IJTRET International Journal of Trendy Research in Engineering and Technology
Volume 3 Issue 1 February 2019
ISSN NO 2582-0958

ACCESSING DATA FROM SMART GRID UNDER SMART CITY MANAGEMENT

DEEPIKA.R[1] , INDHIRA.D[1] , SATHISH KUMAR.P.J[2]
[1]UG Scholar, [2] Assistant Professor, Department of Information and Technology,
S.A.Engineering College Thiruverkadu, Chennai-600077.
muthukumarasamy@saec.ac.in

Abstract: The trend in smart city is partly due to advances in Internet of Things. In any smart city, a significant amount of data is generated at the edge of the network, such as traffic data collected by smart devices on vehicles in smart transportation, and educational multimedia materials captured by and disseminated using smart phones or tablets in smart education. Generally, data is transmitted to the cloud for further processing and storage, which requires significant network resources and has associated security and privacy risks. However, most of the data could be pre-processed to reduce the transmission cost of the network and protect the privacy of the user. For instance, duplicate data cloud be reduced and videos cloud be compressed. To achieve this, some computation is required to be performed at the edge of the network. One commonly seen application in smart city is smart grids, partly due to the rapid digitization of household appliances, service industries, manufacturing processes, etc. Smart meters and other intelligent devices been deployed in each household and business premise, detailed information about the usage of the electricity (and potentially other information) is periodically collected and transmitted to the cloud server.

Keywords: Cloud storage, Cryptography, Data security, Public audit, Secure deduplication, Bilinear pairing, Smart grid.

I. INTRODUCTION

The smart grid is expected to become the next-generation power system and has attracted a lot of attention from both academia and industry over the last decade. Through bidirectional communication and power flows, the smart grid is able to provide more reliable, efficient, and cost-effective power management than the traditional power grid. For example, the execution of the first commercial project using the smart grid technology can save 500 million Euros each year compared with the traditional grid technology. Due to the significant economic benefits, several smart grid projects have been undertaken in various countries recently. Cloud computing technology provides a shared pool of different types of computing resources. By leveraging virtualization technologies, cloud computing can provide extensible services (such as computation, communication, and storage) to users on an on-demand basis. In the cloud paradigm, the cloud service provider is responsible for the underlying cloud infrastructure maintenance and users are only aware of the cloud services that are supported. As a result, the cloud computing reduces user's costs and improves scalability, efficiency, and flexibility. Several types of cloud computing models have been

proposed in the last few decades. For example, Amazon and Google have established and Google App Engine to provide the infrastructure as a service and the platform as a service, respectively.

II.RELATED WORK

To avoid downloading all the data from the remote cloud server, Ateniese *et al* proposed the PDP concept. They also developed a concrete PDP scheme based on the traditional public key cryptography (TPKC). Since their proposal, several PDP schemes based on the TPKC have been proposed for different applications. However, these PDP schemes suffer from the heavy certificate management problem inherited from the TPKC, where the certificate is produced by a trusted third party to establish the relationship between the user's identity and his/her public key. Based on the concept of the identity-based public key cryptography, Wang *et al.* introduced the concept of identity-based PDP to address the heavy certificate management problem that exists in the original PDP scheme. They also defined a security model for the ID-based PDP scheme and proposed a concrete ID-based PDP scheme using bilinear pairing. Then, Wang *et Al* also proposed an ID-based PDP scheme for multicloud storage architectures. To improve the performance, Yu *et al.* proposed an IDbased PDP scheme using the Rivest-Shamir-Adleman (RSA) algorithm. To improve the security, Yu *et al.* proposed an ID-based PDP with perfect data privacy preserving. However, these aforementioned PDP schemes suffer from the key escrow problem, i.e., all users' private keys are generated by the key generation center (KGC), which knows all users' private keys. To address the key escrow problem in the ID-based PKC, Al-Riyami *et al.* proposed the certificateless public key cryptography (CL-PKC). In the CL-PKC, a user's private key consists of two parts. One part is generated by the user and the other part is generated by the KGC. Based on the concept of the CL-PKC, Wang *et al.* proposed the concept and security model of a CL-PDP scheme. However, He *et al.* showed that Wang *et al.*'s CL-PDP scheme is not secure against the type I adversary. To enhance the security, He *et al.* proposed a new CL-PDP scheme using bilinear pairing. Unfortunately, both of Wang *et al.*'s CL-PDP scheme and He *et al.*'s CL-PDP.

