IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 77-84
www.iosrjournals.org

Data Digest-based Authentication for Mobile Cloud Computing

Muzammil H Mohammed[1],Mohammed AlZain[2]
Department of Information Technology, College of Computers and Information Technology
Taif University, Taif, Saudi Arabia

Abstract: *Mobile cloud computing can influence the long run of various applications, like electronic commerce and health IP. With mobile cloud computing, resource-constrained mobile devices maymaximize the computation/storage resources of cloud servers via communication networks, mobile devices in mobile cloud computing arehaving lot of security risks as a result they usuallygot to access cloud servers through untrusted networks from completely different locations. one amongstthe foremostnecessary aspects of mobile cloud computing security is to determinedocumented communication sessions between mobile devices and cloud servers., DDA strategically incorporates hashing, additionally to ancient user ID and passwords, to realize mutual authentication. The effectiveness of DDA is valid with Scyther, security protocol analyser. Our experimental results indicate that DDA is capable of withstanding a rangeof various-security-attacks.*
Keywords: *Cloudcomputing, Security, Mobile devices, Authentication, Hashing*

Date of Submission: 17-01-2018 Date of acceptance: 31-01-2018

I. Introduction

In this paper, we have a tendency tocommit to improve the safety of mobile cloud computing by introducing a unique authentication theme, Data Digest-based Authentication, a mobile cloud uses either user id and watchwordprimarily based authentication, or USIM (universal subscriber identity module) primarily based authentication [2]. DDAemploys hashingand therefore theancient user id/password to makea good authentication mechanism. DDA ensures that mobile cloud computing is secured from any kind of unauthorized access at the startof everycommunication session. DDA employs the shopper registration termination andunidirectional mathematical hashing to cypher the user ID so asto form the authentication methodsafer and a lot of unpredictable. Remote location of resources and virtualization technologies build the cloud computing settingsusceptible to attacks. In cloud computing, all shoppers access a standard resource location that introduces security threat to the system. There'sassociate integrity issue in cases of transfer, storage and retrieval. There is nocommonplaceto make sureknowledge integrity. There isassociate inherent vulnerability within the service offered. If the virtualization platform is compromised, it implies that a majority of the virtual machines arevulnerable, thatcould be apotential threat to knowledge security.To address the top mentionedproblems, it's essential to possessa customary cloud computing style and usage policy, worker trust, proprietary computer code for virtualization. In a mobile cloud computing setting, a mobile device has got to be registered with a cloud server as a pre-requisite methodbefore avail any types of cloud services. The information transmission between the mobile device and therefore the cloud server should be performed once the mobile device authenticates the cloud server and vice-versa. a powerful authentication theme ensures secure communication between 2 legitimate parties although the channel experiences potential vulnerability. Since the mobile device lacks of procedure capability, it's not appropriateto usecomplicated operations within the mobile device for authentication method. In mobile cloud computing setting, if a mobile device is registered with a selected cloud service supplier, each mobile device and cloud server shouldevidenceone anotherin a very uniform mannerso as to secure the communication with one authentication theme, thatpermits a mobile user to access the cloud server from totally completely different completelydifferent locationsmistreatment different networks and differing kinds of mobile devices.

H a: In mobile cloud computing setting, the projected authentication theme introduces hashing primarily basedsecurity, that reduces the vulnerability of the system to attacks. to see the vulnerability of the system, we have a tendency towork out the vulnerability score, Sv. the worth of Sv lies between zero.0 and 1.0:

Ha : 0. zero<= Sv<= 1.0 (1)

A low score of Sv indicates that a theme offers a lot of security

Registration

The registration method of a mobile device or mobile user to a cloud server could be aonly onemethodwhereby the user ID and therefore thewatchwordis setup and few encrypted files arechanged. Upon fitting the mobile user account with cloud server, the cloud server performs a series of operations.

Algorithm1 shows the elaborated registration method adopted in our analysis.

