International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 2937 - 2944

Forward Secrecy Scheme Accessing Cloud Data using Elliptic Curve ID based Signcryption

Mr.S.Navin Prasad
(*MKU Part Time)*
Assistant Professor & Head,
Department of Computer Science,
Nagarathinam Angalammal Arts and Science College,
Madurai, Tamil Nadu, India.

Dr.C.Rekha
Assistant Professor,
Department of Computer Science,
Government Arts College,
Melur, Tamil Nadu, India

Abstract

Cloud computing is a registering model which gives pervasive, helpful, on-request network admittance to a common pool of configurable registering assets that can be quickly provisioned and delivered with almost no forthcoming IT framework ventures costs. Cloud registering moves the application and information to the distributed storage where the administration of the information and administrations may not be completely reliable. Hence, there is a requirement for cloud administration suppliers to give an adequate degree of uprightness for the customer's information. In this paper, we proposed an information security plot utilizing Signcryption and Forward Secrecy via ECC in a logical step.Signcryption scheme dependent on Elliptic Curve saves more computational time and cost.

Keywords*: Cloud Computing, Signcryption, ECC, Forward Secrecy, Public key Cryptosystem, Authentication*

1. **INTRODUCTION**:

In recent years Cloud Computing emerged most powerful in the data sharing for the users. Cloud Computing is most Cloud architecture to store, share and access the data from one end to another end simply via an Internet. The Cloud Computing shares data, software even hardware. Cloud computing is characterize as an appropriated design that concentrates worker assets on a versatile stage in order to give on request registering assets and administrations. Because of the uncommon accomplishment of web in most recent couple of years, processing assets is currently more universally accessible. What's more, this is empowered the acknowledgment of another processing idea called Cloud Computing. Cloud computing climate requires the customary specialist organizations to have two distinct ways. These are framework and specialist co-ops. Framework suppliers oversee cloud stages and rent assets as indicated by use. Specialist organizations lease assets from foundation suppliers to serve the end clients. Cloud computing has drawn in the goliath organizations like Google, Microsoft, and Amazon and considered as an extraordinary impact in today’s Information about innovation industry. Entrepreneurs are drawn to Cloud computing idea in view of a few highlights, despite the fact that there are greater security issues in the Cloud information access. To improve the security there are greater security techniques and measurements are been executed by the new scientists.

In 1984 Shamir proposed the idea of ID-Based Cryptography (IBC) to eliminate the verification, declaration, and security of public key testaments. In IBC customer's exceptional character, as opposed to an irregular number, email address, as the customer's unhindered key, and the customer's identical private key is produced dependent on the customer's unhindered key by the framework's

ISSN: 2233-7853 IJFGCN

confided in association. The association's believed authority is exceptional and is the addresses of the IBC. It is called Private Key Generator (PKG) or Key Generate Center (KGC) [19]. In current years, a few personality based verification conventions have been proposed for cloud [16, 17, 18]. Yang and Chang [18] proposed a personality based distant client verification convention for portable clients dependent on elliptic bend cryptography (ECC). This convention prevails to the characteristics of both personality based elliptic bend and cryptosystem. To eliminate these security blemishes, Chen et al. introduced a high level secret key based validation convention, which is gotten to give shared verification and is fitting for Cloud Computing air [16]. In 2012, Wang et al. [13] showed that Chen et al. convention isn't secured and powerless to disconnected secret phrase speculating assault and key trade off pantomime assault and furthermore go through from clock synchronization issue. Kang also, Zhang [17] proposed short key size character based verification convention, which includes the calculation of bilinear matching on really solitary elliptic bend bunch with enormous component size where the calculation cost of the blending is around multiple times more than that of elliptic bend point augmentation

Customarily the message is utilized to sign first utilizing digital signature and afterward the message is encryption to accomplish both the confidentiality and data integrity. The plan is ordinarily known as signature-then-encryption conspires. The scheme having two issues: Low productivity and significant expense of such recreation. In Modern Era, to take care of the over two issues another cryptographic strategy is utilized called Signcryption. Signcryption satisfy the both the usefulness of advanced mark and encryption in a solitary sensible advance, however with a decreased expense than Sign-then-Encryption. The proposed method has been implemented by the Forward Secrecy via ECC in a single step for more secure access of the data in the cloud. Forward secure identity based Signcryption is for data sharing in the cloud provide secure data sharing within the group in an efficient manner. It also provides the authenticity and anonymity of the users. This method is a promising candidate to construct an anonymous and authentic data sharing system

