# End-User Authentication Control in Cloud-based ERP Systems

Nwanneka Eya
*Department of Computer & Information Sciences*
*University of Strathclyde*
Glasgow, UK
nwanneka.eya@strath.ac.uk

George R S Weir
*Department of Computer & Information Sciences*
*University of Strathclyde*
Glasgow, UK
george.weir@strath.ac.uk

***Abstract*—Cloud Security is the use of latest technology and security techniques to safeguard data, applications and infrastructure associated with Cloud Computing. The set of policies, procedures, technologies, and controls that function jointly to safeguard cloud-based systems, infrastructures and data are known as the Cloud Computing Security Model. This paper reviews several Cloud Computing Security Models with a close look at the model that addresses data security challenges in cloud-based Enterprise Resource Planning (ERP) systems and proposes an End-User Authentication Control Model for Cloud-based ERP systems. This is a cloud computing security model that uses Enterprise Access Directory, Enterprise Data Fragmentation in cloud and End-user Access Queries, to ensure that End users share a greater security responsibility. The proposed model, when compared with other exiting models, will encourage more end-user participation in enterprise data security in the cloud. The proposed model also mitigates the impact that a malicious insider might have on the enterprise cloud data set, since no single user can gain access to the whole cloud-based enterprise database at the same time. The proposed model considers end-user role and responsibility within the enterprise to determine the level of access and to data in the cloud-based ERP system.**

***Keywords—Data Security, Enterprise Resource Planning, Cloud Computing, End-User Model.***

## I. Introduction

Cloud Computing has emerged as technology that provides efficient on-demand services to end-users with a high scalability, over the Internet. Cloud computing is often represented as outsourcing of computing resources over the Internet [1],[2]. Computing resources here can be any feature in traditional computing, like servers, networks, applications, data, etc. Computing cost is greatly reduced by enterprises adopting cloud computing [3], although data security is still a major concern [3-5] and the risk of an unreliable Cloud Service Provider (CSP) is identified as a security threat to cloud computing [6]. Conventionally, data integrity checks and end-user authorization are managed by the enterprise who are the data owners [2]. This may prevent issues that could arise from manual engagement within the CSP centre. Cloud security may seem to be a nebulous quality that covers a wide range of aspects but some researchers note that building a cloud computing data security system is the foundation for building a secured cloud system [7]. Clearly, it is important for enterprises that utilize cloud systems for commercial purposes to safeguard their sensitive data, for instance, trade secrets [7]. Although many data security models for cloud computing have been proposed, these models do not extensively meet the needs of the end-users of the cloud system [2].

There are many security challenges in cloud computing and these can be categorized into four areas: infrastructure challenges, data challenges, end-user/CSP challenges and policy challenges. In the present research, we consider cloud security models that seek to address any of the cloud challenges categories mention above.

In response to perceived shortcomings in the considered security models, we propose a model called the 'end-user authentication control model' for a public cloud-based ERP system. This model will address the security gap created by lack of end-user involvement in their enterprise data security in the cloud. In the following, Section II introduces cloud security models; Section III uses a number of parameters to compare the cloud security models and notes their strengths and weaknesses; Section IV describes attributes of the proposed end-user authentication control model. Thereafter, we draw conclusions and offer recommendations.

## II. Cloud Computing Security Models

To appreciate the need and scope for refining the model for Cloud-based security, we outline the characteristics of five popular approaches, the Multiple Tenancy Model, the Cloud Risk Accumulation Model, the Jericho Forum Cloud Cube Model, the Default Gateway Platform Model and the Multi Cloud Database Model.

### *A. Multiple Tenancy Model (MTM).*

The Multiple Tenancy Model, as the name implies, is the cloud feature that allows multiple customers to access the same application or cloud resources on the same physical server, without compromising security and privacy [11]. In multiple tenancy architecture, virtualization is used to differentiate and process each customer's demand. This is possible because virtualization is able to isolate and share the computing resources, such as processor, memory etc. [12]. Furthermore, the MTM places specific demands on the system architecture, for instance, the computing architecture must be highly scalable, flexible and able to support different customers' demands without their data intertwining [13]. The MTM approach is able to prevent customer data interference (achieving data isolation) and can easily scale up or down as the customer requires (affording architecture extension). The MTM can allow each customer to customise their service requirements (configuration self-definition) and finally, the ability to guarantee that each customer task will be attended to by customizing performance using different workloads [14].