Algorithm 1 Registration: mobile_with_cloud

Require:

isAlive (*mobile, cloud*)

hasNetworkAccess (*mobile*)

Ensure:

Role_Mobile

const *userID*

var *password*

uid = **hash**(*userID*)

pwd = **hash**(*password*)

$cloud \leftarrow$ **send**($uid \| pwd$)

$T_k = uid \oplus pwd$

Role_Cloud

recv($uid \| pwd$)

$T_k = uid \oplus pwd$

EXP = Registration expiry period for the client

$\#CF \leftarrow$ **pointer**{**store**(uid, pwd, T_k)}

MD_{user} = **hash**(usage policy, user access level, user certificate)

MD_{cloud} = **hash**(user add policy, cloud resource restriction, cloud certificate)

MD = **hash**($MD_{cloud} \| MD_{user}$)

$Temp = MD_{user} \| MD_{cloud} \| \#CF \| Pk_{pub\_cloud}$

msz = **encrypt**($Temp, T_k$)

$mobile \leftarrow$ **send**(msz)

The two parties concernedwithin the registration methodare unit mobile device and the cloud server. eachof the parties should be alive or be within the network to accomplish the registration method. Cloud Server stores h a s h, h a s h, and user's mobile device info in massive table for economicaloperation. It generates 2 hashed messages or data digests. The first, DDuser ,that consists of user policy (cloud resource usage policy, and user access level), and User certificate. The second message digest is DD cloud. Upon generating each message digests, cloud server creates associate encrypted message to transmit these info to the mobile device. ETk, whereverPkpub_cloudis that the cloud's public key, DD user and DD cloud area unit the generated message digests, and # C F is that the column reference, that refers to the cloud authentication information for that individual cloud user info. These infoarea unit sent from the cloud server to the mobile device when encrypting with key T k that's generated in each the mobile device and cloud server by XOR-ing (Exclusive OR) hashed userID and hashed parole (Eq. 2).

$$Tk = hash \oplus hash \quad (2)$$

Authentication

The cloud user has 2Data digests DD user , and DD cloud within the mobile device.The authentication methodis split into 2 steps: cloud authenticating mobile device and mobile device authenticating cloud.

3.1.Cloudauthenticatingmobile

when a mobile device desires to send associate authentication request to the cloud server, it generates a key T k ,victimization hashed userID and hashed parole (Eq. 2). The key T k , works because the seed for the PRNG (pseudo random range generator) to getassociate authentication key, A u t h_Keyi . This authentication key A u th_Keyi is needed to code the message digest DD, that is generated by hashing DD cloud and DD user (Eq. 3). The A u t h_Keyiis that then the sequence of bits generated by PRNG that'ssuch as by the state symbol SI. Key Tkis employed to code the state symbol SI, and therefore the encrypted message digest EAuth_Keyi. Finally, theencrypted message, ETk{EAuth_Keyi‖SI} is shipped to the cloud server (Fig. 1)along side the column reference # C F. Therefore, the message sent from mobile