1.1 Cloud Models:

The Cloud computing shares the resources like Networking, Platform, Storage and software infra structure to provide service to the needy. The cloud has been classified into

1.1.1 Private Cloud:

Private cloud alludes to a model of distributed computing where IT administrations are provisioned over Private IT foundation for the committed utilization of a solitary association. A private cloud is generally overseen through inside assets.

1.1.2 Public Cloud:

A public cloud is a pool of virtual assetscreated from equipment possessed and oversaw by an outsider organizationthat is naturally provisioned and allotted among numerous customers through a self-administration interface. It's a clear method to scale out jobs that experience unforeseen interest changes.

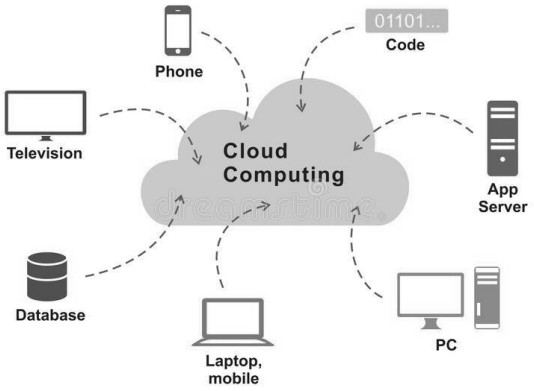
1.1.3 Community Cloud:

A community cloud is a cloud administration model that gives a distributed computing answer for a predetermined number of people or associations that is represented, overseen and gotten usually by every one of the partaking associations or an outsider oversaw specialist co-op.

1.1.4 Hybrid Cloud:

Hybrid cloud administrations are incredible on the grounds that they give organizations more noteworthy authority over their private information. An association can store delicate information on a private cloud or nearby server farm and all the while influence the hearty computational assets of an oversaw public cloud. A hybrid cloud depends on a solitary plane of the executives, dissimilar to a multi-cloud technique wherein administrators should deal with each cloud climate independently.

ISSN: 2233-7853 IJFGCN



1.2Cloud Services:

There are 3 main concepts in Cloud Services they are,

1. Infrastructure-as-a-Service (IaaS)
2. Platform-as-a-Service (PaaS)
3. Software-as-a-Service (SaaS)

1.2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a solitary occupant cloud layer where the Cloud figuring merchant's devoted assets are just imparted to contracted customers at a compensation for every utilization expense. This extraordinarily limits the requirement for colossal introductory interest in figuring equipment like workers, organizing gadgets and preparing power. They likewise permit changing levels of monetary and utilitarian adaptability not found in inward server farms or with collocation administrations, in light of the fact that processing assets can be added or delivered substantially more rapidly and cost-successfully than in an inward data center or with a collocation administration [5]. IaaS and other related administrations have empowered new companies and different organizations centeron their center capabilities without stressing a lot over the provisioning and the board of framework. IaaS totally preoccupied the equipment underneath it and permitted clients to devour infrastructure as a help without trying anything about the fundamental intricacies. The cloud has a convincing incentive as far as cost, yet 'out of the container' IaaS just gives fundamental security (border firewall, load adjusting, and so on) and applications moving into the cloud will require more significant levels of safety gave at the host.

1.2.2 Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a bunch of programming and advancement instruments facilitated on the supplier's workers. It is one layer above IaaS on the stack and edited compositions away everything up to Operating system, middleware, and so on this offers an incorporated arrangement of engineer climate that a designer can tap to fabricate their applications without having any hint about what is happening under the assistance. It offers designers an assistance that gives a total programming improvement life cycle the board, from wanting to plan to building applications to arrangement to testing to upkeep. All the other things is preoccupied away from the "see" of the engineers. Platform as an assistance cloud layer works like IaaS however it gives an extra degree of 'leased' usefulness. Customers utilizing PaaS administrations move much more expenses from capital speculation to operational costs yet should recognize the extra limitations and perhaps some level of lock-in presented by the extra usefulness layers. The utilization of virtual machines go about as an impetus in the PaaS layer in Cloud figuring. Virtual machines should be ensured against malignant assaults, for example, cloud malware. In this manner keeping up the uprightness of uses and well upholding exact validation checks during the move of information across the whole systems administration channels is basic.