### *B. Cloud Risk Accumulation Model (CRAM)*

The Cloud Risk Accumulation Model of CSA is a cloud security model that defines the boundaries of each service model and how each service model relates to each other with respect to cloud security [15]. IaaS is the basic level of all the other service models, where each of the service level inherits the capabilities and security concerns of the service level under it. For instance, IaaS is the basic level service model, and PaaS will inherit the security capabilities and concerns of the IaaS while adding its own particular security capabilities and concerns. Furthermore, the SaaS will add to the security capabilities of the IaaS and PaaS to provide its own specific security capabilities and concerns. This risk accumulations model suggests that it is important to understand the layer dependency of the different cloud service models in other to be able to analyse the security risks of cloud computing [16]. For the cloud risk accumulation model, the end-user's security responsibilities increase or decreases depending on the service level. For instance; at IaaS level, the end-user is responsible for satisfying the monitoring, compliance and the security demands of the cloud system, while in the SaaS, the responsibilities shift to the cloud service provider who is to ensure the monitoring and security of the cloud system [15].

### *C. Jericho Forum Cloud Cube Model (JCCM).*

The Jericho Forum's cloud cube model is a model that categorized the cloud network, using four distinctive features: internal/external, proprietary/open, de-perimeterized/perimeterized, and insourced/outsourced [17]. The aim of a cloud cube model is to provide a secured cloud system through helping to select cloud formation for secured collaboration. Data classification is regarded as an important step, which needs to be performed by any enterprise intending to move their data to a cloud [17, 18]. This is because data classification ensures the deciding authorities can determine which data and processes to move to cloud. This helps to determine which cloud service level the end-user wants to operate in; it can be IaaS, PaaS, or SaaS. The four attributes used to categorise cloud formation in the cloud cube model are considered below.

***Internal/external***: This is an attribute of cloud cube model, which refers to the storage location of the data. A set of data is "internal" if it is located within the data owner's data centre, for instance, when data is stored in the private cloud, it is considered "internal". A set of data is "external" if it is stored in the data centre outside the boundaries of the data owner, for instance any data stored in the public cloud [18]. ***Proprietary/open***: This cloud cube model attribute denotes the proprietorship structure of the cloud technology and its interfaces. When the cloud service provider owns the cloud technology facilities, it is termed the 'proprietary dimension' which means that they have responsibility for guarding the data and cloud facilities under their ownership, as such, it will not allow end-users to easily move their applications to a different cloud service provider [18]. However, in an 'open dimension', end-users are able to transfer their application, share their data or collaborate with other cloud service providers using the open technology, open dimension id possible in a public cloud, which have many cloud service providers. ***Perimeterized/de-perimeterized***: This is simply a type of cloud formation that details whether an end-user is operating within traditional IT security limits or outside it. Being perimeterized means that the end-user application is within the traditional organisational IT boundary. Network firewalls can achieve this. Furthermore, de-perimeterized means that end-user applications operate outside the traditional IT security limit; this implies that the end-user data are exposed. This data exposure is managed using the data encapsulation via metadata and Jericho Forum's mechanism, which prevents unauthorized usage of end-user data [17]. ***Insourced/outsourced***: This feature of the Jericho Forum's cloud cube model refers to the entity managing the cloud in an enterprise. Insourced means that the cloud is managed by the enterprise employee for whom the enterprise has control over their working activities, while outsourced means that the cloud is managed by a third-party. This feature does not involve technical or structural choice but is more a business decision, which will have an impact on the data security in cloud [15].