device to cloud server is $\#CF \| ETk\{EAuth\_Keyi\{MD\} \| SI\}$

$MD=hash\{MDcloud \| MDuser\}$

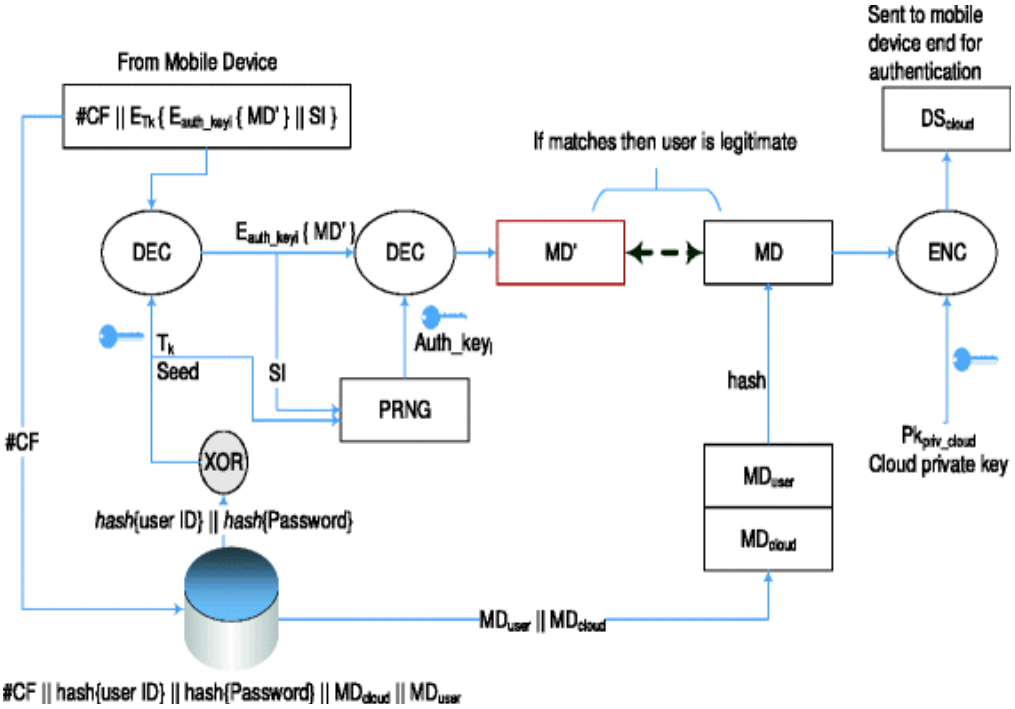

Fig. 1

Algorithm 2 Mobile_to_cloud_auth_req

Require:

isAlive (*mobile, cloud*)
hasNetworkAccess (*mobile*)
isRegistered (*mobile, cloud*)
$uid = \textbf{hash}(userID)$
$pwd = \textbf{hash}(password)$
$cloud \leftarrow \textbf{send}(uid \| pwd)$
$T_k = uid \oplus pwd$

Ensure:

$MD = \textbf{hash}(MD_{cloud} \| MD_{user})$
$Auth\_Key_i \leftarrow T_k$ **PRNG** SI
$Enc_1 = \textbf{encrypt}(MD, Auth\_Key_i)$
$Temp = Enc_1 \| SI$
$Enc_2 = \textbf{encrypt}(Temp, T_k)$
$cloud \leftarrow \textbf{send}(Enc_2 \| \#CF)$

Algorithm 3 Cloud_authenticating_mobile

Require:
isAlive (*mobile, cloud*)
hasNetworkAccess (*mobile*)
isRegistered (*mobile, cloud*)
Ensure:
$cloud \leftarrow \mathbf{recv}(Enc_2 \| \#CF)$
$SearchEntity \leftarrow (uid \| pwd)$
search($SearchEntity, \#CF$)
if $SearchEntity == found$
if $EXP == expired$
triggerUpdatePhase()
else
$T_k = uid \oplus pwd$
$Temp = \mathbf{decrypt}(Enc_2, T_k)$
$Temp = Enc_1 \| SI$
$Auth\_Key_i \leftarrow T_k$ **PRNG** SI
$MD = \mathbf{decrypt}(Enc_1, Auth\_Key_i)$
$MD' = \mathbf{hash}(MD_{cloud} \| MD_{user})$
if $MD == MD'$
integrityCheck(*pass*)
authentication(*pass*)
else
integrityCheck(*fail*)
authentication(*fail*)
endif
endif
else
authentication(*fail*)
endif

Upon receiving the authentication request message, the cloud server performs decipherment operations. The cloud server searches the precise hashed userID and hashed parolewithin the cloud authentication informationsupported the shared column reference # C F that's sent in plain text together with the encrypted message.Once the hashed userID and hashed parolearea unit found, the cloud server checks the registration validity of the user mistreatment EXP, keep at the server. If the user registration isn'tinvalid, then Tk is generated (Eq. 2) by XOR operationThe generated Tk at the cloud server decrypts the message ETk‖SI}, The authentication key, A u t h_Keyi decrypts the encrypted message digests EAuth_Key I .Algorithm3 summarizes the operations concernedwithin the second sub-step.