III. PROPOSED SYSTEM

Our proposed mechanism is the mobile cloud environment to avoid the data over-collection by the application. The idea is the application should only have the permission requirement based on hardware, and write some content in device storage. It should not contain the permission such as read user contacts, read the internal storage, read external storage, etc... But it can access the data through cloud storage. In cloud environment we implement preliminary processing by cloud provider. The cloud service provider deploying the pre-customized process for all authorized application to access the essential users' datasets. All data stored from various applications in device is exported to the mobile cloud storage in the encrypted form. The mobile cloud has the knowledge, whether to share the respective user data to the application which is requested. If the application is in need of the user data, the application should request the mobile cloud for user data. The mobile cloud validates the application data request based on its need and approve the data request if needed or decline if the request for the data is unnecessary for particular application.

IV. USER LOGIN AND REGISTRATION AND KEY GENERATION

The End User Registration is done by inserting respective values of the particular user and the values are inserted towards the respective fields in database and based on the stored values user login is done with respective user name and password fields using

SELECT statement in sql and user is now authenticated and The Authenticator will generate the respective key for user access.The smart city application provided by the mobile cloud provider (MCP) monitor the other service applications and collect the data stored by the various application in the various locations in the device memory storage. Initially user should register their mobile with the cloud and creating an authorized account there selves through smart city application. This account maintains the credentials of users' can access their cloud data as Google drive wherever using their account credentials.

V.PROBLEM DEFINITION

Current smart phones are not comfort to manage users' sensitive data, and they are facing the privacy leakage caused by data over-collection. Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. Collecting the user data apart from the application requirement. Application data storage in system may lead to the space complexity to store further data.

VI.SECURITY PRELIMINARY PROCESS ON CLOUD SERVICE PROVIDER

Security preliminary process have implemented by the mobile cloud provider. Initially cloud provider must predefine the permission of data accessing for the each android applications. Based on the predefining permission mechanism the android application can access permitted and essential data of user's phone through the cloud. MCP should assigning permission individually for each of the application installed in user's android devices. And the person who knows these security constraints about the android application's permission and data over collection can customize their account on cloud and can assign permissions for each of the application.

VII.DATA PRIVILEGE ON CLOUD MOBILE ENVIRONMENT

Data privilege given by our mechanism is the online cloud drive for user's private data. Users can access their phone updates from the cloud. Using these privilege users can trace their phone while phone theft. Users can customize their phone's permissions on cloud hence we provide the data security. We proposed dynamic permission mapping algorithm to provide the customized application permission environment for data over collection as well as for phone application security. Highly secured and recommended cryptography can apply to the data security on future enhancement.

VIII.APPLICATION PERMISSION ANALYZING ON CLOUD

We proposed permission analyzing and assigning permission of each application. Based on the customization of access permission can provide data to application eventually. Our mechanism insists the application can having the device hardware accessing permission only. And rest of the data collection permission will be redirect to the respective cloud account of each user's.

IX. CONCLUSION

To maintain the normal operation of the smart grid, a huge amount of data is collected and analyzed in real-time. It is difficult for the traditional data management system to process such a large volume of data. To address the problem, cloud computing is introduced into the smart grid and the cloud-based data management system is used in the smart grid. To ensure the integrity of the data in the cloud-based

data smart grid management system, we have proposed an efficient CL-PDPD scheme based on bilinear pairing. Due to its robustness and efficiency, the proposed CL-PDP scheme is more suitable for the cloud-based data management systems.

REFERENCES

[1] R. Davies, "Hydro one's smart meter initiative paves way for defining the smart grid of the future," in Proc. 2009 IEEE Power Energy Soc. Gen. Meeting, 2009, pp. 1–2.
[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," IEEE Commun. Surv. Tuts., vol. 15, no. 1, pp. 5–20, First Quarter 2013.
[3] E. Amazon, "Amazon elastic compute cloud (Amazon EC2)," 2010.
[4] A. Zahariev, "Google App engine," Helsinki Univ. Technol., Helsinki, Finland, 2009, pp. 1–5.
[5] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.
[6] C. Napoli, G. Pappalardo, G. M. Tina, and E. Tramontana, "Cooperative strategy for optimal management of smart grids by wavelet rnns and cloud computing," IEEE Trans. Neural Netw. Learn. Syst., vol. 27, no. 8, pp. 1672–1685, Aug. 2016.
[7] J. Kim and Y. Kim, "Benefits of cloud computing adoption for smart grid security from security perspective," J. Supercomput., vol. 72, no. 9, pp. 3522–3534, 2016.
[8] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. P. Chen, "A survey of communication/networking in smart grids," Future Gener. Comput. Syst., vol. 28, no. 2, pp. 391–404, 2012.
[9] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," Comput. Netw., vol. 56, no. 11, pp. 2742– 2771, 2012.
[10] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.
[11] Y. Yu et al., "Cloud data integrity checking with an identity-based auditing mechanism from RSA," Future Gener. Comput. Syst., vol. 62, pp. 85–91, 2016.