Towards Secure Risk-Adaptable Access Control in Cloud Computing

Salasiah Abdullah[1]
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
Bangi, Selangor, Malaysia

Khairul Azmi Abu Bakar[2]
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
Bangi, Selangor, Malaysia

***Abstract*—The emergence of pervasive cloud computing has supported the transition of physical data and machine into virtualization environment. However, security threat and privacy have been identified as a challenge to support the widespread adoption of cloud among user. Moreover, user awareness on the importance of cloud computing has increase the needs to safeguard the cloud by implementing access control that works on dynamic environment. Therefore, the emergence of Risk-Adaptable Access Control (RAdAC) as a flexible medium in handling exceptional access request is a great countermeasure to deal with security and privacy challenges. However, the rising problem in safeguarding users' privacy in RAdAC model has not been discussed in depth by other researcher. This paper explores the architecture of cloud computing and defines the existing solutions influencing the adoption of cloud among user. At the same time, the obscurity factor in protecting privacy of user is found within RAdAC framework. Similarly, the two-tier authentication scheme in RAdAC has been proposed in responding to security and privacy challenges as shown through informal security analysis.**

***Keywords*—Security; privacy; cloud computing; risk-adaptable access control; authentication**

I. INTRODUCTION

Cloud computing has shown a great impact in improvising information sharing between users from a different geographical location. It has led to a greater impact of knowledge sharing as people from different geographical location have the opportunity to access the cloud and share files without limited boundaries and network restriction. Alternatively, cloud computing is known as one of the best platform [1], [2] to meet the needs of consumers as it provides the platform of unlimited storage, managing and accessing data via network of remote server hosted on the internet. Thus, cloud computing has been the major savior to serve the rising needs of user who demands for storage capabilities and security as more and more documents are being created daily.

However, cloud security and privacy have been the major challenges in cloud computing when users lost their control in data storage due to the resources migration from physical to virtual storage [3], [4]. The escalation of trust relationship [5] between user and cloud provider is crucial in managing secured storage in cloud to cater the demand of user and resources that keeps growing.

This situation has been the rise factor of the introduction of access control which is a promised mechanism to ensure the enforcement of security policies in cloud. In the early stages of computing, security experts are eager in designing new security mechanism to handle massive changes in controlling access via cloud computing. Researches [6], [7] on the evolution of access control model such as Identification Based Access Control (IBAC) and Role Based Access Control (RBAC) showed the dependencies on predefined user identity and roles as it is working great in a non-distributed environment.

Besides that, IBAC has a problem with synchronization of remote user authentication and massive increase in administration overhead [8]. Later, RBAC was introduced which is based on role identification to gain access into the system. However, researchers found discrepancies in determining the privilege of user beyond administrative domains using RBAC [9]. Besides that, both IBAC and RBAC are known as conventional access control that only support static, rigid and limited support of access policies [6]. Thus, the concept of Attribute Based Encryption (ABE) has been intoduced to cater the difficulties in maintaining Access Control List (ACL) in a dynamic cloud environment [10]. In addition, [11] applied the concept of Ciphertext-Policy ABE (CP-ABE) to secure the resources and prevent unauthorized access but the implementation is limited to the data center. At the same time, we can see the transition of access control model development that relies on the high security needs and dynamic environment.

Furthermore, the emergence of access control authentication from a conventional secure password establishment to an attribute-based access control has led to the development of an efficient RAdAC to secure data in cloud. The advantages of RAdAC are the ability to cater the dynamic environment in handling exceptional access request and the flexibility in accessing resources [12]. This can resolve the issue using conventional password authentication scheme which depends on static access control policies and vulnerable to the password relevancy. Moreover, password authentication could not support rapid changing environment that involve massive user and resources in bulk.

Although both IBAC and ABAC are still widely used, RAdAC seems to be the latest evolution of access control model as not much research has been done yet. RAdAC applies the concept of analyzing each request dynamically as these request may be granted if the metric of risk is complied. However, there is a need to expand in line with the evolution

of access control model. Most researchers who are involved in the development of RAdAC model only focus on the access authentication and resource encryption but neglect the need to preserve users' privacy.