3.2.Mobileauthenticatingcloud

Once the mobile device is documented, the cloud server sends its digital signature, that consists of DD encrypted with cloud's non-public key Pkpriv_cloud , to the mobile device Alg 4 summarizes the operations performed at the cloud server throughout this section.

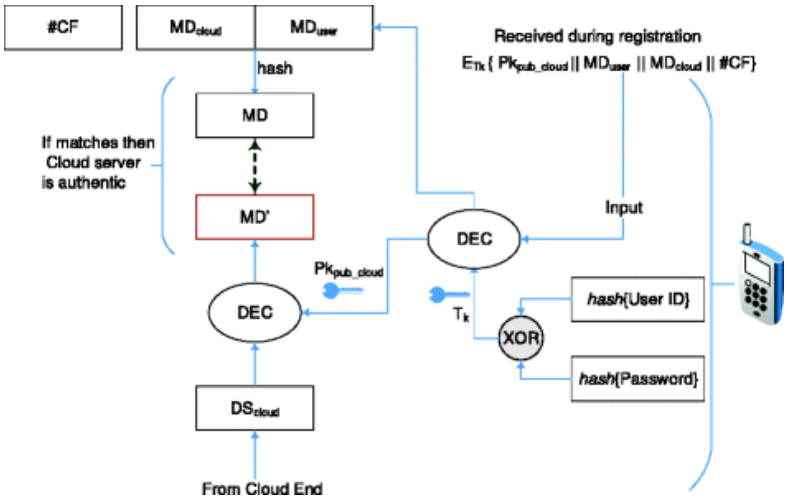

Fig. 2

Algorithm 4 Cloud_to_mobile_auth_req

Require:

isAlive (*mobile, cloud*)
hasNetworkAccess (*mobile*)
isRegistered (*mobile, cloud*)

Ensure:

$MD = \textbf{hash}(MD_{cloud} \| MD_{user})$
$DS = \textbf{encrypt}(MD, Pk_{priv\_cloud})$
$mobile \leftarrow \textbf{send}(DS)$

After receiving the digital signature DS, the mobile device decrypts it with cloud's public key Pkpub_cloud ,keepwithin the mobile device. If the decrypted DD matches with the message digest M D ′ keepwithin the mobile device, then it may bedeclared that the cloud server is legitimate. Alg 5 provides the operations that performed by the mobile device once receiving cloud's digital signature DS.

Algorithm 5 Mobile_authenticating_cloud

Require:

isAlive (*mobile, cloud*)
hasNetworkAccess (*mobile*)
isRegistered (*mobile, cloud*)
$uid = \textbf{hash}(userID)$
$pwd = \textbf{hash}(password)$
$T_k = uid \oplus pwd$

$MD = MD_{user} \| MD_{cloud}$
$msz \leftarrow \textbf{decrypt}((MD \| \#CF \| Pk_{pub\_cloud}), T_k)$
$msz = MD \| \#CF \| Pk_{pub\_cloud}$

Ensure:

$mobile \leftarrow \textbf{recv}(DS)$
$MD' = \textbf{decrypt}(DS, Pk_{pub\_cloud})$
if $MD == MD'$
    authentication(*pass*)
    integrityCheck(*pass*)
else
    authentication(*fail*)
    integrityCheck(*fail*)
endif

Update

During the registration section the cloud server generates terminationperiodfor every mobile consumer. This terminationperiod EXP is checked at the cloud server for every authentication request created by a mobile consumer. the new hashed numare going to becompletely different than the recent hashed num and thereby the generated Tk (Eq. 2) are going to becompletely different.

