International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Data sharing in cloud computing using forward security Authentication

Mr.V.Sudarshan[1] , Mr.A.Dileep Kumar [2] and Ms. Vemulapalli Bhavya [3]

[1] Associative Professor ,Department of Computer Science & Engineering,Khammam Institute of Technology & Sciences(KITS),Khammam,T.S-India, sudharshan.cse@gmail.com. [2]

[2]Asstistant Professor ,Department of Computer Science & Engineering, Khammam Institute of Technology & Sciences(KITS), Khammam ,A.P-India, achinni.dileepkumar@gmail.com

[3]PG Scholar Department of Computer Science & Engineering, Khammam Institute of Technology & Sciences(KITS), Khammam ,A.P-India vemulapallibhavya1992@gmail.com

Abstract In the advanced cloud computing world Data sharing has never been more facile task. Data communication with a sizably voluminous number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Cellular automata image is a promising candidate to construct an innominate and authentic data sharing system. The segmented sanctions a data owner to anonymously authenticate his data which can be put into the different places of cloud for storage or analysis purport. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Forwarded Identity-predicated (IDbased) ring signature which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of Forwarded ID-predicated ring signature by providing with segmented cellular automata scheme. If a secret key of any utilizer has been compromised, all precedent engendered segments that include with a utilizer still remain valid. This property is especially consequential to any immensely colossal scale data sharing system, as it is infeasible to ask all data owners to re authenticate their data even if a secret key of one single utilizer has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

Keywords: Authentication, data sharing, cloud computing, forward security, smart grid

1. Introduction

Now a day's network security becomes a crucial quandary. When we aurally perceive network security we might only cerebrate hackers. The main goal of network security is providing authentication, integrity, consistency etc. To maintain security of network data sundry methods, technology and algorithms are utilized. It obviates data to being hack by hackers. Maintaining the authenticity of the data that signifies only sanctioned or legitimate utilizer can access the data which is shared by utilizing network. To check sender's authenticity and sender's data verification in network sundry techniques are utilized such as digital certification and VPN. But cost of such technology is very extravagant. The project provides a cost efficient way to securely shared authentic data between clients.

It is a networking and information security predicated project used to surmount the cost of checking certification when data are shared on network predicated. The main concept of this application to provide cost efficient way for certification and data security. For minute

organization or start up organization the other techniques that are utilized nowadays are very extravagant. Such organization can't afford such kinds of solution to checking certification. The project is felicitous for minuscule and commence up organization. The structure and design of this application is utilizer amicable. Anyone can facilely operate this application. The project design and architecture are to fortify scalability for enhancements and facilitate of changes as well as amicable utilization from users of the system.

Cloud computing is additionally kenned as on-demand computing. As the term betokens cloud computing provides sharing of resources and data among computers or other network contrivances through Internet on the substructure of utilizer demands. Could system holds sundry resources like network, storage, applications, accommodations, software's and servers. These resources can be shared on demand by the utilizer with the could sanction. Cloud will enable utilizer to access pool of resources and it is rapidly managed by cloud with minimal effort. Cloud storage provides users/companies/institutions to store and process their sundry types of data through third party data centers.

Due to the advantages of high computing potency, frugal cost of accommodations, high performance, scalability, accessibility as well as availability, cloud computing has become highly injuctively sanctioned utility. Cloud computing has some drawbacks, that need to be addressed to make cloud computing accommodations more reliable and utilizer cordial. The present availability of high-capacity networks, low-cost computers and storage contrivances as well as the adoption of hardware virtualization, accommodation-oriented architecture, and autonomic and utility computing have led to a magnification in cloud computing.