Subsequently, the challenges in cloud security and the privacy-concern issue in RAdAC development has led us to propose a reliable and secure authentication scheme in two-tier architecture. Mutual authentication takes place as only authorized user get the privilege to access the resources in cloud. Besides that, user authenticity is verified using two-factor authentication which is user ID with password and signed token.

The structure of this paper consists of Section II which highlights on the related work in preparing secured cloud and discusses on the preliminaries of cloud computing and RAdAC. At the same time,the authentication scheme with two-tier security architecture has been proposed by expanding the capability of RAdAC model. It follows by informal security analysis presented in Section III shows that the proposed scheme offers privacy preserving access control through anonymous data transaction and mutual authentication. Furthermore, secured fine-grained access control is shown by the capability of the scheme in handling user revocation and password guessing attack. This is followed by conclusion in Section IV.

II. Material and Method

In this section, we discuss on the related work in handling cloud issues and security risk. It is follows by the overview of cloud computing, its security issues and proposed solution. In addition, we also discuss on RAdAC model and analyse existing framework.

A. Related Work

Various researchers have conducted researches focusing on security issues and challenges in controlling cloud technology. There are several organizations that play their role to initiate programs such as FT7, SWIFT and POSITIF in order to study and improve the dimensions of future cloud architecture [13].

Discussion in [14] revealed that the security issues could pose a threat to cloud computing and proposed security measures to handle the problem. However, the study focuses only on the current security issues and measures without considering on long-term cloud perspectives. Later, an expectations of future cloud research has successfully proposed in [15] by analyzing the strengths and weaknesses of security resolution to maintain a safe cloud environment. In addition, a study conducted in [16] towards security issues in services model of cloud computing is valuable but the security solution is applicable only on Cloud Service Provider (CSP).

Furthermore, reliability is believed to be one of the important aspect in decision support system to convince users that the resources obtained from the cloud are safe and accurate [17]. Nevertheless, awareness on the paramount secured factor in the cloud service environment has motivated significant researches towards reliable authentication framework in cloud computing [18].

In the nutshell, understanding how cloud works as well as identifying issues and security risks in cloud technology would be an important aspect to improve the possibility of users in adopting the technology. Moreover, determining the level of cloud capabilities and challenges may lead to the effective development of access control.

B. Cloud Computing

Cloud computing is the internet-based technology that includes a storage service and communication, efficient resource management and incurs minimal cost. In addition, cloud computing imposed on virtualization technology in providing computing resources based on user's requirement [19]. Based on standard definition by National Institute of Standards and Technology (NIST), cloud computing is a model that allows network access to resources on configured computing (network, servers, applications, storage hub and services) with minimal administration or interaction [20].

Cloud computing architecture as Fig. 1 consists of four different layers which are standard definition, key features, service and deployment model. The standard definition of cloud acts as the first layer that shape the key features of cloud computing. Next, the second layer consists of five key characteristics of the cloud that drives consumer engagement in service model and deployment model.

On demand self-service is the ability of users to handle computing functions without service provider interaction. Pervasive network is a wide accessibility network from different user platform. Next, the resource pooling such as storage and network bandwidth is locally managed by the service provider in accordance to request from different users. Rapid elasticity is the ability of resource management and user to be scalable at any time. Lastly, measured service is the cloud's ability to automatically control and use resources in an optimal mode with the metering capability (pay-per-use basis).

