ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

Fortify Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography

[1] S Venkata Ramanaiah, [2] A. Anil Kumar Reddy, [3] N.Prashanti
[1][2][3] Asst. Prof, Dept. of CSE, CMR Engineering College, Hyderabad, India

***Abstract*— An ever increasing number of organizations start to give various types of Cloud computing administrations for Internet clients in the meantime these administrations additionally bring some security issues. As of now the larger part of Cloud computing frameworks give computerized personality to clients to get to their administrations, this will bring some burden for a mixture cloud that incorporates various private mists as well as open mists. Today most Cloud computing framework utilize uneven and tradi-tional open key cryptography to give information security and shared authentica-tion. Personality based cryptography has some fascination qualities that appear to fit well the prerequisites of Cloud computing. In this paper, by receiving sustained erated personality administration together with various leveled character based cryptogra-phy (HIBC), the key conveyance as well as the shared confirmation can be streamlined in the cloud.**

I. INTRODUCTION

An ever increasing number of organizations start to give various types of Cloud computing administrations for Internet clients in the meantime these administrations additionally bring some security issues. As of now the larger part of Cloud computing frameworks give computerized personality to clients to get to their administrations, this will bring some burden for a mixture cloud that incorporates various private mists as well as open mists. Today most Cloud computing framework utilize uneven and tradi-tional open key cryptography to give information security and shared authentica-tion. Personality based cryptography has some fascination qualities that appear to fit well the prerequisites of Cloud computing. In this paper, by receiving sustained erated personality administration together with various leveled character based cryptogra-phy (HIBC), the key conveyance as well as the shared confirmation can be streamlined in the cloud.

As of now, as appeared in Figure 1, there are fundamentally three kinds of mists: private mists, open mists and half and half mists [15]. Private mists, additionally called inner mists, are the private systems that offer Cloud computing administrations for an extremely restric-tive arrangement of clients inside interior system. For instance, a few organizations and universi-ties can utilize their inside systems to give Cloud computing administrations to their own particular clients. These sorts of systems can be thought as private mists. Open mists or outer mists allude to mists in the customary sense [13], for example, undertakings that give Cloud computing administrations to general society clients. Crossover mists are the mists that incorporate different private and additionally open mists [14]. Giving security in a private cloud and an open cloud is less demanding, contrasting and a half breed cloud since usually a private cloud or an open cloud just has one specialist organization in the cloud. Giving security in a half breed cloud that comprising different specialist organizations is significantly more troublesome particularly for key dissemination and common confirmation. Additionally for clients to get to the administrations in a cloud, a client computerized character is required for the servers of the cloud to deal with the entrance control. While in the entire cloud, there are many vary ent sorts of mists and each of them has its own character administration framework. In this manner client who needs to get to administrations from various mists needs numerous computerized identi-ties from various mists, which will bring bother for clients. Utilizing unified character administration, every client will have his special computerized personality and with this personality, he can get to various administrations from various mists.

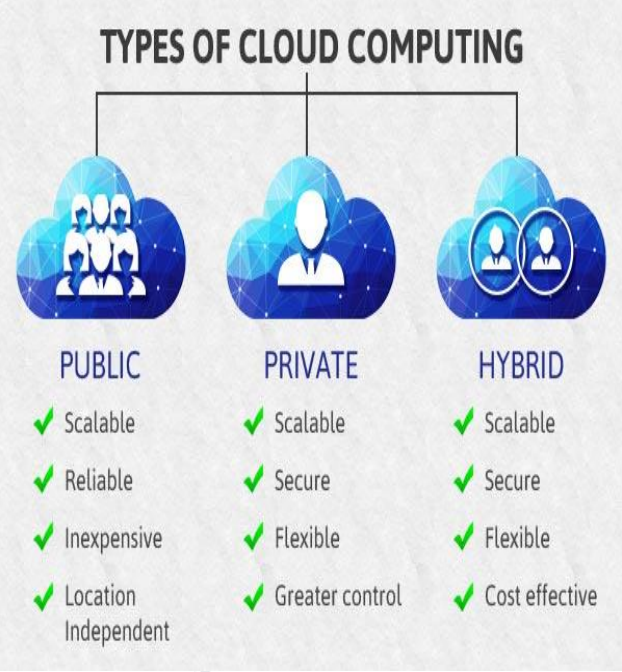
Character based cryptography [10] is an open key innovation that permits the utilization of an open identifier of a client as the client's open key. Chain of command character based cryptography is the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