### *D. Default Gateway Platform Model (DGPM).*

The Default Gateway Platform is a data-centred cloud security model. This model identifies three types of data that are found in the cloud system network, namely transmission data, storage data and processing data [19]. Transmission data is any data in transit, processing data is any data being processed and storage data is any data that is at rest. On one view [20], most existing cloud data security models do not cater for data at rest and thereby create a security gap that the Default Gateway Platform addresses. The default gateway platform uses a three-level defence system formation; in which each defence level contributes its own responsibilities to ensure data security of cloud system. One Time Password (OTP) is use in the initial stage to ensure a good authentication process. The subsequent stage uses a data encryption process to encrypt data quickly and automatically. End-users can also encrypt their delicate data manually by using any of the modern encryption processes, for example by using True-Crypt software to ensure that delicate data are encrypted. Furthermore, the integrity of the encrypted data is ensured by using hashing process. Hashing is a way of ensuring data integrity and security especially for transmission data because it ensures that only the intended recipient accesses the transmitted data. The final stage of the defence system structure is the data recovery phase; this is the stage where the user-data are quickly recovered on demand.

### *E. Multi Cloud Database Model (MCDM).*

Multi Cloud Database Model is a type of cloud security model that is concerned with the cloud system whose database is located with different Cloud Service Providers (CSP) [21]; for instance, when an enterprise is subscribed to Database as a Service (DaaS) of different CSP. This is not the same with a typical scenario of a single cloud storage database by a single CSP; like the cloud services provided by the Amazon cloud. Since this model is concerned with the multi cloud database, the security it provides is not able to cover for the single cloud database [22]. It uses the process of applying "multi shares" on the different cloud provider server to ensure the privacy and security of the cloud database. M. A. AlZain et al (2012) [22] believed that multi cloud database model (MCDM) have many advantages of data security over the single cloud, it stated that the security risk posed by a malevolent employee is highly minimized in the MCDM. Encryption techniques although a good security process was believed to pose some negative impact on the cloud network, which can be minimized using the MCDM.

Data replication and multi sharing technique are the two approach the MCDM uses to achieve data privacy and security of the different databases with the different CSP.

The running between the cloud user and the CSP is managed using the data management system (DMS). From the end-user, the cloud network receives queries or entries to the server, which is stored in the cloud server that is supposed to be a trusted cloud server; the challenge will arise if the cloud server is not surely secured. We further propose that each database of each CSP to be further fragmented after data classification; this is to ensure further security of cloud data by ensuring no single end-user has access to the entire database of an enterprise at once.

## III. COMPARISON OF CLOUD COMPUTING SECURITY MODELS

To review the above identified cloud security models (CSM); we considered certain parameters to be used as yardstick for the compares. We identify the different features and objectives of the cloud security model that helps them to stand out and compared them using the following parameters, the technology used, security responsibility, security effectiveness, security porosity, targeted cloud feature and practicality [17].

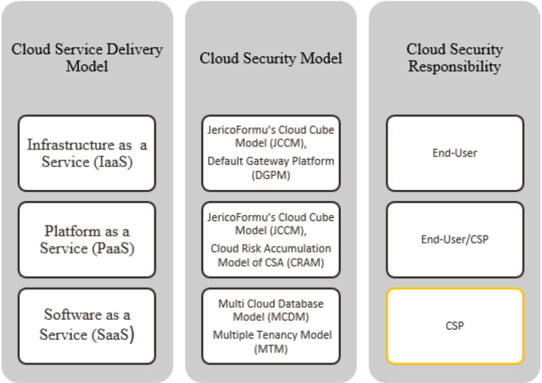
### A. The Technology Used Parameter

The "technology used" is describing the CSM features along the underlining technology it uses to achieve its cloud security promises. Security technology can range from virtualization, layer dependency, algorithm sharing mechanism, to something as simple as encryption [16].