ISSN: 2233-7853 IJFGCN

1.2.3 Software as a Service:

Software-as-a-Service is a product dispersion model in which applications are facilitated by a seller or specialist organization and made accessible to clients over an organization, normally the Web. SaaS is turning into an inexorably common conveyance model as hidden advancements that help web administrations and administration arranged engineering (SOA) develop and new formative methodologies become famous. SaaS is additionally regularly connected with compensation asyougo membership permitting model.

1.3 Cloud Characteristics

There are various cloud computing characteristics for provide a good service to the users. The characteristics

1.3.1 On-demand self-service

A customer can get to various administrations viz. registering abilities, stockpiling administrations, programming administrations and so forth depending on the situation consequently without specialist co-op's mediation [6].

1.3.2 Broad network access

To profit distributed computing administrations, web fills in as a spine of distributed computing. All administrations are accessible over the organization and are likewise available through standard conventions utilizing web empowered gadgets viz. PCs, PCs, cell phones and so forth [6].

1.3.3 Resource pooling

The assets that can be allocated to clients can be preparing, programming, stockpiling, virtual machines and organization transfer speed. The assets are pooled to serve the clients at a solitary actual area as well as at various actual areas as per the optimality conditions (for example security, execution, buyer interest). The cloud gives an impression of asset area freedom at lower level (for example worker, center) however not at the more elevated level (for example datacenter, city, country) [6].

1.3.4 Rapid elasticity

The excellence of distributed computing is its flexibility. The assets appear to clients as inconclusive furthermore, are additionally available in any amount whenever. The assets can be provisioned without specialist organization intercession and can be rapidly scale in and scale out as per the client needs in a safe manner to convey top notch administrations [6].

1.3.4 Measured service

A metering ability is sent in cloud framework to charge clients. The clients can accomplish the diverse nature of administrations at various charges to enhanced assets at distinctive degree of reflection appropriate to the administrations (for example SaaS, PaaS, and IaaS) [6].

II. RELATED WORK

2.1 Signcryption:

YuliangZheng [8] characterizes signcryption as cryptographic crude which joins both the elements of advanced signature and public key encryption legitimately in a solitary advance, and with a computational expense fundamentally not exactly that required by the customary sign thenencryption approach. Doing encryption and computerized signature activities independently is pricey as far as computational expense and correspondence overhead due to the calculation on huge numbers and broadened bits created during and after the tasks. Y.Zheng [8] certified that signcryption limits computational expense and correspondence overhead.

ISSN: 2233-7853 IJFGCN

A signcryption conspire ordinarily comprises of three calculations: Key Generation, signcryption, Unsigncryption. The key age calculation creates every one of the public keys needed for signcryption and unsigncryption.The key age calculation creates every one of the public keys needed for signcryption and unsigncryption. Signcryption calculation is a probabilistic calculation which produces signature and ciphertext. What's more, Unsigncryption calculation is deterministic in nature which confirms the realness of mark and performs decoding. Any signcryption plan ought to have the accompanying properties [9]:

2.2 Elliptic Curve Cryptography:

Cryptography is a electronic technique that is used to protect valuable data over transmission. Mainly cryptography is science to provide security to information. To protect our data by using different authentication scheme is the main objective of cryptography. when authentication of data is main consider that should be less cost than the value of original information.

Two main terms that is used for the cryptography technique are Encryption and Decryption. Encryption technique is used to send confidential data over communication .The process of encryption require two things (1) an encryption algorithm and (2) key.

Decryption is the reverse process of encryption. It is technique to convert the encrypted data to its original data that is now readable. Decryption technique need separate Decryption algorithm and a key. Encryption and Decryption algorithm are same.