Cloud computing provides wide range of storage accommodations, data security, data integrity and data sharing. Data sharing with several cloud users must be secured. There is a chance of hacking data by the assailer during data sharing. To eschew data leakage sundry mechanisms have been implemented. Each one will fixate on data security while data sharing. Ring structure is one of the mechanisms that will sanction the utilizer to anonimize the data and provides authentic data sharing scheme. Ring structure mechanism uses user's certificate to verify whether the utilizer in the group is authenticated or not. Certificate verification conventionally crosses the economic cost of the utilizer. So it is a major quandary to utilize ring structure for data sharing.

2.Related Work

2.1 Existing System:

Utilizer uploading the data to a third party platform such as Microsoft Hohm. From the accumulated data a statistical report is engendered, and one can compare their energy consumption with others (e.g., from the same block). This faculty to access, analyzes, and responds too much more precise and detailed data from all levels of the electric grid is critical to efficient energy utilization.

At this point Datacenter's signature is equivocal and so C will not be convinced of anything at all by visually perceiving it. We visually perceive that the tendering process is immune to abuse by A. Integrating forward security to it can further ameliorate the security aegis level. With forward security, the key exposure of either party does not affect the e-contracts anteriorly signed

2.2 Proposed System:

Data sharing with an astronomically immense number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an in nominate and authentic data sharing system. It sanctions a data owner to anonymously authenticate his data which can be

put into the cloud for storage or analysis purport. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-predicated (ID-predicated) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-predicated ring signature by providing forward security: If a secret key of any utilizer has been compromised, all anterior engendered signatures that include this utilizer still remain valid. This property is especially paramount to any sizably voluminous scale data sharing system, as it is infeasible to ask all data owners to re-authenticate their data even if a secret key of one single utilizer has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

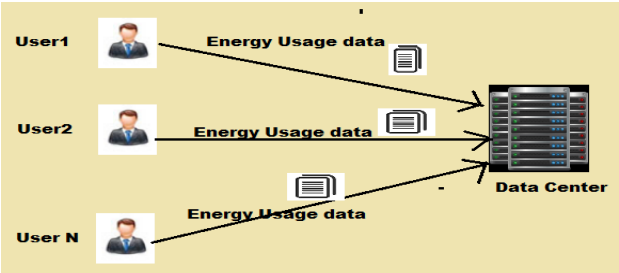

Fig 1. Energy usage data sharing in smart grid.

3. Implementation

After careful analysis the system has been identified to have the following modules:

- **Authentication.**
- **Data sharing.**
- **Cloud computing.**
- **Identity-based Ring Signature**
- **Forward security.**
- **Smart grid.**

Authentication:

Authentication is the act of attesting the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of verbally expressing or otherwise designating a claim purportedly attesting to a person or thing's identity, authentication is the process of genuinely corroborating that identity. It might involve corroborating the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ascertaining that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

Data Sharing:

Data sharing is the practice of making data utilized for scholarly research available to other investigators. Replication has a long history in science. The motto of The Royal Society is 'Nullius in verba', translated "Take no man's word for it."[1] Many funding agencies, institutions, and publication venues have policies regarding data sharing because transparency and openness are considered by many to be a component of the scientific method.

A number of funding agencies and science journals require authors of peer-reviewed papers to apportion any supplemental information (raw data, statistical methods or source code) obligatory to understand develop or reproduce published research. A great deal of scientific research is not subject to data sharing requisites, and many of these policies have liberal exceptions. In the absence of any binding requisite, data sharing is at the discretion of the scientists themselves. In integration, in certain situations agencies and institutions proscribe or rigorously limit data sharing to bulwark proprietary intrigues, national security, and subject/patient/victim confidentiality. Data sharing may withal be restricted to bulwark institutions and scientists from utilization of data for political purposes.

Data and methods may be requested from an author years after publication. In order to enhearten data sharing and obviate the loss or

corruption of data, a number of funding agencies and journals established policies on data archiving.

Cloud computing:

Cloud computing is a computing term or metaphor that evolved in the tardy 2000s, predicated on utility and consumption of computer resources. Cloud computing involves deploying groups of remote servers and software networks that sanction different kinds of data sources be uploaded for authentic time processing to engender computing results without the desideratum to store processed data on the cloud.