### B. The Security Responsibility Parameter

The "security responsibility" is the yardstick we adopted to describe the security sharing responsibility of the different CSM. It simply states between the end-user and CSP who holds more security responsibility in the different CSM. For some of the CSM, the end-user holds more security responsibility, for instance in a cloud delivery model like the IaaS (infrastructure as a service). However, for SaaS (software as a service), the CSP holds more of the security responsibility. For the different CSM, one would find that depending on the cloud delivery model that a particular CSM is targeting, this would also determine the security responsibility of such CSM. The Fig.1. below shows that for a SaaS delivery model, the cloud service provider (CSP) holds the sole security responsibility. The two-cloud security model that focuses on SaaS delivery model are the multi cloud database model and the multiple tenancy model. Therefore, following an extensive literature review on the need for end-user sharing a security responsibility for a SaaS delivery model, we proposed an end-user centric model that addresses this gap by grouping concepts of MCDM and MTM together and removing overlapping concepting and adding new attributes to enhance its security porosity.

Y. Chou (2010) [4] also attempted to classify the responsibilities sharing structure between the end-users and the CSP which from his diagram in Fig.2. below, it can be clearly seen that data responsibilities are not the end-user's responsibility in a SaaS cloud deployment model; but in every other deployment model, the end-user shares or holds the responsibility of data. Servers, storage, and networking are also main computing features of cloud security; therefore, at every point the CSP hold the responsibility of these features, it is safe to assume they also hold the responsibility of securing the cloud. This is only exempted from the On-Premises or Private Cloud, where the end-user has the entire responsibilities of the cloud system.



| Cloud Service Delivery Model | Cloud Security Model | Cloud Security Responsibility |
|---|---|---|
| Infrastructure as a Service (IaaS) | JericoFormu's Cloud Cube Model (JCCM),<br>Default Gateway Platform (DGPM) | End-User |
| Platform as a Service (PaaS) | JericoFormu's Cloud Cube Model (JCCM),<br>Cloud Risk Accumulation Model of CSA (CRAM) | End-User/CSP |
| Software as a Service (SaaS) | Multi Cloud Database Model (MCDM)<br>Multiple Tenancy Model (MTM) | CSP |

Fig. 1. Classification of the Different Security Responsibilities between the End-Users and the CSP in the various Cloud Security Models (CSM).

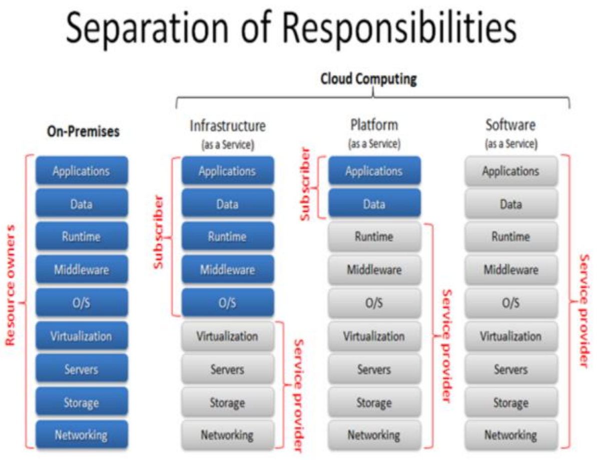


Fig. 2. Separation of responsibility between the end-user and CSP using different cloud deployment model [4]

### C. The Security Effectiveness Parameter

The "security effectiveness" is the yardstick we adopted to describe how effective CSM are at securing the cloud system. We use "averagely secured" to denote when a CSM of a cloud system is having a medium security; on the other hand, we used "highly secured" to denote when the CSM provides an effectively high security.

### D. The Security Porosity Parameter

The "security porosity" is the yardstick we used to describe the CSM, which have the more likely hood of been porous to an attacker, for instance; classifying the CSM that a malicious insider can easily bypass the security modalities of such model.

### E. The Targeted Cloud Feature Parameter

The "targeted cloud feature" is used to describe what the CSM is targeting to secure more in the cloud system, some of the CSM is targeting to secure the cloud data, weather it is data at rest or transit data, other CSM may be targeted at protecting the cloud network infrastructures, while other are targeted at protecting the end-user. The feature is used to indicate which aspect of cloud system a CSM is focused on protecting.