Evaluation-Methodology

We assume that the mobile device is already registered with the cloud server and obtained DD cloud , DD user , # C F, and Pkpub_cloudonce a registered mobile sends the authentication request ‖SI}‖#CF} to the cloud server, or once the cloud server sends authentication response Pkpriv_cloud to the mobile device, Methodology N is thevariety o attacks that area unit launched on the plannedtheme and N success is that thevariety of victorious attacks that area unit recorded. Then, the probability of victorious attacks on the theme defines its vulnerability score (S v) (Eq. 4). Lesser vulnerability score indicates that the plannedthemewillstopa lot ofvariety of attacks,thevalue of Sv lies between zero and 1.0 (Eq. 1) Sv=NsuccessN(4)We designed the Teddy boy setup and therefore the protocol analyserScyther for collateral the DDAtheme. Scyther is designed from the setting choice to launch every type of attacks. Scyther tried to launch different kinds of attacks considering hackers have initial information of the system. The plannedtheme uses public key cryptographywithin the registration method, parallelcryptography in authentication method and a typical hashing algorithmic rule in generating the message digests. We have used RSA (Rivest, Shamir, andAdelman) the public key cryptographyalgorithmic rule, SHA1 (Secure Hash algorithmic rule 1) the hashing algorithmic rule, and AES (Advanced cryptography Standard) theparallel key cryptographyalgorithmic rule. The man-in-the-middle attack object is activated willy-nilly, and it changed the request frames that area unit sent. Among one thousand frames, 256 frames area unitchanged in transit. The cloud server running DDAtheme has rejected all the changed request frames. mobiledevice, reset of EXP forces the cloud server to reject the authentication request. If EXP resets, a registration object is initialized to perform the re-registration.

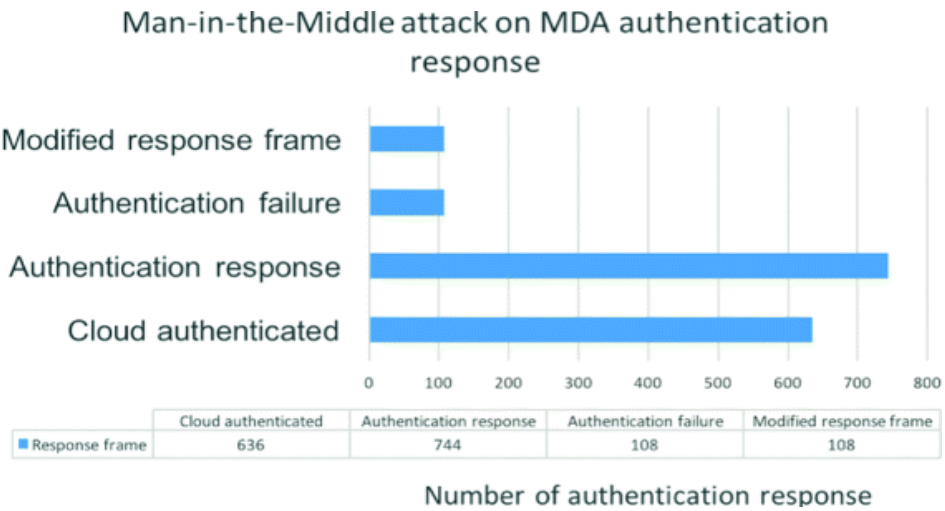

Fig. 3 Man-in-the-middle attack on DDA authentication response

Security Analysis Results

Table 1 summarizes our claims and how secure the scheme is for each claim. In this section, we provide detailed security analysis of the claims that are validated using *Scyther*.