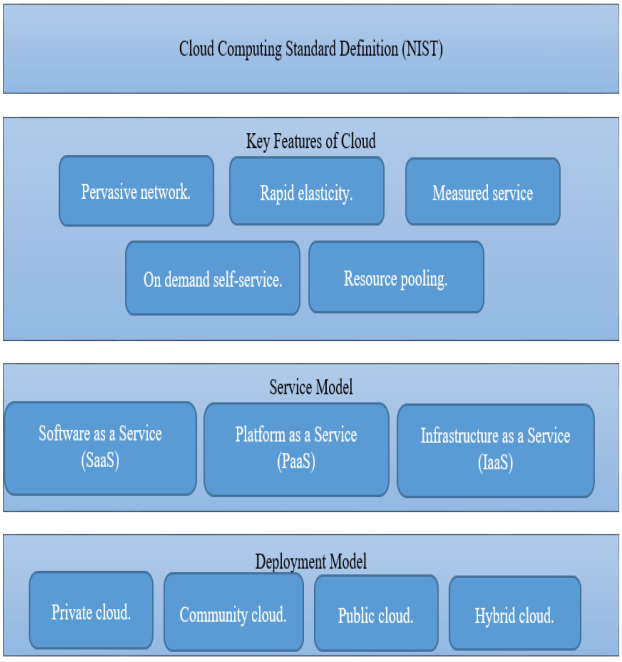

Fig. 1. Adaptation of Cloud Computing Architecture [14],[16],[20].

The third layer includes three service models in cloud computing which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [21]-[22]. Service provider provides application software based on user demands in SaaS which has been the most common model in the organisation [23]. On the other hand, PaaS allows service provider to totally support the computing environment while in IaaS, service provider offers virtual infrastructure components to users.

In the deployment model, private cloud is an environment that is going through in-house development with specific resources to certain organizations while the public cloud is developed for general use. In addition, the community cloud is targeted to specific customer groups that share the same interest while hybrid cloud is a combination of private, public and community clouds. All of the mentioned type of clouds act as the fourth layer of cloud computing architecture [24].

Intelligibility of user on cloud computing architecture and its importance, as well as the use of cloud has increased the potential of the cloud to grow in the information technology industry. Failure to facilitate the cloud computing with high security control will lead to malicious attack as it may increase the possibility of information leakage. Healthcare industry may benefits most from the utilization of cloud services to cater the needs in protecting of sensitive information [25].

TABLE I. SECURITY ISSUE AND EXISTING SOLUTION IN CLOUD COMPUTING

Author	Security Issues	Existing Solution
Subashini and Kavitha [14]	• Security, integrity, confidentiality and data access. • Vulnerability in virtualization. • Availability, authentication and identity management.	• Intensify the Service Level Agreement (SLA). • Develop security framework. • Apply encryption and access control.
Zissis and Lekkas [17]	• Confidentiality and privacy. • Integrity. • Availability.	• Effective security management. • Develop security framework. • Apply cryptography encryption. • Implement access control.
Shahzad [27]	• Denial of Service (DoS). • Cloud storage security. • Integrity,confidentiality and data availability.	• Secured access control. • Effective identity management. • Encryption during authentication.
Y. Liu et al. [15]	• Data and security control. • Storage virtualization. • Authentication.	• Apply encryption. • Strengthen access control. • Effective security management.
Suzic et al. [13]	• Identity management. • Authentication and trust.	• Implement access control. • Apply cryptography for encryption.
Hepsiba and J.G.R. Sathiasee-lan [16]	• Malicious attack. • Denial of Service (DoS). • Security, integrity, confidentiality and data availability.	• Strong encryption and access control. • Management of information security. • Authentication protocol.

In addition, the level of privacy in the cloud environment could help to preserve the confidentiality of the data while protecting user identity. Whereas, level of reliability relies on effective cloud management by providing storage and communications to cater user needs. Thus, the level of privacy and reliability are the dependent factor to support the development of cloud technology in an organization.

1) Security issues and existing solutions: Previous study conducted on the issues and challenges of cloud security is a catalyst and serve as a benchmark in developing a comprehensive cloud environment. Organization is advised to analyze the security risk of cloud computing before jumping into an agreement to fully utilize the technology [21]. Table 1 summarizes a conducted past study in identifying security issues, challenges and proposed solutions in the cloud environment.

Existing solution as the Table 1 complies with the Information Security Principle which has been outlined as confidentiality, integrity and availability [21]. User needs to ensure security requirements in cloud such as reliability, authentication and identity management has been applied to protect the robustness of virtualization environment. However, the biggest challenge to rule out the principle is ensuring the capability of cloud in processing its resources with zero knowledge on the resources nor the identity of user [26].