### *F. The Practicality Parameter*

The "Practicality" is the yardstick adopted to identify the different CSM in terms of weather they are system centred or they are user centred. All cloud security models have similar objective of trying to secure the cloud system, although they differ in the mechanism and preferred approach. This feature will help us to identify the CSM that are more user centred. The table 1 tried to itemize the CSM against these features and compare them.

## IV. STRENGTH AND WEAKNESS OF CLOUD SECURITY MODELS

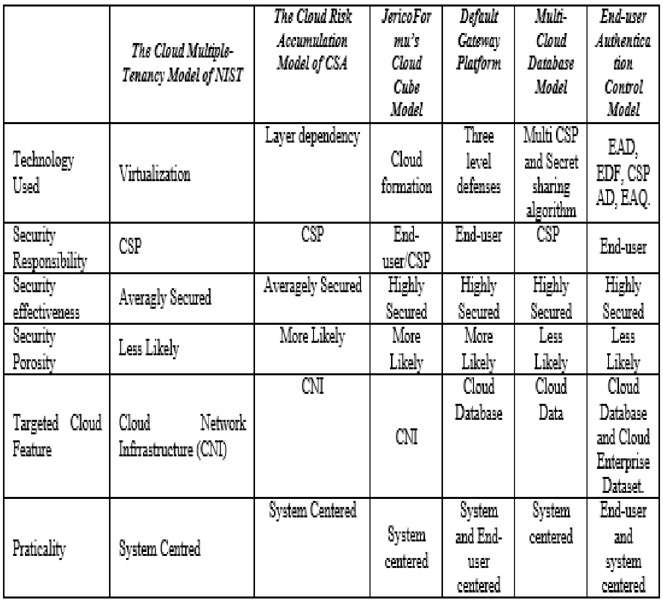
Reviewing the strengths and weakness of the different CSM in a bid to identify similarities, differences and gaps that can be researched further. The obvious similarity shared by all the CSM is, they have common objective of securing the cloud system. Although some of the CSM is targeted more at securing the user data/database; for instance, the Multi Cloud Database Model (MCDM), while others like Cloud Risk Accumulation Model of CSA is focus more on the cloud infrastructure level. Since providing cloud system security is their primary responsibility; the CSM with the "highly secured" security effectiveness and "less" security porosity would be the most preferred in achieving the main objective of the CSM. From Table 1 below, one can see that the multi-clouds database model seems to be the CSM that meets the CSM objective better; although it is believe by B. Kaur, and S. Sharma [16] to be more expensive and more time consuming than the other cloud security models. However, in the MCDM. the risk associated with failing of the cloud services is minimal and the risk of a malicious end user is also minimal. The end-user of the cloud system does not have any major security responsibility in MCDM; this CSM supports most SaaS cloud platforms.

It is important to note that cloud ERP's (Enterprise Resource Planning) applications modules is accessed over the Internet using the SaaS delivery model. Therefore, MCDM is the CSM closely associated with cloud ERP's. For this reason, since most enterprises especially the SMEs are keen on moving to Cloud ERP but are challenged by the security concerns associated with cloud; we proposed an end-user centric model that is based on the integration of insights from research literature and existing cloud security models after conducting an extensive comparison study of the CSM and the parameters for determining the importance of end-user involvement in security responsibility. A closer look at MCDM and cloud ERPs could help determine how this improvement can boost cloud security and cloud ERP adoption by an enterprise. Our main research activity attempted to validate the concepts of the proposed model.

The cloud multiple tenancy model of NIST has its strength in its ability to separate virus, intrusion and malfunctioning features from the different virtual machines and the cloud hardware. It also minimises the associated risk of a malicious application on the cloud. However, its setbacks are found in the technology difficulties like performance customization, data isolation and architecture extension. The Jericho Forum's Cloud Cube model have its strength in the ability end-user to choose cloud formations for a joint effort in securing the cloud system. However, with this CSM, there is a risk of data leaks especially if the backup with the CSP was not erased at the end of the service agreement. To manage this end-user are advised to ensure that data are properly transferred, managed, and deleted from all CSP backups at the end of the service agreement.