improvement from it with a specific end goal to take care of the versatility issue. As of late character based cryptography and progressive system personality based cryptography have been proposed to give security to some Internet applications. For instance, applying personality based cryptography in the network figuring and web benefit security have been investigated in [11] [8] [12] and [5].

This paper proposes to utilize united character administration in the cloud to such an extent that every client and every server will have its own one of a kind personality, and the character is allo-cated by the framework progressively. With this interesting personality and progressive character based cryptography (HIBC), the key circulation and common verification can be incredibly streamlined.



Whatever is left of this paper is composed as takes after. In Section 2, we present security issues and related arrangements in Cloud computing. In Section 3, we depict the standard of personality based cryptography and HIBC. In Section 4, we depict how to utilize unified character administration and HIBC in the Cloud computing framework to ace vide security. Segment 5 finishes up the paper.

2 SECURITY IN CLOUD COMPUTING

Cloud computing have many points of interest in cost lessening, asset sharing, efficient for new administration sending. While in a Cloud computing framework, most information and programming that clients utilize dwell on the Internet, which bring some new difficulties for the framework, particularly security and protection. Since every application may utilize asset from numerous servers. The servers are possibly based at various areas and the administrations gave by the cloud may utilize distinctive frameworks crosswise over associations. Every one of these qualities of Cloud computing make it entangled to give security in Cloud computing. To guarantee satisfactory security in Cloud computing, different security issues, for example, confirmation, information classification and honesty, and non-renouncement, all should be considered. As of now, WS-Security benefit is uncontrollably utilized as a part of the cloud to give security to the framework. In WS-Security, XML encryption and XML mark are utilized to give information privacy and respectability. Common confirmation can be bolstered by including X.509 authentication and Kerberos tickets into SOAP message header.

As said before, there are three kinds of mists as a rule: private cloud, open cloud and half and half cloud. In an open cloud, assets are powerfully provisioned on a fine-grained, self-benefit premise over the Internet. Administrations in the cloud are given by an off-site outsider supplier who shares assets and bills on a fine-grained utility processing premise. While in most private mists, with restricted figuring assets, it is troublesome for a private cloud to give all administrations to their clients, as a few administrations may a bigger number of assets than inward cloud can give. Mixture cloud is a potential answer for this issue since they can get the processing assets from outer Cloud computing suppliers. Private mists have their favorable circumstances in company administration and offer dependable administrations, and additionally they permit more control than open mists do. For the security concerns, when a cloud domain is made inside a firewall, it can furnish its clients with less introduction to Internet security dangers. Likewise in the private cloud, every one of the administrations can be gotten to through inner connec-tions as opposed to open Internet associations, which make it simpler to utilize existing safety efforts and norms. This can influence private mists more to suitable for administrations with delicate information that must be secured. While in a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

mixture cloud, it incorporates more than one area, which will build the trouble of security arrangement, particularly key administration and common validation. The areas in a half breed cloud can be heterogeneous systems, henceforth there might be holes between these systems and between the diverse administrations suppliers. Indeed, even security can be all around ensured in each of private/open cloud, while in a crossover cloud with more than one sort of mists that have various types of system conditions and distinctive secu-rity arrangements, how to give productive security assurance is substantially more troublesome. For instance, cross space validation can be an issue in a half breed cloud with distinctive spaces. Albeit some validation administrations, for example, Kerberos can genius vide multi-area verification, yet one of the prerequisites for the multi-space Kerberos confirmation is that the Kerberos server in every area needs to impart a mystery key to servers in different Kerberos areas and each two Kerberos servers should be enrolled with each other. The issue here is if there are N Kerberos spaces and each of them need to believe each other, at that point the quantity of key trades is N(N-1)/2. For a half and half cloud with countless, this will bring an issue for adaptability. In the event that diverse systems in a half and half cloud utilizing distinctive authen-tication conventions, this issue can be more intricate.