C. Risk-Adaptable Access Control (RAdAC)

The increasing capacity of resources in access control system embarks the dynamic features in the architecture of RAdAC model. There are four components in existing RAdAC architecture which are Policy Enforcement Point (PEP), Policy Decision Point (PDP), Subject and Risk Engine as Fig. 2. The decision process starts when subject issues access request for specific resources. PEP handles access request from subject and sends it to PDP for access decision. If the request complies with the risk policy, Risk Engine performs risk quantification and analysis based on agreed metrics and response back to PDP. PEP will enforce obligation immediately after receiving decision from PDP. However, the existing architecture is vulnerable to security attacks by the curious component.

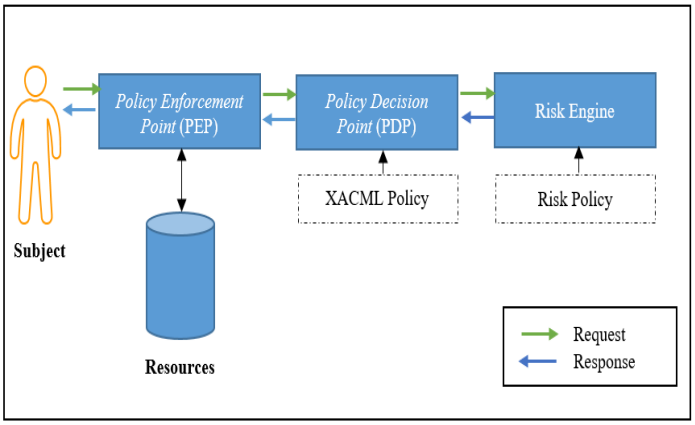

Fig. 2. Existing Architecture of Risk based Access Control [12].

The capability of RAdAC in managing ad-hoc request has become more prominent in access control environment compared to conventional predefined policies. RAdAC also works well in rapid-change environment to cater larger range of increase in users and resources. Nevertheless, failure in managing user identity and access structure in RAdAC has led to poor cloud management [12]. Thus, the implementation of RAdAC model is advantageous if the management of user identity and hidden access structure can be carried out effectively.

There are several works by other researchers in RAdAC development. Risk based access control which has been developed by [28] proposes the application of Policy Decision Point (PDP) with classifiers to quantify risk. Furthermore, RAdAC model has been implemented in healthcare information system to protect sensitive data and support dynamic health environment [29]. However, the implementation of RAdAC model in cloud computing is still in its infancy.

Thus, the fidelity of Risk Adaptive Authorization Mechanism (RAdAM) implementation in cloud has been proposed by [30] to determine access decision and introduce adaptable algorithm in cloud computing. However, the capability of RadAM in managing cloud federation has not been studied extensively.

Ontology in risk based access control is the extended work of [12] to define the independent risk policies of RAdAC model in specific hierarchical process. Subsequently, the ontology approach in RAdAC allows risk quantification without the need of cloud federation. At the same time, the indicative structure of the proposed model has been demonstrated by the privilege of Cloud Service Provider and its inference capability to support dynamism in access decision.

Subsequently, failure in managing identity of user in access control model may disrupt the effective implementation [12]. Thus, this research has been the benchmark for this paper in designing the architecture of proposed authentication scheme. Afterwards, most of previous works bypass the need to protect privacy of user in developing risk based access control model [28], [31], [32].

The analysis of existing RAdAC Model involved determining the related framework and refining the elements into the corresponding characteristics. Table II is a summary of publications related to RAdAC framework and published in journals and conferences. However, risk assessment is not within the scope of this paper as it highlights only on the privacy preserving in RAdAC.

As a result, three of the existing model shows the relationship involving the adaptation of risk metrics into RBAC model [31], [33], [34]. This concept supports the statement regarding access control evolution to adapt with flexible and dynamic features in cloud computing. Therefore, RAdAC is a continuous model that has been built using existing access control model as a basis. However, the development of RAdAC involves extensive improvement on additional function with element of risk and current context to cater the dynamicity of cloud environment.