Table 1Security Analysis

Role	Sl.Num.	Claim	Status	Comment
Mobile	1	secret $Auth\_Key_i$	Ok	No Attacks
	2	secret *SI*	Ok	No Attacks
	3	secret *password*	Ok	No Attacks
	4	secret *userID*	Ok	No Attacks
	5	secret MD_{user}	Ok	No Attacks
	6	secret MD_{cloud}	Ok	No Attacks
	7	Alive	Ok	No Attacks
	8	Weakagree	Ok	No Attacks
	9	Niagree	Ok	No Attacks
	10	Nisynch	Ok	No Attacks

Cloud	1	secret $Auth\_Key_i$	Ok	No Attacks
	2	secret *password*	Ok	No Attacks
	3	secret *userID*	Ok	No Attacks
	4	secret *SI*	Ok	No Attacks
	5	Alive	Ok	No Attacks
	6	Weakagree	Ok	No Attacks
	7	Niagree	Ok	No Attacks
	8	Nisynch	Ok	No Attacks

Cond 1: Auth_Keyi remains secret throughout the authentication method.
Auth_Keyiis employed to write and decode the Data digest DD to produce multi layer security. A Mobile device sends the Data digest DD to the cloud server by encrypting with A u t h_Keyi , thatcould be aradically symmetrical key. Each parties, the mobile device and also the cloud server willseverally generate the Auth_Keyivictimization state symbol SI. Since Auth_Keyiisn'tchanged between each of the parties, it remains secret.

Cond2: StatesymbolSIissecret.SI is that the state symbol for PRNG specify the n th sequence of PRNG because the desired pattern. The mobile device sends SI to the cloud server for specifying the n th sequence of PRNG to come up with the Auth_Keyi . SI is shipped from mobile device to cloud server when encrypting with key Tk . The claim at the mobile being secret is validvictimizationScyther. On the opposite hand, the cloud server doesn't share or send SI, therefore, it's safe at the cloud end.

Cond3:Passwordissecret.The safety of the secret password depends on the user. Generallynobody shares their secret, thereby keeping it safe. The secret passwordmay be a 512 bit string, that is hashed and a duplicate of the user‘s secret is kept at the cloud server throughout registration method. The mobile device doesn't send the secretthroughout authentication method, howeveritis used at each ends to come up with the key Tk . Our secret password safety claim is valid by Scyther, but, in reality, it'shooked in to the user.

Cond 4: UserIdentification is confidential. UserID is shipped to the cloud server solelythroughout the registration method, that is neededbeside the secretto come up withTk . The userID is hashed and a duplicate is keep at the cloud server throughout registration method. The mobile device doesn't send userID to the cloud server throughout authentication method. Therefore, userID remains safe. Our userID safety claim is valid by Scyther, but, in reality, it'shooked in to the user.

Cond 5: The themeneeds DD user to be a secret. DD user is that the hashed dataassociated with the user, which can contain policy data and distinctivedataregarding the user. This data is generated at the cloud server and sent to the mobile device whenuser sent registration method. This is hashed and encrypted with Auth_keyi before transmission from the user mobile device to the cloud finish. Scythervalid our claim that DD user is safe..

Cond 6: Mobile device and also the cloud server remains alive throughout the execution of the protocol.The cloud server is alleged to be alive if it's been victimization the plannedtheme for the initial (i−1) messages changed with the mobile device, once the latter sends the ith message. The protocol instrumentScyther validates the aliveness claim

.

II. Conclusion

During this paper, we tend to propose a unique authentication theme for mobile cloud computing,Data Digest-based Authentication consists of 3 phases: registration, authentication, and update. With these phases, Data Digest Authentication utilizes hashing, additionally totraditional user id and secretprimarily based uthentication, to make sure confidentiality and integrity throughout the authentication method.Itcan survive a rangeof various attacks, like man-in-the-middle, replay attacks, etc.

References

[1]. Abolfazli S, Sanaei Z, Shiraz M, Gani A (2012) MOMCC: Market-oriented architecture for Mobile Cloud Computing based on Service Oriented Architecture In: 2012 1st IEEE International, Conference on Communications in China Workshops (ICCC), 8–13. doi:http://dx.doi.org/10.1109/ICCCW.2012.6316481.

[2]. Ahmad Z, Mayes KE, Dong S, Markantonakis K (2011) Considerations for mobile authentication in the Cloud. InfSecur Tech Rep 16(3–4): 123–130. ISSN 13634127. doi:http://dx.doi.org/10.1016/j.istr.2011.09.009.