In a cloud, the distributed computing framework needs to give a solid and easy to understand path for clients to get to a wide range of administrations in the framework. At the point when a client needs to run an application in the cloud, the client is required to give a computerized personality. Typically, this character is an arrangement of bytes that identified with the client. In light of the computerized personality, a cloud framework can realize what right this client has and what the client is permitted to do in the framework. The majority of cloud stages incorporate a personality benefit since character informa-tion is required for most disseminated applications [3]. These distributed computing frameworks will give an advanced character to each client. For instance, client with a Windows Live ID can utilize distributed computing administrations gave by Microsoft and client who needs to get to distributed computing administrations from Amazon and Google additionally needs an Amazon-characterized personality and Google account. Here, each of these organizations is an open cloud. The issue here is this computerized character must be utilized as a part of one private cloud or one open cloud. Clients need to get to administrations in the cloud that gave by various mists should have different characters, each for one of the cloud. This is obvi-ously not easy to understand.
To tackle these issues in the cloud, we propose to utilize unified character man-agement in mists with HIBC. The proposed plot does not just enable clients from a cloud to get to administrations from different mists with a solitary advanced character, it additionally simpli-fies the key dissemination and common confirmation in a half and half cloud.

3 IDENTITY-BASED CRYPTOGRAPHY AND SIGNATURE

Personality based cryptography and mark plans were initially proposed by Shamir [10] in 1984. In any case, just in 2001, an effective approach of character based encryption plans was created by Dan Boneh and Matthew K. Franklin [2] and Clifford Cocks [4]. These plans depend on bilinear pairings on elliptic bends and have provable security. As of late various leveled personality based cryptography (HIBC) has been proposed in [6, 7] to enhance the adaptability of conventional character based cryptography plot.

Personality based cryptographic plan is a sort of open key based approach that can be utilized for two gatherings to trade messages and successfully check each other's marks. Not at all like in customary open key frameworks that utilizing an irregular string as the general population key, with character based cryptography client's personality that can particularly distinguish that client is utilized as the general population key for encryption and mark confirmation. Character based cryptography can facilitate the key administration many-sided quality as open keys are not required to be appropriated safely to others. Another favorable position of personality based encryption is that encryption and unscrambling can be led disconnected without the key age focus.

In the personality based cryptography approach, the PKG ought to makes an "ace" open key and a relating "ace" private key right off the bat, at that point it will make this "ace" open key open for all the intrigued clients. Any client can utilize this "ace" open key and the character of a client to make the general population key of this client. Every client needs to get his private key needs to contact the PKG with his character. PKG will utilize the personality and the "ace" private key to create the private key for this client. In Dan Boneh and Matthew K. Franklin's approach, they characterized four calculations for a finish personality based cryptography framework. It

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

incorporates setup, remove, encryption also, unscrambling.

1. Setup: PKG make an ace key m K and the framework parameters P. m K is kept mystery and used to create private key for clients. Framework parameters P are made open for every one of the clients and can be utilized to create clients' open key with their personalities.

2. Concentrate: When a client asks for his private key from the PKG, PKG will utilize the personality of this client, framework parameters P and ace key m K to produce a private key for this client.

3. Encryption: When a client needs to scramble a message and send to another client, he can utilize the framework parameters P, recipient's character and the message as contribution to produce the figure content.

4. Decoding: Receiving a figure content, recipient can utilize the framework parameters P and his private key got from the PKG to unscramble the figure content.

In a system utilizing identity based cryptography, the PKG needs not exclusively to create private keys for every one of the clients, yet in addition to check the client personalities and build up secure channels to transmit private keys. In a vast system with just a single PKG, the PKG will have a troublesome activity. For this situation, HIBC [6] can be a superior decision. In a HIBC arrange, a root PKG will produce and disperse private keys for space level PKGs furthermore, the area level PKGs will create and circulate private keys to the clients in their own particular area. HIBC is appropriate for a vast scale organize since it can lessen the workload of root PKG by disperse crafted by client confirmation, private key age furthermore, conveyance to the distinctive level of PKGs. It can likewise enhance the security of the system since client validation and private key conveyance should be possible locally. The HIBC encryption and mark calculations incorporate root setup, bring down level setup, extraction, encryption, and unscrambling.

