead due to few parameters that has to be chosen.
(b) Challenge verification scheme was designed in easy and efficient way to prevent data from Man in middle attacks and data dependability detection.
(c) Servers ensure that the tokens were saved successfully without block modifications. This can be achieved by two way token checking.
(d)Token generation algorithm is very cost effective as it does not require any costly certification.
(e)It requires very less time consuming process as itperform simple and easy results.
(f) It reduces the threat on confidentiality as it stops the disclosure of data from attackers.
(g)In case token in stolen, deleted or misplaced by any outsider, will to unable to access the victims account.

IV. CONCLUSION

In this paper, review says that there is a problem of data security in server storage systems. To ensure the correctness of user's data in storage systems scheme of the token generation using attributes base parameters by the user ensures that the token is generated securely by server. Hence was sent to the server with the purpose of addressing shortcomings of existing authentication solution. The generation of token and storing it to Server ensures confidentiality of data. Data storage on server provides better performance and can easily distribute the data to different Server for more data availability. Data Synchronization is easily possible simply by challenge verification of token and utilizing the token with distributed verification achieves the integration of storage correctness insurance and data error localization.

REFERENCES

1. Jan Camenisch, Anja Lehmann, Gregory Neven, and Alfredo Rial, Privacy-Preserving Auditing for Attribute-Based Credentials, 'IBM Research, Zurich, Switzerland'.
2. Sohil Sharma, VivekPeherwar, ArushiVarma, ParjeetKode, andTheresBemila,'Preserving Security In Clouds using ABAC Policies', International Journal of Engineering and Science and Computing, (IJESC), Volume 6, Issue 4, pp. 3581-3583, 2016.
3. Twinkle Graf.F, Mrs.Prema.P, 'Secure Collaborative Privacy in Cloud Data with Advanced Symmetric Key Block Algorithm', International Journal of Computer Science and Engineering (SSRG-IJSCE), Volume 2, Issue 2, pp.45-49, 2015.
4. HimiksParmar, Nancy Nainan, and SumaiyaThaseen, 'Generation of Secure One-Time Password Based on Image Authentication', pp.195-206, 2012.
5. Deepali C. Ghosalkar, 'Implementation Idea for Secure Data DE duplication Using Hybrid Cloud Approach', International Journal ofComputer Science Trends and Technology(IJCST), Volume 4, Issue 1, pp. 136-139, Jan-Feb2016.
6. AparnaAjitPatil and DhanshreeKulkarni,'Block level Data Duplication on Hybrid Cloud Storage System', International Journal ofAdvanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 5, Issue 8, pp. 340-345, 2015.
7. Xin Jin, Ram Krishnan and Ravi Sandhu,'Role and Attribute Based Collaborative Administration of Intra-Tenant Cloud IaaS', International Journal of Computer Networks (IJCN),Volume 3, Issue 3, pp. 159-166,2011.
8. S.B.Patil, YashodaA. Kumbhar, and Swapnali Mane, 'Data Deduplication Using Hybrid Cloud', International Research Journal of Engineering and Technology (IRJET), Volume 2, Issue 7, pp. 1009-1012, 2015.
9. MadhuriGhodke, PriyankaBais, AbhirupaSaha, Poonam Singh, and Prof. G.M.Gaikwad, 'Securely Eradicating Duplication by Generating File Tags and Tokens over Hybrid Cloud Using Security Algorithm', International Journal of Advanced Research in Computer Communications Engineering, (IJARCCE), Volume 5, Issue 3, pp. 151-153, 2016.
10. P. Srinivas and K. Rajesh Kumar R,'Secure Data transfer in Cloud Storage Systems using Dynamic Tokens',International Journal of Research inComputer and Communication Technology, (IJRCCT), Volume 2, Issue 1,pp. 6-10 ,2013.
11. BhagyashreeAlhat and Prof Amar Buchade, 'Revisiting Secure Cloud Storage by Replacing token Generation with SHA',International Journal of Advance Foundation And Research In Science & Engineering, (IJAFRSE), Volume 1, Issue 12, pp. 14-20, 2015.
12. BhartiDhote and A.M. Kanthe, 'Secure Approach for Data in Cloud Computing', International Journal of Computer Applications, Volume 64, Issue 22, pp. 19-24, 2013.
13. Jesudoss A. and Subramannium N.P, 'A Survey n Authentic Attacks and Countermeasures in a Distributed Environment', Indian Journal of Computer Science and Engineering, (IJCSE), Volume 5, pp. 71-77, 2014.
14. Ming Li and Keishi Tajima,'Automatic Generation of Authentication Question from Private Messages', IEEE/WIC/ACM/International Conference on Web Intelligence Intelligent Agent Technology, pp. 505-510, 2015.
15. Hacker Intelligence Initiative, 'Man in the Cloud Attacks (MITC)', IMPERVA, 2015.
16. I Gede N. AgungJayarana,A.A.Kt.Agungcahyawan and Gasti Made AryaSasmita, 'Dynamic Mobile Token for Web Security using MD5 and OTP Method', International Journal of Computer Applications, Volume 55, Issue 6, pp. 1-6, 2012.
17. ManavSinghal and ShahsikalaTapasvi, 'SoftwareToken Based Two Factor Authentication Scheme', Volume 2 , Issue 3, pp. 383-386. 2012.

BIOGRAPHY

Rahil Amin Bhurani is a Student pursuing M.E (Computer Science and Engg) Final Semester in Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon(M.S.),India.

Dr. K.P. Adhiyais an Associate Professor in Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon(M.S.),India.

Prof. Dr.Girish K. Patnaik is an Professor and Head in Department of Computer Engineering, SSBT's COET, Bambhori, Jalgaon(M.S.),India.

DOI: 10.15680/IJIRCCE.2016. 0412028