The Cloud Risk Accumulation model of CSA, because of the layer dependency of the model, the security of the cloud system can easily be analysed. The noticeable challenge here is that the CSP security responsibility stays in the IaaS that is the lower service level; on the assumption that the more the end-user have security responsibility, the greater the risk of security breach. Default Gateway Platform has its advantage as a more end-user oriented CSM, given the end-user the leverage to encrypt sensitive data using TrueCrypt before processing. The challenges as well is that the more end-user security responsibility the more the security porosity is likely.

TABLE .1. CLOUD SECURITY MODELS PARAMETRIC ANALYSIS.



| | *The Cloud Multiple-Tenancy Model of NIST* | *The Cloud Risk Accumulation Model of CSA* | *JericoFormu's Cloud Cube Model* | *Default Gateway Platform* | *Multi-Cloud Database Model* | *End-user Authentication Control Model* |
|---|---|---|---|---|---|---|
| Technology Used | Virtualization | Layer dependency | Cloud formation | Three level defenses | Multi CSP and Secret sharing algorithm | EAD, EDF, CSP AD, EAQ. |
| Security Responsibility | CSP | CSP | End-user/CSP | End-user | CSP | End-user |
| Security effectiveness | Averagly Secured | Averagely Secured | Highly Secured | Highly Secured | Highly Secured | Highly Secured |
| Security Porosity | Less Likely | More Likely | More Likely | More Likely | Less Likely | Less Likely |
| Targeted Cloud Feature | Cloud Network Infrastructure (CNI) | CNI | CNI | Cloud Database | Cloud Data | Cloud Database and Cloud Enterprise Dataset. |
| Praticality | System Centred | System Centered | System centered | System and End-user centered | System centered | End-user and system centered |

## V. ATTRIBUTES OF THE PROPOSED END-USER AUNTHETICATION CONTROL MODEL

There are many identified cloud security issues, this includes embedded securing issues, application issues, trust and conviction issues, client management issues, cloud data storage issues, clustering computing issues and operating system-based issues. The above-mentioned cloud security issues can either be system centred or user centred or both. This paper is proposing a new cloud security model that will focus on incorporating the different components of end-user management issues in the model, which will enhance enterprise cloud data security and end- user experience. It can be classified as a user centred cloud security model which has both system and end-user practicality.

The end-user management issues can be broken down into the following issues: End-user experience issues, End-user authentication issues, End-user centric privacy, Service level management, Human factor, Forensic value, Reputation, Governance, Trusted third party and Lack of end-user trust. All the end-user management issues identified can be summed up into the “the role of human factor”; this is because the system end-users are humans and if all human factors influences are positive, then these issues can be managed if not eliminated. If human factors play no influencing role, there may be no issues at all. Subsequently the proposed model will look at the following: the different cloud delivery model (IaaS, PaaS, SaaS), the security responsibilities of the CSP and the end-user, the cloud data security (which are data integrity, data confidentiality and data availability) and the different technology possible.

End-user authentication control model in public ERP software based in cloud; is a cloud computing security model that use Enterprise Access Directory (EAD), Enterprise Database Fragmentation (EDF) in cloud and End-user Access Quires (EAQ) to control who have access to the enterprise data in cloud. There is need for a cloud authentication control model for an ERP software in cloud environment. The proposed model is to encourage end-user participation in enterprise cloud data security and to reduce the impact of malicious insider on the enterprise cloud data. The proposed model has the following distinctive features EAD, EDF and EAQ and can be classified as a SaaS data security model in cloud environment. For most SaaS, the CSP have the responsibility of security of the cloud system, but this issue is addressed in this model, as the new model will encourage the involvement of end-user in the SaaS cloud data security system.