1. Root setup: root PKG will create the root PKG framework parameters and a root mystery. The root mystery will be utilized for private key age for the bring down level PKGs. The root framework parameters are made freely accessible also, will be utilized to produce open keys for bring down level PKGs and clients.

2. Lower-level setup: Each lower-level PKG will get the root framework parameters what's more, create its own particular lower-level mystery. This lower-level mystery will be used to create private keys for the clients in its area.

3. Concentrate: When a client or PKG at level t with its personality (1,..., t ID) demands his private key from its upper-level PKG, where (1,..., I ID) is the character of its progenitor at level I ($1 \leq I \leq t$), the upper-level PKG will utilize this personality, framework parameters and its own particular private key to produce a private key for this client.

4. Encryption: User who needs to encode a message M can utilize the framework parameters, recipient's character and the message as contribution to create the figure content.

C = Encryption (parameters, beneficiary ID, M).

5. Decoding: Receiving a figure content, beneficiary can utilize framework parameters and his private key got from the PKG to unscramble the figure content.
M = Decryption (parameters, k, C), k is the private key of the recipient

6. Marking and confirmation: A client can utilize parameters, its private key, and message M to create a computerized mark and sends to the collector. Collector also, check the mark utilizing the parameters, message M, and the sender's ID.
Mark = Signing (parameters, k, M), k is the sender's private key.
Confirmation = (parameters, sender ID, M,Signature).

There are some inborn confinements with the personality based cryptography [1]. One of the issues is the key escrow issue. Since clients' private keys are produced by PKG, the PKG can decode a client's message and make any client's advanced mark without approval. This in truth implies that PKGs must be exceedingly trusted. So the identitybased plot is more proper for a shut gathering of clients, for example, a major organization or then again a college. Since just under this circumstance, PKGs can be set up with clients' trust In a framework utilizing HIBC, each PKG in the progressive system knows the clients' private keys in the area under the PKG. Albeit key escrow issue can not be evaded, this can restrain the extent of key escrow issue. Another downside of the personality based cryptography is the denial issue. Since every one of the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

clients in the framework utilize a few special identifiers as their open keys, on the off chance that one client's private key has been traded off, the client need to change its open key. For instance, if people in general key is the client's name, address, or email address, it is badly arranged for the client to transform it. One answer for this issue is to add a day and age to the identifier as general society key[2], however it can not tackle this issue totally.

4 USING FEDERATED IDENTITY MANAGEMENT IN CLOUD

4.1 Federated Identity Management in the Cloud

Contrasted and concentrated character, which is utilized to manage security issues inside similar systems, united personality is received to manage the security issues that a client might need to get to outside systems or an outer client may need to get to inner systems. Combined character is a standard-based instrument for distinctive association to share character amongst them and it can empower the movability of personality data to crosswise over various systems. One regular utilization of united personality is secure Internet single sign-on, where a client who sign in effectively at one association can get to all accomplice systems without logging in once more. Utilizing character league can build the security of system since it just requires a client to distinguish and confirm him to the framework for one time and this character data can be utilized as a part of various systems. Utilization of personality league principles cannot just push the client to over various systems incorporate outside systems with just a single time sign in, yet additionally can help clients from various systems to believe each other.

