EXECUTION OF DATA ENCRYPTION STRATEGY IN MOBILE CLOUD COMPUTING

[1]G.Sravani , [2]Dr.B.Geetha Vani,

[1] Assistant Professor, [2] Professor ,
Dept. of CSE,
Narayana Engineering College, Nellore, A.P, India

ABSTRACT:
Privacy has become a considerable issue when the applications of big data are dramatically growing in cloud computing. The benefits of the implementation for these emerging technologies have improved or changed service models and improve application performances in various perspectives. However, the remarkably growing volume of data sizes has also resulted in many challenges in practice. The execution time of the data encryption is one of the serious issues during the data processing and transmissions. Many current applications abandon data encryptions in order to reach an adoptive performance level companioning with privacy concerns. A novel data encryption approach is proposed, which is called Dynamic Data Encryption Strategy (D2ES). Proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints. This approach is designed to maximize the privacy protection scope by using a selective encryption strategy within the required execution time requirements. The performance of D2ES has been evaluated in experiments, which provides the proof of the privacy enhancement.

I. INTRODUCTION

Introducing mobile cloud computing techniques has empowered numerous applications in people‟s life in recent years. Involving humans in the cloud computing and wireless connection loops becomes an alternation for information retrieval deriving from observing humans‟ behaviors and interactivities over various social networks and mobile apps. Moreover, as an emerging technology, cloud computing has spread into countless fields so that many new service deployments are introduced to the public, such as mobile parallel computing, and distributed scalable data storage. Penetrations of big data techniques have further enriched the channels of gaining information from the large volume of mobile apps‟ data across various platforms, domains, and systems. Being one of technical mainstreams has enabled big data to be widely applied in multiple industrial domains as well as explored in recent paper works.
Despite many benefits of using mobile cloud computing, there are great concerns in protecting data owners‟ privacy during the communications on social networks or mobile apps. One of the privacy concerns is caused by unencrypted data transmissions due to the large volume of data. Considering an acceptable performance level, many applications abandon using cipher texts in mobile cloud data transmissions. This phenomenon can result in privacy leakage issues since plain texts are unchallenging for adversaries to capture information in a variety of ways, such as jamming, monitoring, and spoofing. This privacy issue is exigent because it faces to a contradiction between the security levels and performance that is usually attached to timing constraints.

II. LITERATURE SURVEY

Cloud computing uses a network of remote servers hosted on the internet to store, manage and process data rather than a local server or a personal computer. Cloud provides the space to store the data i.e. the user can store his data in the cloud service. Attackers now have the ability to use the information to remotely access sensitive data stored on the cloud additionally attackers can falsify and manipulate information through hijackers credentials.Any person can use their authorized access to an organisation cloud-based services to misuse or access information such as customer accounts, financial forms and other sensitive

information.Malware injection is one of the security issue in the cloud based services. Malware injection is executed and the cloud begins operating in tandem with it , attackers can eavesdrop compromise the integrity of sensitive information and steal data. Malware injections are scripts or code embedded into cloud services that acts as "valid instances" and run as software as a service to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of software or service that is running within the cloud servers themselves.

Cloud security is a shared responsibility between the provider and client. Data On cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. Denial of service attacks are designed to prevent users of a service from being able to access the data or applications. By forcing the targeted cloud services to consume inordinate amounts of finite system resources such as processor power, memory ,disk space, or network bandwidth, attacker can cause a system slow down and leaves all legitimate service users without access to services. For users it is necessary to take full advantage of cloud storage service and also to ensure data privacy. Therefore an efficient access control solution has to be developed. The traditional access control strategy cannot effectively solve the security problems that exist in data sharing. Data security issues brought by data sharing have seriously hindered the development of the cloud computing. There are various solutions to achieve encryption and decryption of the data sharing.DDoS attack source traceback is an open and challenging problem. Deterministic packet marking (DPM) is a simple and effective traceback mechanism, but the current DPM based traceback schemes are not practical due to their scalability constraint. We noticed a factor that only a limited number of computers and routers are involved in an attack session. Therefore, we only need to mark these involved nodes for traceback purpose, rather than marking every node of the Internet as the existing schemes doing. Based on this finding, we propose a novel marking on demand (MOD) traceback scheme based on the DPM mechanism. In order to traceback to involved attack source, what we need to do is to mark these involved ingress routers using the traditional DPM strategy. Similar to existing schemes, we require participated routers to install a traffic monitor. When a monitor notices a surge of suspicious network flows, it will request a unique mark from a globally shared MOD server, and mark the suspicious flows with the unique marks. At the same time, the MOD server records the information of the marks and their related requesting IP addresses. Once a DDoS attack is confirmed, the victim can obtain the attack sources by requesting the MOD server with the marks extracted from attack packets. Moreover, we use the marking space in a round-robin style, which essentially addresses the scalability problem of the existing DPM based traceback schemes.