### A. *Enterprise Access Directory*

This is a distinctive feature of the model. This is the directory that is created after the initial data classification within the enterprise. EAD is a list of key roles and responsibilities of the different roles within the enterprise and the level of data access for each role. This is roles and responsibilities database within the enterprise which should be the first point of call when an end-user intends to access data in cloud. The important advantage of the EAD is that no single role will have access to all the enterprise dataset at the same time. This feature of the model will resolve the impact an incident involving a malicious insider will have on the enterprise.

### B. *Enterprise Database Fragmentation*

This is a feature of the model that proposes that after an enterprise had undergone data classification as part of the procedures for moving data to private or public or hybrid cloud; the CSP should provide an enterprise database fragmentation for each set of the enterprise data being moved to cloud. A fragmented enterprise database in cloud would mean that enterprise authorised end-users only get access to the authorized set of information needed for their role at their enterprise.

### C. *CSP Access Directory*

Although a feature of the model but not a distinctive feature as this feature have already being proposed by authors like Kumari and Nath (2018) [2] in their paper “Data Security Model in Cloud Computing Environment”. This is simply a directory of cloud usernames and passwords kept by the CSP to use in validating each time an end-user is accessing data in cloud.

### D. *End-user Access Queries*

This is a distinctive feature of the cloud security model that triggers a set of queries when the end-user role is not classified in the EAD or when the end-user username/password is not determined by the CSP Access Directory. It will simply alert the Enterprise Cloud Administrator and denial access to the end-user. This will prompt the end-user to answer a set of generic questions that will help the Enterprise Cloud Administrator determine the end-user identity. The determined identity can then be used to set up or update the Enterprise Cloud Directory to accommodate the new end-user.

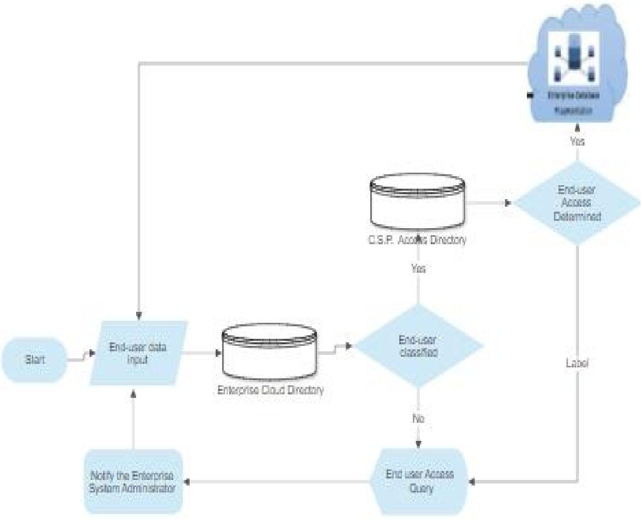

Enterprise Database Fragmentation
Yes
End-user Access Determined
C.S.P. Access Directory
Yes
Start
End-user data input
Enterprise Cloud Directory
End-user classified
Label
No
Notify the Enterprise System Administrator
End user Access Query

Fig. 3. End-user authentication control model in public cloud-based ERP software

## VI. Conclusion

This paper presented an end-user authentication control model in public ERP software based in cloud; as seen in Fig 3 above. The proposed model has two separate phases, the first security phase is handled by end-user enterprise and the second phase is handled by the CSP enterprise. The first security responsibility phase is when the enterprise classifies their data set according to their security importance and prepare their Enterprise Cloud Directory using their distinctive enterprise roles and responsibilities against the already classified dataset. The security responsibility of this first phase is managed by the end-user enterprise. The second security phase starts when a classified end-user is using the correct username and password to have access to a fragment of the enterprise database in the cloud. The second security phase has three features, the CSP Access Directory, the Enterprise Database Fragmentation and End-user Access Queries. The three features are managed by the Cloud Service Provider (CSP) and its security responsibility is solely the CSP to ensure. The proposed model when compared with other exiting model will encourage more end-user participation in their enterprise data security in cloud. The model also mitigates the impact a malicious insider will have on the enterprise cloud data set in cloud, since no single user can get access to the whole enterprise database in cloud at the same time. A look at MCDM and cloud ERPs could help determine how this improvement can boost cloud security and cloud ERP adoption by an enterprise. Our main research activity attempted to validate the concepts of the proposed model.