Utilizing personality organization in the cloud implies clients from various mists can utilize a combined distinguishing proof to recognize themselves, which normally suit the prerequisite of personality based cryptography in distributed computing. In our approach, clients and servers in the cloud have their own particular remarkable characters. These characters are various leveled personalities. To get to administrations in the cloud, clients are required to validate themselves for each administration in their own particular mists. At times, servers are likewise required to confirm themselves to clients. In a little and shut cloud, this necessity can be fulfilled effortlessly. While in a crossover cloud, there are different private or potentially open mists and these mists may depend on various verification instruments. Giving powerful validations for clients and servers from various cloud spaces would be troublesome. In this paper, we propose to utilize unified character administration and HIBC in the cloud. In the cloud trusted expert PKGs are utilized and these PKGs won't just act as PKGs in conventional personality based cryptography framework yet in addition distribute various leveled characters to clients in their spaces. There is a root PKG in general space of each cloud, and each sub-level area (private or open cloud) inside the cloud additionally has its own particular PKG. The root PKG will deal with the entire cloud, every private cloud or open cloud is the principal level and clients and servers in these mists are the second level. The root PKG of the cloud will apportion and verify characters for all the private and open mists. For instance, it can distribute character UiS to a private cloud of University of Stavanger. Every private cloud and open cloud utilizes its own area PKG to dispense and deal with the characters of the considerable number of clients and servers in its own cloud. Every client and server in this space has its own particular personality and this character is a various leveled personality, which incorporates both the character of the client or server and the personality of the space.

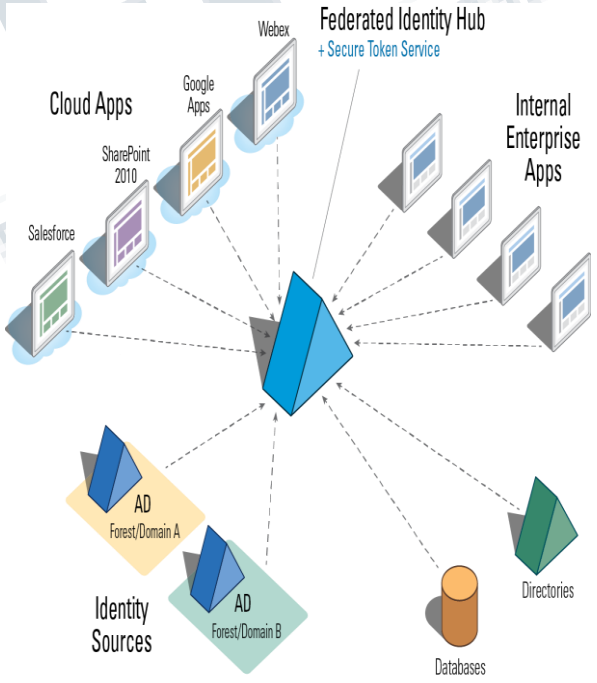


Fig. 2. Federated identity management in cloud

4.2 Key Generation and in the Cloud

Utilizing HIBC in the cloud, a critical part is key age and appropriation. As appeared in [6], the security of HIBC conspire depends on the utilizing of permissible blending.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

Let 1 G and 2 G be two gatherings of some extensive prime request q and 1 G is an added substance gathering and 2 G is a multiplicative gathering, we can call ˆe a permissible blending if ˆ e :

G 1 × G 2 → G 2 have the accompanying properties.

1. Billinear: For every one of the 1 P , Q ∈ G and , q a b ∈ Z ∗ , eˆ(aP, bQ) = eˆ(P,Q)ab .

2. Non-deteriorate: There exits 1 P,Q ∈ G , with the end goal that eˆ(P,Q) ≠ 1.

3. Processable: For every one of the 1 P,Q ∈ G , there exits a proficient approach to ascertain

eˆ(P ,Q) .

An allowable matching can be produced by suing a Weil blending or a Tate matching [2]. Here, in the cloud we utilize two levels PKG, the root PKG is 0 level PKG and the PKGs in the private or open mists are 1 level PKGs. The root setup should be possible as take after:

1. Root PKG creates 1 G , 2 G and an acceptable matching

$$e\hat{}(aP, bQ) = e\hat{}(P, Q)^{-1}(G, G, e\hat{}, P, Q, H, H)\ e\hat{}: G_1 X\ G_2 -> G_2$$

2. Root PKG

$P \in G_1$ and $S_0 \in Z_q^*$ and set of $Q_0 = s_0 P_0$.