Identity-based Ring Signature:

Private or hybrid Identity-predicated (ID-predicated) cryptosystem, introduced by Shamir,eliminated the desideratum for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an IDbased cryptosystem, the public key of each utilizer is facilely computable from a string corresponding to this user's publicly kenned identity (e.g., an electronic mail address, a residential address, etc.). A private key engenderer (PKG) then computes private keys from its master secret for users. This property eschews the desideratum of certificates (which are obligatory in traditional public-key infrastructure) and associates an implicit public key (utilizer identity) to each utilizer within the system. In order to verify an ID-predicated signature, different from the traditional public key predicated signature, one does not require verifying the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a paramount preserve in communication and computation when an immensely colossal number of users are involved (verbalize, energy utilization data sharing in astute-grid).

Forward security:

In cryptography, forward secrecy (FS; withal kenned as impeccable forward secrecy, or PFS) is a property of key-acquiescent protocols ascertaining that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

Even worse, the "group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised utilize in the "group" of his cull. As a result, the exposure of one user's secret key renders all aforetime obtained ring signatures invalid (if that utilizer is one of the ring members), since one cannot distinguish whether a ring signature is engendered prior to the key exposure or by which utilizer. Consequently, forward security is an obligatory requisite that an immensely colossal data sharing system must meet. Otherwise, it will lead to an astronomically immense waste of time and resource. While there are sundry designs of forward-secure digital signatures integrating forward security on ring signatures turns out to be arduous. As far as the authors ken, there are only two forward secure ring signature schemes . However, they are both in the traditional public key setting where signature verification involves sumptuous certificate check for every ring member. This is far below copacetic if the size of the ring is immensely colossal, such as the users of an Astute Grid.

Smart grid:

An astute grid is a modernized electrical grid that utilizes analog or digital information and communications technology to amass and act on information - such as information about the deportments of suppliers and consumers - in an automated fashion to amend the efficiency, reliability, economics, and sustainability of the We implement the Keenly intellective Grid example introduced in Section 1, and evaluate the performance of our IDFSRS scheme with veneration to three entities: the private key engenderer (PKG), the energy data owner

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

(utilizer), and the accommodation provider (data center). In the experiments, the programs for three entities are implemented utilizing the public cryptographic library MIRACL , programmed in C++. All experiments were reiterated 100 times to obtain average results shown in this paper, and all experiments were conducted for the cases of jNj = 1024 bits and jNj = 2048 bits respectively. The average time for the PKG to setup the system is shown in Table 4, where the testbed for the PKG is a DELL T5500 workstation equipped with 2.13 GHz Intel Xeon dual-core dual-processor with 12GB RAM and running Windows 7 Professional 64-bit operating system. It took 151 ms and 2198 ms for the PKG to setup the whole system for jNj = 1024 bits and jNj = 2048 bits respectively. The average time for the data owner (utilizer) to sign energy utilization data with different culls of n and T are shown in Fig. 3 and 4, for jNj = 1024 bits and jNj = 2048 bits respectively. The testbed for the utilizer is a laptop personal computer equipped with 2.10 GHz Intel CPU with 4GB RAM and running Windows 7 operating system. The average time for the the accommodation provider (data center) to verify the ring signature with different culls.

4.Experimental Work

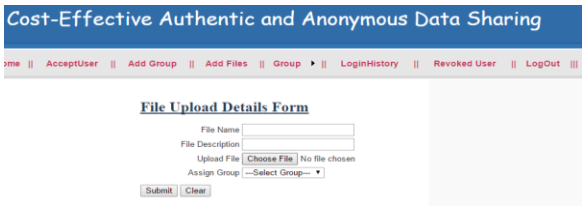

Fig 2: File Upload to cloud details.

