IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 1, Ver. I (Jan.-Feb. 2017), PP 79-81
www.iosrjournals.org

Security and Privacy of Big Data in Mobile Devices

Zulkhairi B Md Dahalin[1], Azman Ta'a[2], Ahmed Babalaji Ndanusa[3]
[1,2,3]*Dept. of Information Technology, College of Arts and sciences, Universiti Utara Malaysia, Malaysia.*

Abstract: *Presently, the volume of data generated via mobile devices is at an exponential rate due to the rapid advancement in internet-enabled mobile devices, which makes it complex to ensure the privacy and security of this data. Cloud-based server is currently considered one of the most reliable solutions to address these issues. Nevertheless, the increasing uncertainties of storing useful and sensitive big data in a public cloud have suppressed the exploration of this option. In our paper, we meticulously reviewed the drawbacks in the current adopted solutions for security and privacy of big data within mobile devices. As the utilization of mobile platforms is increasingly generating large data, the current traditional methods of cryptography will not be able to efficiently ensure the security and privacy of this big data. Therefore, this paper will propose the utilization of Federated Identity Management that is Openstack cloud-based as an effective solution that can ensure the privacy and security of big data within mobile device ecosystem.*

Keywords: *Big Data; Cloud computing; Encryption; Privacy; Security*

I. Introduction

The continuous use of mobile devices has induced an exponential growth of data within the domain of telecommunications [1]. This usage ranges from social media, banking transactions and educational purposes [2]. The activities involved in the utilization of mobile devices have led to the generation of varied and massive amount of data being acquired at a very high velocity for distinctive purposes (Variety, Volume, Velocity, Volume and Value); a typical characteristics of Big Data (5Vs) [3]. This big data can be utilized by government or an organization to support decision-making in areas of law enforcement, creating awareness, security as well as social services. Nevertheless, this intrusive tendency may not always be accepted by the targeted individuals [4]. Although, this big data can help in proffering useful information, however, it also presents monumental issues with regards to storage and its corresponding costs, and above all, the security of the stored data. In reality,one of the primary limitations of big data in mobile devices is the lack of individual privacy [4].

Additionally, the absence of defined regulations amongst ecommerce providers has continued to expose the security and privacy of this big and sensitive data. For instance, a user's profile and the records of transaction made can be privately kept by an ecommerce provider; on the other hand, the same details may not be protected by another provider. Thus, placing the user at a high risk once these unprotected data sets are perceived by a hacker.Therefore, the need for an implementation of a defined and common standardization amongst ecommerce websites, as well as other web site that profile users' private detailsin order to protect the records as well as the details of a user that are generated when exploring mobile devices [5].Because as the devices are being explored, traces of the users' transactional activities and his or her locations are retained [4]. Furthermore, the current proliferation of internet-enabled mobile devices and the continuous concern on privacy and data security displayed by users require an adoption of a more prudent safety measures to address issues related to the privacy and security of big data in mobile ecosystem [6].According to the Data Protection Directive of the EU, processing personal details of a user can only be performed based on a specific motive (Art. 6,1), Directive 95/46/EC) [7].The novel approach of utilizing big data hassubjected the concept of "compatible utilization" to a certain level of pressure by outspreading and broadening its significance. As this new techniques of using big data have put the notion of "compatible use" under pressure by extending and stretching its meaning which consequentlyjeopardizesthe privacy of the users [6].Furthermore, the EU generally believes confidentiality is a fundamental human right which frowns at rendering users vulnerable to attacks or being targeted. This pertains the confidentiality of personal details of users and the use of those details. Whereas for organizations, this privacy encompasses the adoption of laws and policies to ensure a proper handling of Personally Identifiable Information (PII)[8].Therefore, as the need for mobile devices increases, the necessity for privacy and the security of this big data equally requires a corresponding enhancement.In this paper, we proposea solutionwhich can efficiently accomplish the privacy and security of big data in mobile devices using a novel open source approach to address the existing security and privacy gaps in mobile ecosystems.Our various contributions are segmented into three-folds. Firstly, the paper discusses the vulnerability of big data in mobile devices, the growing concern shown by the users and the need to implement privacy and security measuresas well as a standard policy to ensure privacy and security of big data in mobile devices. Secondly, section tworeviews thepros and cons insome of the related work which are aimed at addressing the numerous challenges of big data privacy and security in order to propose a solution to the aforementioned problems, whilesection

three explains the proposed solution using Federated Identity in an open source environment, and finally the conclusion.