3. Root PKG picks hash function H_1:{ 0 , 1}* -> G and H2:G2→{ 0 , 1}^{n}.

At that point the framework parameters are (G_1,G_2,, eˆ, P ,Q , H_1 , H_2) and are open accessible, s_0 is the root PKG's mystery and is known just by the root PKG. For the lower level PKGs and clients and servers in the cloud, they can utilize the framework parameters and any client's personality to produce its open key. What's more, every client or servers in the cloud can interface the PKGs in their cloud area to get their private keys. For instance, the PKG in private billow of University of Stavanger with character UIS, its open key can be produced as P_{uis} = H(UIS) and the root PKG can produce its private key as u is 0 u is s = s P . For a client with personality UIS. Alice in the private cloud University of Stavanger , her open key.

4.3 Date Encryption and Digital Signature

In the cloud, a champion among the most basic security issues are shared confirmation among customers and servers, affirmation of data mystery and genuineness in the midst of data ransmission by encryption utilizing mystery keys. In a cloud utilizing united character, any client and server has its extraordinary personality and any client and server can get the personality of some other client/server in response to popular demand with the PKGs. With HIBC, the general population key dissemination can be incredibly disentangled in the cloud. Clients and servers don't have to ask an open key registry to get people in general key of different clients and servers as in conventional open key plans. On the off chance that any client or server needs to scramble the information that transmitted in the cloud, the sender can obtain the character of the recipient, at that point the sender can encode the information with recipient's character. Right now, WS-Security (Web benefit Security) convention which can give end-to - end message level security utilizing SOAP messages is broadly connected in distributed computing to ensure the security of most distributed computing related web administrations. WS-Security utilizes SOAP header component to convey security-related data. Since SOAP message is a sort of XML message and conventionally XML message portrayal is about 4 to 10 times substantial contrasted and their equal parallel organizations, including security data into SOAP header will extraordinarily build the expenses of information correspondence and information parsing. For instance, if XML mark is utilized to secure information trustworthiness or verification, the SOAP header will incorporate the mark data about the mark strategy, signature esteem, key data and some reference data like process technique, changes, and process esteem. Also, the key data component may incorporate keys names authentications and some open key administration data [16]. In the event that RSA and X.509 are picked as general society key cryptography and endorsement organize in XML signature, the key information component in the SOAP header more often than excludes an open key declaration or a reference indicating a remote area. While utilizing HIBC in a cloud, any client and server can get its own particular private key from its space PKG and can alculate people in general key of some other gathering in the cloud knowing its character. At that point

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

it is simple for a sender to include an advanced mark utilizing its private key and for a collector to check a computerized signature utilizing the sender's open key. At that point the key data might be not required in the SOAP header, and this will incredibly diminish the SOAP messages should be transmitted in the cloud and in this way spare the cost.

4.4 Secret Session Key Exchange and Mutual Authentication

Personality based cryptography is an open key cryptography conspire, it is much slower when it is contrasted and symmetric key cryptography. By and by, open key cryptography isn't utilized for information encryption in the greater part of the mists. For instance, in XML encryption, XML information is scrambled utilizing symmetric cryptography, for example, AES and Triple-DES. This mystery symmetric key is scrambled utilizing people in general key encryption and included the SOAP message and after that transmitted to the collector. While in the cloud with HIBC, this mystery symmetric key conveyance can be maintained a strategic distance from since personality based cryptography can be utilized for mystery session key trade. As indicated by [9], for each two gatherings in the framework utilizing personality based cryptography, it is simple for every last one of the two gatherings to compute a mystery session key between them utilizing its own private key and open key of other gathering, this is call character based noninteractive key dissemination. For instance, two gatherings Alice and Bob in a cloud with their open keys and private keys Palice ,Q alice , Pbob and Pbob can ascertain their mutual mystery session key by figuring This implies in a cloud utilizing HIBC, every client or server can compute a mystery session key amongst it and the other party it needs to speak with without message trade. This favorable position of character based cryptography can diminish message transmission as well as can keep away from session key exposure amid transmission. This mystery session key can be utilized for information encryption, as well as for common verification [8]. We expect if a client with character Alice@UiS and a server with personality Storage@google in the cloud need to validate each other. To begin with, they can ascertain a mystery session key s K between them. At that point Alice can make an impression on the server as:

Here M is an arbitrarily chosen message and f is a restricted hash work. Here, to figure the right hash esteem, a right mystery session key s K is required. Since s K calculation requires Alice's private key and this private key must be designated from the PKG in the private billow of University of Stavanger, along these lines Alice can be checked that she is a lawful client of this cloud. Additionally the server can validate itself to Alice a similar way. We can see that this common confirmation does exclude any confirmation shape an outsider.