TABLE II. COMPARISON TABLE OF RADAC FRAMEWORK

Elements	**Framework**				
	Ricardo dos Santos et al. [12]	***Khambhammettu et al.*** [35]	***Baracaldo and Joshi*** [33]	***Bijon et al.*** [34]	***Choi et al.*** [31]
Domain	Cloud computing	Not available	Not available	Not available	Real-time system.
Reliability	Make inferences by modifying weightage values based on risk metric.	Protect object in term of sensitivity and evaluate the user reliability on specified value.	Set threshold to prevent unauthorized access and abusive of data.	Deactivate user when system detects anomalies in user and run-time.	Identify specific method of medical analysis based on classified context.
Approach	RAdAC + Ontology	Threat assessment.	RBAC + risk and reliability assessment.	RBAC + risk assessment.	RBAC + risk assessment.
Advantage	Flexibility and dynamicity.	Protect from outsider attack.	Protect from insider attack.	Provide dynamic access.	Support medical information system.
Protection of users' privacy	Not available	Not available	Trust-based	Not available	Not available.
Access Decision	Depends on Aggregated Risk Score.	Depends on threat assessment score.	Depends on reliability threshold.	Depends on risk threshold.	Depends on risk level of patient.

Based on Table II, [34] is focusing only on the implementation of dynamic user authentication access while other studies [24]-[25], [27]-[28] discussed on the protection aspect of objects and resources with encryption methods or proven algorithm. At the same time, four from the five framework in the table did not mention about privacy protection of user. Hence, the need in safeguarding users' privacy in the RAdAC model has not been discussed in depth. Newer enhancement on the security and privacy landscape is compulsory to accelerate widespread adoption of cloud utilization among user.

D. Proposed Authentication Scheme

Authentication verifies user's identity and enables authorization to dictate different access of user. It is the way security system challenges user to prove identity credential based on something you know (e.g. password), what you have (e.g. digital certificate) and what you are (e.g. fingerprint) [36]. The architecture of risk based access control that has been defined in this paper is the extension from existing one-tier architecture of RAdAC Model that has been discussed by [12]. However, this scheme is the extended version of previous work which applied two-tier architecture as it offers protection of users' privacy by guaranteeing anonymity of information transfer using secure asymmetric cryptography method.

This method uses encrypting mechanisms by ensuring encapsulation of message to remain anonymous. Additionally, this method uses dual-keys which are public key for message encryption and private key for decryption of message. kc is assumed to represent the function of access decision value to support data transfer process as follows

$$kc : \mathbb{U}(U) \times S \times \mathbb{U}(P) \rightarrow \{0,1\} \quad (1)$$

kc determines whether user with a set of identity attributes $u = \{u_1, \ldots, u_n\} \subset U$ get the permission to access resources $s \in S$ based on access policy $p = \{p_1, \ldots, p_n\} \subset P$. When subject/user U sends an access request for resources S in cloud, they need to register at Identity Provider (IdP) to comply with authentication process.

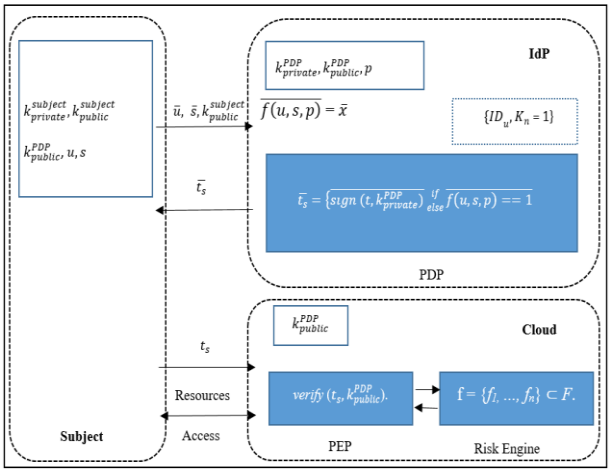

Fig. 3. Proposed Authentication Scheme using Asymmetric Cryptography.