II. Related Work

The current approaches utilized in cloud-based solutions to store data in a clear form on a serve owned and managed by another firm or organization to implement security and privacy measures of big data within mobile devices pose inherent limitations as discussed by the following works:

In a study conducted in [8], the aim was to ensure finegrainedness, data privacy as well as simultaneous scalability. A schema was proposed to attain the objective by utilizing both KPABE and exclusively combining it with approaches related to proxy re-encryption and lazy re-encryption. Additionally, the proposed schema permits data to be delegated on most of computational overhead by owners to potent cloud-based servers, which ensured the privacy ofaccess rights assigned to users as well as the accountability of the confidential key. The efficiency of the cryptography model in ensuring the data privacy of the schema was confirmed by Formal Security**.**Although, the schema permits the delegation by the owners, however, the schema **s**upports only a single privilege consequently; it is not a suitable solution [9], as multiple privileges will be required to manipulate the big data that is securely stored on a server.

Similarly, in a study conducted in [10], a data outsourcing and sharing framework was used on hybrid-based cloud computing of both public and private cloud storage. Within this approach, the encrypted data was tested using the storage server and a similar value was returned without knowing the data or the decryption key. In this framework contrary to the previous work, a dual-layered access control was supported by the framework. On the first layer, the rights of users to delegate are provided by the trusted private cloud in order to achieve a secured access control mechanism.While the second layer ensures the restriction of encrypted data by the owner using the access control mechanism. The result of this framework indicates the confidentiality of the message and the keyword.Despite the success recorded in ensuring the data privacy, this technique is constrained by some limitations because, proffering security within a hybrid cloud that involves numerous service providers is more complex, particularly in the distribution of the key as well as in the shared authentication [11].Also for users to access the services in a cloud, a user digital identity is needed for the servers of the cloud to manage the access control. While in the whole cloud, there are many different kinds of cloud and each of them has its own identity management system. Thus, user who wants to access services from different clouds needs multiple digital identities from different clouds which will inconvenience the user. However, using federated identity, a user can access different services from cloudswhich will considerably mitigate the various security and privacy issues of big data in the mobile ecosystem [11] as presented in the ensuingsection:

III. Federated Identity

Identity in this context represents the elements related to personal data that are restricted to Personal Identifying Information (PII), which are the details associated to an individual that aid in his or her identification. In a nut shell, the PII is simply associated with the attributes of individuals, such as the color of the hair, vocal sound, names, qualifications as well the medical records[12].

3.1Addition OfFederated Identity Management To Openstack

OpenStack is a cloud-based open source computational environment attracting a lot of attention because of its strength in Federated Identity Management (FIM) which enables authentication as well as authorization to be implemented with flexibility**.**There is no license requirement for hardware or software covering the installation of the service tools of this platform and can equally be personalized [12]. The various service tools include [13]**:**

- Swift: The block storage and object storage are provided by this storage services;
- Nova: Voluminous network of virtual machines are provided and managed by this services;
- Neutron: The Internet Protocol addresses and networks are managed by this network services;
- Nova: Voluminous network of virtual machines are provided and managed by this services;
- Glance: The image-based services that proffers registration, finding and transferring of virtual machine images. It utilizes the services of Swift in storing images, while it uses Neutron in transferring those images, and Nova services to execute them;
- Keystone: The token required to authenticate users in order to authorize them the use of numerous OpenStack service that is provided by this identity service. The platform uses the token to obtain the user's authorization identification, his domain and his corresponding rights. These services utilize either access control to define which rights are accessible to the roles, or the utilization of Access Control Lists (ACL) to grant access to individuals with the aid of any of the corresponding token formats in the following subsection.