.

III. SYSTEM ANALYSIS

Zhang et al. proposed an approach named SCLPV for cloud-based Cyber Physical Social Systems (CPSS) to avoid malicious auditors. This approach concurrently provisioned certificateless public verification as well as resistance against malicious auditors for the purpose of verifying the integrity of outsourced data in CPSS. Wang et al. focused on developing an approach offering a secure cloud system that could support privacy preserving public auditing. This paper work had explored the method of defining adversaries from the data storage side. One paper work solved the problem by building up a two-dimensional paired connections over the Radio Frequency for Consumer Electronics (FR4CE) for both appliances and controllers, while users attempt to connect with appliances. Another paper work also addressed user machine interaction issues but in a different standpoint. The paper work argued that the significant hemisphere of protecting privacy is establishing an effective approach emphasizing both humans" involvements and system controls. Both sides need to be matched and combined in order to accurately predict adversaries. Multi-channel communications could be considered an alternative using various data protection methods for increasing the level of the privacy protection under different constraints. In addition, the vulnerability detection is also an important aspect of preventing privacy leakage. Mulliner et al. proposed a detective approach that focused on the vulnerabilities caused by the instances of Graphical User Interface (GUI) element misuse. This method considered the misuses of the GUI element attributes in the GUI-based application context. In the context of big data, an efficient privacy policy compliance checking mechanism is a significant part in building up a secure searching system. Lack of tracking functionality in Web browsers can result in privacy issues since adversaries are not surveilled under most current operating environments. An efficient secure networking system can also reduce the rate of the threat amplifications. However, there are a variety of vulnerabilities even though many access control models have been developed.

IV. PROPOSED SYSTEM

We implement an access control scheme called PSACS, which is privilege separation based on privacy protection. The key-aggregate encryption (KAE) scheme and hierarchy attribute-based encryption (HABE) schemes are used to implement read access control scheme in the PSD and PUD. The KAE scheme greatly improves access efficiency. The HABE scheme largely reduces the task of a single authority and protects the privacy of user data.

Dynamic Encryption Determination (DED) algorithm
Require: S Table, M- Table, Tc, Tm
Ensure: P (Encryption Strategy Plan)
Step 1: User upload data „D" to cloud server
Step 2: Assign privacy weight value for uploaded data column.
Step 3: Input S Table, M Table, Tc, Tm
Step 4: while S Table is not empty do
Step 5: Get Di having the highest priority from S Table
Step 6: Arrive encryption strategy
Step 7: Encrypt the column arrived by Step 6
Step 8: Outsource data to cloud server
Step 10: End

V. CONCLUSIONS & FUTURE SCOPE

This work focused on the privacy issues of big data and considered the practical implementations in cloud computing. The proposed approach, D2ES, was designed to maximize the efficiency of privacy protections. Main algorithm supporting D2ES model was DED algorithm that was developed to dynamically alternative data packages for encryptions under different timing constraints. The experimental evaluations showed the proposed approach had an adaptive and superior performance.
Privacy protection technology as a growing academic paper work has a wide range of applications in many fields in recent years. This work focuses on the review of privacy protection technologies involves in data mining. First we introduce the study of privacy protection status and the main paper work method, and then introduce privacy protection methods such as distortion, encryption, privacy and anonymity. For the three protections corresponding literature is illustrated. Because privacy protection technology involves the development of multi-disciplines, there are still many issues to be further study: Mobile data mining and data stream mining concerning about privacy in data mining which is a promising direction. With the growth of spatial and geographic data, new applications based on user mobility patterns of behavior will emerge. Another area of concern is the incremental privacy protection data release, and challenge in this area is to redesign data mining algorithms to process data increment. Finally, in addition to the field-driven paper work, a framework for estimating and comparing a variety of privacy protection data mining algorithms should be design.