Based on Fig. 3, IdP with dual key $(k^{PDP}_{public}, k^{PDP}_{private})$ acts as PDP which received access request from subject and generate user ID, ID_u and temporary password PW_u randomly by $RPW_u = h\ (PW_u \,||\, R_u)$ in the sign-up phase. Next, IdP will store $\{ID_u, K_n = 1\}$ in ID management table as $K_n = 1$ refers to active user who signs up once. K_n represented the number of registration that has been done by user. Login phase continues when user U send login request message $< ID_u, RPW_u >$ to IdP.

Encryption mechanism will takes place as PDP will sign the token and send the encrypted format to be verified by user and cloud manager (act as PEP) using PDP public key (k^{PDP}_{public}). Session key k^{PDP}_{public} is to be used by user and cloud manager as it is assumed to be delivered during the access request. Furthermore, user is occupied with dual key $(k^{subject}_{private}, k^{subject}_{public})$ to support the encryption mechanism. Next, authorization process begins as risk engine that has been invoked by the PEP started to analyze the risk policies based on risk metrics initiated by the cloud service provider or resource owner. User access to cloud is granted based on the predefined threshold that has been set at the first place.

III. Results and Discussion

In this section, informal security analysis shows the capability of authentication scheme in managing secure transaction.

Proposition 1: Proposed scheme offers secure anonymous transaction and mutual authentication.

Proof: In the recent scheme, identity of user is transmitted during the access request thus revealed the sensitive information of user to the cloud. In our proposed scheme, cloud cannot misuse user information as it only holds encrypted data of user. Anonymous transaction takes place as user send his public key $k^{subject}_{public}$ with identity attributes and requested resources in an encrypted format, $\bar{u}$ dan $\bar{s}$. PDP will user the session key $k^{subject}_{public}$ to encrypt p to $\bar{p}$ to compute *kc*. Next, $\overline{f(u,s,p)}$ generated encapsulated value $\bar{x}$ to ensure fine-grained access control. At the same time, this scheme offers privacy preserving of user identity, requested resources and the basic policy structure in the IdP. PDP will issue encrypted identity token $\bar{t_s}$, by signing the token t using $k^{PDP}_{private}$ as follows:

$$\bar{t_s} = \overline{\{sign\ (t, k^{PDP}_{private})\ \underset{else}{if}\ f(u,s,p) == 1} \quad (2)$$

Next, user will decide whether $\bar{t_s}$ fulfil his access request before decrypted the $\bar{t_s}$ using $k^{subject}_{private}$. Furthermore, user will use k^{PDP}_{public} to generate t_s as the verification process will be assigned by PEP using *verify* (t_s, k^{PDP}_{public}). Authorization process takes places as access decision is based on risk metrics $f = \{f_1, \ldots, f_n\} \subset F$ and risk threshold. Risk metrics such as user or device characteristic and situational, heuristic or environmental factors might influence the access decision.

Nevertheless, mutual authentication in this scheme is proved by two factor user authentication which is user ID with temporary password $< ID_u, RPW_u >$ and identity token that has been issued by IdP. It shows that access to cloud is granted only to an authorized user with valid credential.

Proposition 2: Proposed scheme support revocation or re-registration phase.

Proof: To initiate the revocation process, user U will send revoke request message to IdP. Next, IdP will store $\{ID_u, K_n = 0\}$ in its database where $K_n = 0$ shows user has been revoked and deactivated. If user need to re-register the services again, user need to prove his last valid ID ID_u and IdP will update back its data into $\{ID_u, K_n = 1\}$.

Proposition 3: Proposed scheme is secure against password guessing attack.

Proof: Password guessing attack by malicious user or untrusted cloud is impossible as they cannot initiate the value of parameter R_u. IdP will generate the temporary password randomly $RPW_u = \text{h}(PW_u \,||\, R_u)$ during the sign-up phase.

The informal analysis has been conducted as the justification to identify correct implementation and proof of concept of the authentication scheme. Thus, the scheme is viable in managing secure transaction, handling revocation and password guessing attack.