Elliptical curve cryptography (ECC) is a (PKC) public key encryption technique based on elliptic curve theory that can be used to create faster in speed, smaller in size, and more efficient Cryptographic keys to provide authentication scheme to RFID system. ECC is PKC based crypto system like RSA (Rivest- Shamir-Adleman) but it different from RSA because of its quicker evolving capacity and it provide attractive and alternative way to researchers to create cryptographic algorithm according to their requirement that means how much security they want to provide to the system.

$y^2 = x^3+ax+b$ (1)

Common Public Elements:

Step 1: $E_q(a,b)$ elliptic curve has the parameter a, b and q whereas q is called as prime number

Step 2: G is the point of elliptic curve has the large number n.

User X Key Generation:

Step 1: Choose the private key n_A; $n_A<n$

Step 2: Compute the public key P_A

Step 3: $P_A = n_A G$

User Y Key Generation:

Step 1: Choose the private key n_B; $n_B<n$

Step 2: Compute the public key P_B

Step 3: $P_B = n_B G$

Compute the Secret Key for X:

Step 1: $K=n_A P_B$

Compute the Secret Key for Y:

Step 1: $K=n_B P_A$

ISSN: 2233-7853 IJFGCN

Encrypting by X for Y's Public Key

Step 1: Alice chooses message P_m and a random positive integer 'k

Step 2: Cipher text $C_m = \{k_G, P_m + kP_B\}$

Decryption by Y from his own key:

Step 1: Ciphertext C_m

Step 2: $= P_m + k(n_BG) – n_B (kG)$

III. PROPOSED WORK

Allow us to accept we have two associations X and Y. X and Y go about as public cloud with information, programming and applications. A need to send information to Y's cloud safely and information ought to be validated. Here the concept of attempting to send protected information from X to Y by applying signcryption in Elliptic curve cryptography. Assume Y needs information from X's cloud then, at that point Y's client will put a solicitation to X's client. X's client select comparing information from X's cloud information storage capacity, sign the information with his private key and encode marked information with Y's public key utilizing Elliptic Curve calculation all the while. Signcrypted information will be ship off Y. Y's programming unscramble the scrambled information got with his private key and confirm the mark with X's public key in a solitary calculation.

Start Up:

The Security Parameter λ, the PKG will generate 2 random k bit of primary numbers such as p and q where$p=2p' + 1$ *and* $q=2q' + 1$ were $p' q'$ are prime numbers. This computes the value as N=p*q. from the parameter choose the prime number e $2^l < w < 2^{l+1}$ and gcd$(e,\phi(N))=1$. Choose 2 hash function $H1:\{0,1\}^* \rightarrow ZN^*$ and $H2 : \{0,1\}^* \rightarrow \{0,1\}$. The public parameters are $(k,l,e,N,H1,H2)$ and master secret key msk is(p,q)

Extraction:

For the user i, belongs to Z with the identity $i \epsilon \{0,1\}^*$ with the time period for the secret key where $0 \leq t < T$, to compute the PKG of the user key using factorization of N

$$sk_{i,t} = [H1(Id_i)]e^{\frac{1}{(T+1-t)}} \ mod\ N$$

Update:

Secret Key skI,t for the period of the time t were as t<T the updating of the user secret key or the key will be expired.

Encryption:

To encrypt the message whereas m $\epsilon \{0,1\}^*$ in the period of time t where $0 \leq t < T$

1) For all iϵ{1,….,n},I ≠ π, then choose the random $A_i \epsilon Z^*N$ and compute

$$R_i = Ai^{e\frac{1}{(T+1-t)}} \ mod\ N \text{ and } hi=H2(L,m,t, Id_i,R_i)$$

2) Form the random number Aπ ϵ Z*N

$$R\pi = A\pi^{e\frac{1}{(T+1-t)}}$$

$$\prod_{i=1,i\neq\pi}^{n} H1(IDi)^{-hi} \ mod\ N$$

$$h_\pi = H2(L,m,t, Id_\pi,R_\pi)$$

ISSN: 2233-7853 IJFGCN

Comparison:

For verifying the signature σ for all message m, in that the list tf identifies L and the time t, hi=H2 (L,m,t,Idi,Ri) for j= 1,….,n

$$\prod_{i=1,i\neq\pi}^{n} (Ri.Hi(IDi)^{-hi} \ mod\ N$$

Comparison is checked for valid or not .