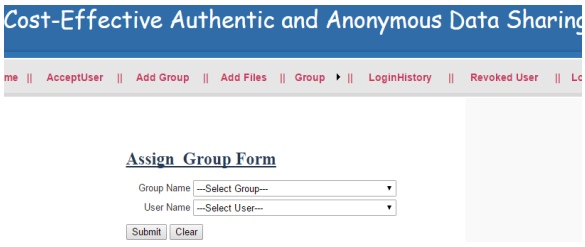

Fig 3: Assigning Group form page.

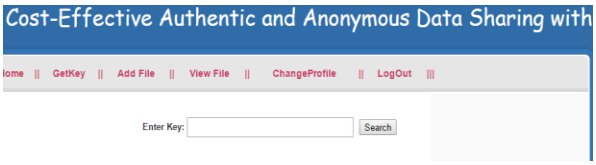

Fig 4: Key search Page.

5. Conclusion

Incentivized by the practical needs in data sharing, we proposed an incipient notion called forward secure ID-predicated ring signature. It sanctions an ID-predicated ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-predicated setting. Our scheme provides unconditional anonymity and can be proven forward-secure unforgivable in the arbitrary oracle model, postulating RSA quandary is hard. Our scheme is very efficient and does not require any pairing operations. The size of utilizer secret key is just one integer, while the key update process only requires an exponentiation. We believe our scheme will be very subsidiary in many other practical applications, especially to those require utilizer privacy and authentication, such as ad-hoc network, e-commerce activities and keenly intellective grid. Our current scheme relies on the arbitrary oracle postulation to prove its security. We consider a provably secure scheme with the same features in the standard model as an open quandary and our future research work.

6. References

[1].M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, “ID-based ring signature scheme secure in the standard model,” in Proc. 1st Int. Workshop Security Adv. Inform. Comput. Security, 2006, vol. 4266, pp. 1–16.

[2] A. K. Awasthi and S. Lal, “Id-based ring signature and proxy ring signature schemes from bilinear pairings,” CoRR, vol. abs/cs/ 0504097, 2005.

[3] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements and a construction based on general assumptions," in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Techn., 2003, vol. 2656, pp. 614–629.

[4] M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.

[5] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul. \Aug. 2013.

[6] A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie-Hellman group signature scheme," in Proc. 6th Int. Workshop Theory Practice PublicKey Cryptography: Public Key Cryptography, 2003, vol. 567, pp. 31–46.

[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc.Annu.Int.Cryptol.Conf.Adv.Cryptol.,2004, vol.3152,pp.41–55.

[8] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, vol. 2442, pp. 465–480.

[9] J. Camenisch, "Efficient and generalized group signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1997, vol. 1233, pp. 465–479.

[10] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sublinear size without random oracles," in Proc. 34th Int. Colloq. Automata, Lang. Programming, 2007, vol. 4596, pp. 423–434.

[11] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing:Avisionforsociallymotivatedresource sharing,"IEEE Trans.Serv.Comput.,vol.5,no.4,pp.551–563,FourthQuarter2012.

V.Sudharshan received the M.Tech degrees in computer science Engineering and Information Technology from the JNTUH University, Hyderabad, in 2005 and 2010, respectively, and is currently pursuing the Ph.D. degree in Computer Science & Engineering at the JNTUH—Hyd..He has a vast experience in network-related software-development from several startup companies. His research interests include Secure Cloud Computing, content caching, cellular networks, and traffic redundancy elimination.

A.Dileep Kumar received the M.Tech degree in Computer Science & Engineering from the University JNTUH, Hyderabad.

Name: Vemulapalli Bhavya:B.tech college: Medha Institute Of Science and Technology (MIST) , B.Tech Percentage: 66 %, khammam, Year of completion: april 2014 B.Tech branch : CSE(Computer Science And Engineering) M.tech: CSE (Computer Science And Engineering)

Mail id:vemulapallibhavya1992@gmail.com
Mobile No:9866724637