VI. REFERENCES

[1] S. Yu, W. Zhou, S. Guo, and M. Guo. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers,65(5):1418–1427, 2016.
[2] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic. Malware propagation in large-scale networks. IEEE Transactions on Knowledge and Data Engineering, 27(1):170–179, 2015.
[3] S. Liu, Q. Qu, L. Chen, and L. Ni. SMC: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Transactions on Big Data, 1(2):68–81, 2015.
[4] S. Rho, A. Vasilakos, and W. Chen. Cyber physical systems technologies and applications. Future Generation Computer Systems, 56:436–437, 2016.
[5] L. Wu, K. Wu, A. Sim, M. Churchill, J. Choi, A. Stathopoulos, C. Chang, and S. Klasky. Towards real-time detection and tracking of spatio-temporal features: Blob-filaments in fusion plasma. IEEE Transactions on Big Data, 2(3), 2016.
[6] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar. Dependable demand response management in the smart grid: A stackelberg game approach. IEEE Transactions on Smart Grid, 4(1):120–132, 2013.
[7] M. Qiu, M. Zhong, J. Li, K. Gai, and Z. Zong. Phase-change memory optimization for green cloud with genetic algorithm. IEEE Transactions on Computers, 64(12):3528–3540, 2015.

[8] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. Yang. Role-dependent privacy preservation for secure V2G networks in the smart grid. IEEE Transactions on Information Forensics and Security, 9(2):208–220, 2014.
[9] F. Tao, Y. Cheng, D. Xu, L. Zhang, and B. Li. CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system. IEEE Transactions on Industrial Informatics, 10(2):1435–1442, 2014.
[10] G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, and X. Qin. A decentralized approach for mining event correlations in distributed system monitoring. Journal of parallel and Distributed Computing, 73(3):330–340, 2013.
[11] F. Schuster, M. Costa, C. Fournet, C. Gkantsidis, M. Peinado,G. Mainar-Ruiz, and M. Russinovich. VC3: Trustworthy data analytics in the cloud using SGX. In IEEE Symposium on Security and Privacy , pages 38–54, San Jose, CA, USA, 2015. IEEE.
[12] M. Maffei, G. Malavolta, M. Reinert, and D. Schroder. Privacy and access control for outsourced personal records. In IEEE Symposium on Security and Privacy, pages 341–358, San Jose, CA, USA, 2015.IEEE.
[13] C. Mulliner, W. Robertson, and E. Kirda. Hidden GEMs: Automate discovery of access control vulnerabilities in graphical user interfaces.In IEEE Symposium on Security and Privacy, pages 149–162, San Jose, CA, USA, 2014. IEEE.
[14] S. Sen, S. Guha, A. Datta, S. Rajamani, J. Tsai, and J. Wing. Bootstrapping privacy compliance in big data systems.In IEEE Symposium on Security and Privacy, pages 327–342, San Jose, CA, USA, 2014.IEEE.

[15] J. Vilk, D. Molnar, B. Liv shits, E. Ofek, C. Rossbach, A. Moshchuk,H. Wang, and R. Gal. SurroundWeb: Mitigating privacy concerns in a 3D web browser. In IEEE Symposium on Security and Privacy, pages 431–446, San Jose, CA, USA, 2015.IEEE.
[16] L. Zhu, Z. Hu, J. Heidemann, D. Wessels, A. Mankin, and N. So-maiya. Connection-oriented DNS to improve privacy and security. In IEEE Symposium on Security and Privacy, pages 171–186, San Jose,CA, USA, 2015. IEEE.