[3]. Alizadeh M, Hassan WH (2013) Challenges and opportunities of Mobile Cloud Computing In: 2013 9th International, Wireless Communications and Mobile Computing Conference (IWCMC), 660–666. doi:http://dx.doi.org/10.1109/IWCMC.2013.6583636.

[4]. Alrokayan M, Buyya R (2013) A web portal for management of aneka-based multicloud environments In: Proceedings of the Eleventh Australasian Symposium on Parallel and Distributed Computing - Volume 140, 49–56.Google Scholar

[5]. Behl A, Behl K (2012) An analysis of cloud computing security issues In: World Congress on, Information and Communication Technologies (WICT), 109–114. doi:http://dx.doi.org/10.1109/WICT.2012.6409059.

[6]. BehlA (2011) Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation In: 2011 World Congress on Information and Communication Technologies, 217–222. doi:http://dx.doi.org/10.1109/WICT.2011.6141247.
[7]. Benkhelifa E, Fernando DA (2014) On a Real World Implementation of Advanced Authentication Mechanism in a Multi-Tenant Cloud Service Delivery Platform In: 5th International Conference on Information and Communication Systems (ICICS), 1–6.Google Scholar
[8]. Bouayad A, Blilat A, El HoudaMejhed N, El Ghazi M (2012) Cloud computing : security challenges. Colloquium in Information Science and Technology (CIST).Google Scholar
[9]. Carpendale S, Kerren A, Stasko JT, Fekete J-D, North C (2008) Evaluating Information Visualizations In: Information Visualization, volume 4950 of Lecture Notes in Computer Science, Springer, Berlin Heidelberg, ISBN 978-3-540-70955-8, 19–45. doi:http://dx.doi.org/10.1007/978-3-540-70956-5_2.
[10]. Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H (2011) A Strong User Authentication Framework for Cloud Computing In: 2011 IEEE Asia-Pacific Services, Computing Conference, 110–115. doi:http://dx.doi.org/10.1109/APSCC.2011.14.
[11]. Chow R, Jakobsson M, Davis UC, Shi E (2010) Authentication in the Clouds: A Framework and its Application to Mobile Users. CCSW10, Chicago.Google Scholar
[12]. Cremers C (2008) The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols In: Proceedings of the 20th International Conference on Computer Aided Verification, Princeton.Google Scholar
[13]. Dash SK, Mohapatra S, Pattnaik PK (2010) A Survey on Applications of Wireless Sensor Network Using Cloud Computing. International Journal of Computer Science & Emerging Technologies 1(4): 50–55.Google Scholar
[14]. Dinh HT, Lee C, Niyato D, Wang P (2011) A Survey of, Mobile Cloud Computing : Architecture, Applications, and Approaches. Published online in Wiley Online Library. doi:http://dx.doi.org/10.1002/wcm.1203/abstract.
[15]. Eaves A, Stockman M (2012) Desktop as a service proof of concept In: Proceedings of the 13th annual conference on Information technology education - SIGITE '12, 85. doi:http://dx.doi.org/10.1145/2380552.2380577.
[16]. Ficco M, Rak M (2015) Stealthy denial of service strategy in cloud computing. IEEE Trans Cloud Comput 3(1): 80–94. ISSN 2168-7161. doi:http://dx.doi.org/10.1109/TCC.2014.2325045.
[17]. Guan L, Ke X, Song M, Song J (2011) A Survey of Research on Mobile Cloud Computing In: 2011 10th IEEE/ACIS International Conference on Computer and Information Science, 387–392. doi:http://dx.doi.org/10.1109/ICIS.2011.67.
[18]. Joshi JBD, Takabi H, Ahn G (2010) Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, IEEE 8: 24–31.View ArticleGoogle Scholar..
[19]. Joshi JBD, Takabi H, Ahn G (2010) Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, IEEE 8: 24–31.View ArticleGoogle Scholar..

Muzammil H Mohammed."Data Digest-based Authentication for Mobile Cloud Computing." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 77-84.