4.5 Key Escrow

For a framework utilizing character based cryptography, key escrow issue is innate and can not be stayed away from since PKG knows the private keys of the considerable number of clients. While in the various leveled character based cryptography framework, just the PKG in an indistinguishable space from the clients can knows their private keys. PKGs in different areas or at different levels can not know these private keys, such the key escrow issue can be confined in a little run.

5 CONCLUSION

The fast improvement of distributed computing bring some security issues and also many advantages to Internet clients. Current arrangements have a few burdens in key administration and verification particularly in a half and half cloud with a few open/private mists. In this paper, we portrayed the standards of personality based cryptography and various leveled personality based cryptography and discover the properties of HIBC fit well with the security requests of cloud. We proposed to utilize combined personality administration and HIBC in the cloud and portrayed by what method can the framework create and circulate people in general and private keys to clients and servers. Looked at with the present Ws-Security approach, we can see our approach has its favorable circumstances in disentangling open key dissemination and lessening SOAP header estimate. Additionally we appeared how the clients and servers in the cloud can create mystery session key without message trade and verify each other with a straightforward way utilizing personality based cryptography. Likewise we can see the key escrow issue of personality based cryptography can be limited with HIBC approach.

6 REFERENCES

1. Beak, J., Newmarch, J., Safavi-Naini, R., Susilo, W.: A Survey of Identity-Based Cryptography. In: Proc. of the 10th Annual Conference for Australian Unix User's Group (AUUG 2004), pp. 95–102 (2004)

2. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil Pairing. In: Kilian, J.(ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 433–439. Springer, Heidelberg (2001) 3. Chappell, D.: A Short Introduction to Cloud Platforms,http://www.davidchappell.com/CloudPlatforms –Chappell.pdf

4. Cocks, C.: An Identity-based Encryption Scheme Based on Quadratic Residues. In: Proceeding of 8th IMA International Conference on Cryptography and Coding (2001)

5. Crampton, J., Lim, H.W., Paterson, K.G.: What Can Identity-Based Cryptography Offer to Web Services? In: Proceedings of the 5th ACM Workshop on Secure Web Services (SWS 2007), Alexandria, Virginia, USA, pp. 26–36. ACM Press, New York (2007)

6. Gentry, C., Silverberg, A.: Hierarchical ID-Based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002) 7. Horwitz, J., Lynn, B.: Toward Hierarchical Identity-Based Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002)

8. Mao, W.: An Identity-based Non-interactive Authentication Framework for Computational Grids. HP Lab, Technical Report HPL-2004-96 (June 2004)

9. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan (January
2000)

10. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

11. Lim, H.W., Robshaw, M.J.B.: On identity-based cryptography and GRID computing. In: Bubak, M., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2004. LNCS, vol. 3036, pp. 474–477. Springer, Heidelberg (2004)

12. Lim, H.W., Paterson, K.G.: Identity-Based Cryptography for Grid Security. In: Proceedings of the 1st IEEE International Conference on e-Science and Grid Computing (e-Science 2005). IEEE Computer Society Press, Los Alamitos (2005)

13. Defining Cloud Services and Cloud Computing, http://blogs.idc.com/ie/?p=190

14. IBM Embraces Juniper For Its Smart Hybrid Cloud, Disses Cisco (IBM), http:// www. business sinsider .com /2009 /2/ ibm- embrace s-juniper-for-its-smart-hybrid-cloud- disses-cisco-ibm

15.http://en.wikipedia.org/wiki/Cloud_computing#cite_note-61

16. XML Signature Syntax and Processing (Second Edition)http://www.w3.org/TR/xmldsig-core/#sec-KeyInfo