## ACKNOWLEDGMENT

This work would not have been possible without the financial support of the University of Strathclyde Faculty of Science Elite Scholarship Programme.

## REFERENCES

[1] S. Bhardwaj, L. Jain, and S. Jain, “An approach for investigating perspective of cloud software-as-a-service (SaaS),” *International Journal of Computer Applications,* vol. 10, no. 2, pp. 40-43, 2010.

[2] M. Kumari, and R. Nath, "Data Security Model in Cloud Computing Environment," *Cyber Security*, pp. 91-100: Springer, 2018.

[3] J. Janulevičius, L. Marozas, A. Čenys, N. Goranin, and S. Ramanauskaitė, "Enterprise architecture modeling based on cloud computing security ontology as a reference model." pp. 1-6. 2017

[4] Y. Chou, “Cloud Computing Primer for IT Pros,” *Microsoft: TechNet*, 2010.

[5] A. Q. Pei, M. Yang, and Y. B. Tang, "The Research Based on Security Model and Cloud Computing Strategy." pp. 1600-1603.

[6] S. H. Abbdal, H. Jin, A. A. Yassin, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien, and D. Zou, "An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage." pp. 412-417. 2016

[7] Z. Xin, L. Song-qing, and L. Nai-wen, "Research on cloud computing data security model based on multi-dimension." pp. 897-900.2012

[8] X. Li, J. Chen, and M. Luo, "A simple security model based on cloud reference model." pp. 155-159.

[9] K. Z. Bijon, R. Krishnan, and R. Sandhu, "A formal model for isolation management in cloud infrastructure-as-a-service." pp. 41-53.

[10] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud authentication based on anonymous one-time password," *Ubiquitous Information Technologies and Applications*, pp. 423-431: Springer, 2013.

[11] B. Tang, R. Sandhu, and Q. Li, “Multi-tenancy authorization models for collaborative cloud services,” *Concurrency and Computation: Practice and Experience,* vol. 27, no. 11, pp. 2851-2868, 2015.

[12] W.-T. Tsai, Q. Shao, and J. Elston, "Prioritizing service requests on cloud with multi-tenancy." pp. 117-124.

[13] H. Takabi, J. B. Joshi, and G.-J. Ahn, “Security and privacy challenges in cloud computing environments,” *IEEE Security & Privacy,* vol. 8, no. 6, pp. 24-31, 2010.

[14] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” *Journal of Internet services and applications,* vol. 1, no. 1, pp. 7-18, 2010.

[15] J. Che, Y. Duan, T. Zhang, and J. Fan, “Study on the security models and strategies of cloud computing,” *Procedia Engineering,* vol. 23, pp. 586-593, 2011.

[16] B. Kaur, and S. Sharma, “Parametric analysis of various cloud computing security models,” *International Journal of Information and Computation Technology, ISSN*, pp. 0974-2239, 2014.

[17] D. A. Chaturvedi, and S. A. Zarger, “A review of security models in cloud computing and an Innovative approach,” *International Journal of Computer Trends and Technology (IJCTT),* vol. 30, no. 2, pp. 87-92, 2015.

[18] M. A. Shahid, and M. Sharif, “Cloud computing security models, architectures, issues and challenges: A survey,” *SmartCR,* vol. 5, no. 6, pp. 602-616, 2015.

[19] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Data security model for cloud computing,” *Journal of Communication and Computer,* vol. 10, no. 08, pp. 1047-1062, 2013.

[20] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing." pp. CC-12-CC-17.

[21] I. Morozan, “Multi-clouds database: A new model to provide security in cloud computing,” *online)* https://www.researchgate.net/publication/273136522 *(accessed on Apr. 1, 2020)*.

[22] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-clouds." pp. 5490-5499. 2012