IV. Conclusions

Access control is one of the fundamental requirements in managing security risk. However, the rising needs in preserving users' privacy has been seen as the imperative obligation to protect identity of user. Therefore, security risks and privacy challenges in cloud should be taken into serious considerations. Furthermore, it plays a fundamental role in ensuring the wide adoption of cloud computing technology.

Similarly, the implementation of access control is crucial as RAdAC model offers dynamic characteristic in addressing vulnerabilities as it is able to deter the capabilities of conventional access control. In this paper, we have identified the general cloud architecture that serve as a benchmark in educating user on the paramount secured factor in the cloud computing service environment. Furthermore, analyzing security issues in cloud computing has diverse existing solution in defining a secure and reliable strategy against threats and vulnerabilities.

Subsequently, RAdAC model has been discussed by summarizing the existing framework to formulate a strategy in a systemic point of view. Thus, this discussion has envisioned the future roadmap in cloud by the introduction of two-tier security architecture in the authentication scheme. Informal security analysis demonstrated that the proposed scheme serves as a promising solution to cater security and privacy issues in cloud.

In the future, we plan to develop a framework of risk based access control with hidden access policy and apply the concept in real cloud platform.

References

[1] Meva and C. K. Kumbharana, "Issues and challenges of security in cloud computing environment.," Int. J. Adv. Netw. Appl., pp. 108–111, 2015.

[2] S. Abolfazli, Z. Sanaei, A. Tabassi, S. Rosen, A. Gani, and S. U. Khan, "Cloud adoption in Malaysia: Trends, opportunities, and challenges," IEEE Cloud Comput., vol. 2, no. 1, pp. 60–68, 2015.

[3] L. Wei et al., "Security and privacy for storage and computation in cloud computing," Inf. Sci. (Ny)., vol. 258, pp. 371–386, 2014.

[4] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Secur. Priv., vol. 8, no. 6, pp. 24–31, 2010.

[5] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, "Access control as a service for the cloud," J. Internet Serv. Appl., vol. 6, no. 1, 2015.

[6] A. H. Karp, H. Haury, and M. H. Davis, "From ABAC to ZBAC : The evolution of access control models," ISSA J., no. April, pp. 22–30, 2010.

[7] M. Mulimani and R. Rachh, "Analysis of access control methods in cloud computing," no. July, 2016.

[8] V. Boyko, P. Mackenzie, and S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman," Eurocrypt, vol. 2, pp. 156–171, 2000.

[9] Y. Zhu, D. Huang, C.-J. Hu, and X. Wang, "From RBAC to ABAC: constructing flexible data access control for cloud storage services," IEEE Trans. Serv. Comput., vol. 8, no. 4, pp. 601–616, 2015.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. Comput. Commun. Secur. - CCS '06, p. 89, 2006.

[11] A. Sudarsono, M. U. Harun, and A. Rasyid, "Secure data sensor in environmental monitoring system using attribute-based encryption with revocation," vol. 7, no. 2, pp. 609–624, 2017.

[12] D. Ricardo dos Santos, R. Marinho, G. Roecker Schmitt, C. Merkle Westphall, and C. Becker Westphall, "A framework and risk assessment approaches for risk-based access control in the cloud," 2016.

[13] B. Suzic, A. Reiter, F. Reimair, D. Venturi, and B. Kubo, "Secure data sharing and processing in heterogeneous clouds," Procedia Comput. Sci., vol. 68, no. 316, pp. 116–126, 2015.

[14] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[15] Y. Liu, Y. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: Solutions and future directions," J. Comput. Sci. Eng., vol. 9, no. 3, pp. 119–133, 2015.

[16] C. L. Hepsiba and J.G.R.Sathiaseelan, "Security issues in service models of cloud computing," Int. J. Comput. Sci. Mob. Comput., vol. 5, no. 3, pp. 610–615, 2016.

[17] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[18] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and J. L. Hoon, "A strong user authentication framework for cloud computing," in Proceedings - 2011 IEEE Asia-Pacific Services Computing Conference, APSCC 2011, 2011, pp. 110–115.

[19] C. G. Song, N. Y. Hwang, H. C. Yu, and J. B. Lim, "A dynamic resource manager with effective resource isolation based on workload types in virtualized cloud computing environments," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 7, no. 5, pp. 1771–1776, 2017.