IV. CONCLUSION

The Forward Secure ID-Based Signature endorses an ID-based sign plan to have forward security. It is the first in the writing to have this component for sign in ID-based setting. The plan gives unlimited obscurity and can be demonstrated forward-secure unforgeable in the aimless prophet model. The plan is effective and does not need any blending tasks. The size of utilizer secret key is only one whole number, while the key update measure just requires an exponentiation. This will be entirely utilizable in numerous other useful applications, particularly to those require utilizer protection also, verification, like impromptu organization, online business exercises and perspicacious framework. The framework withal executed in multi-cloud framework to enhance the proficiency, sizably voluminous capacity and information sharing framework. Accordingly Reduce calculation involution of assignment and confirm. Decrease existence essentials improve the expense proficient instrument. The current plot depends on the discretionary prophet hypothesis to demonstrate its security. Think about a provably secure plan with similar highlights in the standard model as an open problem and our future exploration work

REFERENCES

[1] Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou “Cost-effective authentic and anonymous data sharing with forward security”.DOI:10.1109/TC.2014.2315619,IEEE Transactions on Computers.
[2] Javier Herranz IIIA, “ Identity-Based Ring Signatures From RSA ” Artificial Intelligence Research Institute, CSIC, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain
[3] MihirBellare and Sara K. Miner” A Forward-Secure Digital Signature Scheme” Dept. of Computer Scienc e, &EngineeringUniversity of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA.
[4] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, “Security And Privacy-Enhancing Multicloud Architectures” Member, IEEE,Luigi Lo Iacono.
[5] Gene ItkisBoston University Computer Science Dept.111 Cumming ton St.Boston, “Forward security: Adaptive cryptography-time evolution”MA 02215, USAitkis@bu.edu
[6] Y. Wu, Z. Wei, and R. H. Deng.” Attribute-based access to scalable media in cloud-assisted content sharing networks” .IEEE Transactions on Multimedia, 15(4):778–788, 2013.
[7] A. Shamir. “Identity-Based Cryptosystems and Signature Schemes”.In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science,pages 47–53. Springer, 1999.
[8] D. S. Wong, K. Fung, J. K. Liu, and V. K. Wei. “On the RS-CodeConstruction of Ring Signature Schemes and a Threshold Settingof RST”. In ICICS, volume 2836 of Lecture Notes in Computer Science,pages 34–46. Springer, 2003.
[9] P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong. A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity (extended abstract). In ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166–183. Springer, 2010.
[10] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forward- secure identity-based signature: Security notions and construc- tion. Inf. Sci., 181(3):648– 660, 2011.
[11] H. Xiong, Z. Qin, and F. Li. An anonymous sealed-bid electronic auction based on ring signature. I. J. Network Security, 8(3):235– 242, 2009.
[12] W. Susilo, Y. Mu, and F. Zhang.Perfect Concurrent Signature Schemes. In ICICS 2004, volume 3269 of Lecture Notes in Computer Science, pages 14–26. Springer, Oct. 2004.

ISSN: 2233-7853 IJFGCN

[13] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. Privacy- preserving public auditing for secure cloud storage. IEEE Trans. Computers, 62(2):362– 375, 2013.
[14] G. Yan, D. Wen, S. Olariu, and M. Weigle. Security challenges in vehicular cloud computing. IEEE Trans. Intelligent Transportation Systems, 14(1):284– 294, 2013.
[15] X. Cao, W. Kou, and X. Du, "A pairing-free identitybased authenticated key agreement protocol with minimal message exchanges".Information Sciences, pp. 2895-2903, 180, 2010.
[16] T.H. Chen, H. Yeh and W. Shih " An advanced ECC dynamic id-based remote mutual authentication scheme for cloud computing". 2011 Fifth FTRA international conference on multimedia and ubiquitous engineering, IEEE Computer Society, pp.155-159.2011.
[17] L. Kang and X. Zhang "Identity-based authentication in cloud storage sharing". In: International conference on multimedia information network and security (MINES). IEEE Computer Society.pp. 851-855, 2010.
[18]J.H. Yang. And C.C. Chang " An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem". Computers & Security, pp. 138-143, 28(3), 2009

ISSN: 2233-7853 IJFGCN