1.1.1 Token Formats

Keystone provides numerous token formats explained as thus[14]:

1. UUID Token: The format of UUID token is an arbitrarily generated 32-character string which are distributed and validated by the services of identity. In order to ensure that the token contains only hexadecimal digits, a hexdigest() method is utilized. This method renders tokens URL safe and friendly to transfer within a non-binary location.A typical UUID token caries the format of: 621ba557bd1c3821bbc5def0498fk339. The token is stored in a database for subsequent validation. In the case of revoking a UUID token, a request using "Delete"command is made with the corresponding desired ID in order to remove the token.
2. PKI Tokens: The token within the PKI formats possesses the whole validation response acquired from keystone that entails the issuing and the expiring data, the ID of a user, domain, rights services as well as other details which are represented in JSON-based document payload, while the payload is signed with cryptographic message syntax (CMS). The token caries the formats of:NYYDsAYCCAokGCSqGSIb3DQEHAaCCAnoEggJ2ew0KICAgICJhY2QogICAgICAgI...EBMFwwVzELMAkGA1UEBhMCVVMxDjAHMgHHBAgTBVVuc2V0MCoIIDoTCCA50CAQExCTAHBgUrDgMQ4wDAYDVQQHEwVVbnNldDEOMAwGA1UEChM7r0iosKscpnfCuc8jGMobyfApz/dZqJnsk4lt1ahlNTpXQeVFxNK/ydKL+tzEjg
3. Fernet Tokens: This is an improved format of the aforementioned tokens in various ways containing 255 characters. Firstly, it is relatively small compared toPKI but larger than UUID tokens. Additionally, it encompasses sufficient information to allow the token possess details that the remaining required information can be generated. The format is: gAAAAABU7roWGiCuOvgFcckec-0ytpGnMZDBLG9hA1Hr9qfvdZDHjsak39YN98HXxoYLIqVm19Egku5YR3wyI7heVrOmPNEtmrfIM1rtahudEdEAPM4HCiMrBmiA1Lw6SU8jc2rPLC7FK7nBCia_BGhG17NVHuQu0S7waA306jyKNhHwUnpsBQ%3K.Anditsvalidation is done by performing a similar reverse process in the creation of the token.

IV. Conclusion

In this paper, we have proposed an open source solution using Openstack and Federated Identity Management (FIM), which is aimed at proffering an effective and efficient means of ensuring the security and privacy of big data within mobile devices.

In the future work, we intend to deploy an effective open source environment to explore the various potentials of Openstack with Federated Identity Management (FIB) in order to implement any of the key formats with the aim of ensuring the security and privacy of big data in mobile devices.

References

[1]. Musolesi, M. (2014). Big mobile data mining: good or evil?.*IEEE Internet Computing*, *18*(1), 78-81.

[2]. Manovich, L. (2011). Trending: The promises and the challenges of big social data.*Debates in the digital humanities*, *2*, 460-475.

[3]. Kitchin, R. (2014). The real-time city?Big data and smart urbanism.*GeoJournal*, *79*(1), 1-14.

[4]. Michael, K., & Miller, K. W. (2013). Big data: New opportunities and new challenges [guest editors' introduction]. *Computer*, *46*(6), 22-24.

[5]. Gantz, J., &Reinsel, D. (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. *IDC iView: IDC Analyze the future*, *2007*, 1-16.

[6]. Van Der Sype, Y. S., &Maalej, W. (2014, August). On lawful disclosure of personal user data: What should app developers do?. In *Requirements Engineering and Law (RELAW), 2014 IEEE 7th International Workshop on* (pp. 25-34). IEEE.

[7]. Krebs, D. (2012). Regulating the cloud: a comparative analysis of the current and proposed privacy frameworks in Canada and the European Union.

[8]. Pearson, S., &Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 693-702).IEEE.

[9]. Kalluri, V., &Haritha, D. (2014). CIPHER-Text Policy Attribute Based Access to Cloud.

[10]. Li, J., Jia, C., Li, J., & Liu, Z. (2012, September). A novel framework for outsourcing and sharing searchable encrypted data on hybrid cloud. In *Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on* (pp. 1-7). IEEE

[11]. Yan, L., Rong, C., & Zhao, G. (2009, December). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In *IEEE International Conference on Cloud Computing* (pp. 167-177).Springer Berlin Heidelberg.

[12]. Chadwick, D. W. (2009). Federated identity management.In*Foundations of security analysis and design V* (pp. 96-120).Springer Berlin Heidelberg.

[13]. Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., &Germonville, D. (2014). Adding federated identity management to openstack. *Journal of Grid Computing*, *12*(1), 3-27.

[14]. Martinelli, S., Nash, H., &Topol, B. (2015). *Identity, Authentication, and Access Management in OpenStack: Implementing and Deploying Keystone*. " O'Reilly Media, Inc.".