[20] P. Mell and T. Grance, "The NIST definition of cloud computing recommendations of the National Institute of Standards and Technology," Nist Spec. Publ., vol. 145, p. 7, 2011.

[21] B. Hari Krishna, S. Kiran, G. Murali, and R. Pradeep Kumar Reddy, "Security issues in service model of cloud computing environment," in Procedia Computer Science, 2016, vol. 87, pp. 246–251.

[22] Nurul Elliza Jasmin and Mohammad Khatim Hasan, "Framework for the implementation of E-Government system based on cloud computing for

Malaysian public sector," Ejournal.Ukm.My, vol. 7, no. 1, pp. 1–18, 2018.

[23] N. Jafri and M. M. Yusof, "Managing data security risk in model Software As a Service (Saas). Pengurusan risiko keselamatan data dalam model perisian sebagai perkhidmatan (Software As a Service)(Saas)," vol. 7, no. 1, pp. 99–117, 2018.

[24] M. H. Kayali, N. Safie, and M. Mukhtar, "Literature review of cloud based E-learning adoption by students: State of the Art and Direction for Future Work," IOP Conf. Ser. Mater. Sci. Eng., vol. 160, no. 1, 2016.

[25] A. Meri, M. K. Hasan, and N. Safie, "Success factors affecting the healthcare professionals to utilize cloud computing services," Asia-Pacific J. Inf. Technol. Multimed., vol. 6, no. 2, pp. 31–42, 2017.

[26] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," J. Syst. Softw., vol. 86, no. 9, pp. 2263–2268, 2013.

[27] F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," 5th Int. Conf. Emerg. Ubiquitous Syst. Pervasive Networks (EUSPN-2014)/ 4th Int. Conf. Curr. Futur. Trends Inf. Commun. Technol. Healthc. (ICTH 2014)/ Affil. Work., vol. 37, no. 0, pp. 357–362, 2014.

[28] I. Molloy, L. Dickens, C. Morisset, P.-C. Cheng, J. Lobo, and A. Russo, "Risk-based security decisions under uncertainty," Proc. Second ACM Conf. Data Appl. Secur. Priv., no. February, pp. 157–168, 2012.

[29] K. Lee, S. G. Choi, D. H. Lee, J. H. Park, and M. Yung, "Self-Updatable encryption: Time constrained access control with hidden attributes and better efficiency," Adv. Cryptol. - ASIACRYPT 2013, vol. 8269, pp. 235–254, 2013.

[30] D. Fall, T. Okuda, Y. Kadobayashi, and S. Yamaguchi, "Risk Adaptive Authorization Mechanism (RAdAM) for Cloud Computing," J. Inf. Process., vol. 24, no. 2, pp. 371–380, 2016.

[31] D. Choi, D. Kim, and S. Park, "A Framework for context sensitive risk-based access control in medical information systems," Comput. Math. Methods Med., vol. 2015, 2015.

[32] D. Díaz-López, G. Dólera-Tormo, F. Gómez-Mármol, and G. Martínez-Pérez, "Dynamic counter-measures for risk-based access control systems: An evolutive approach," Futur. Gener. Comput. Syst., vol. 55, pp. 321–335, 2016.

[33] N. Baracaldo and J. Joshi, "An adaptive risk management and access control framework to mitigate insider threats," Comput. Secur., vol. 39, no. Part B, pp. 237–254, 2013.

[34] K. Z. Bijon, R. Krishnan, and R. Sandhu, "A framework for risk-aware role based access control," in 2013 IEEE Conference on Communications and Network Security (CNS), 2013, pp. 462–469.

[35] H. Khambhammettu, S. Boulares, K. Adi, and L. Logrippo, "A framework for risk assessment in access control systems," Comput. Secur., vol. 39, pp. 86–103, 2013.

[36] K. A. Abu Bakar and G. R. Haron, "Context-Aware analysis for adaptive unified authentication platform," in Proceedings of the 5th International Conference on Computing & Informatics, 2015, pp. 417–422.