Trust-based Access Control Model with Quantification Method for Protecting Sensitive Attributes

Mohd Rafiz Salji[1], Nur Izura Udzir[2], Mohd Izuan Hafez Ninggal[3],
Nor Fazlida Mohd. Sani[4], Hamidah Ibrahim[5]
Faculty of Information Management,
Universiti Teknologi MARA, Malaysia[1]
Faculty of Computer Science and Information Technology,
Universiti Putra, Malaysia[2]

***Abstract*—The prevailing trend of the seamless digital collection has prompted privacy concerns to the organization. In enforcing the automation of privacy policies and laws, access control has been one of the most devoted subjects. Despite the recent advances in access control frameworks and models, there are still issues that hinder the implementation of successful access control. This paper illustrates the problem of the previous model which typically preserves data without explicitly considering the protection of sensitive attributes. This paper also highlights the drawback of the previous works which provides inaccurate calculation to specify user's trustworthiness. Therefore, a trust-based access control (TBAC) model is proposed to protect sensitive attributes. A quantification method that provides accurate calculation of the two user properties is also proposed, namely: seniority and behaviour to specify user's trustworthiness. Experiment have been conducted to compare the proposed quantification method and the previous quantification methods. The result shows that the proposed quantification method is stricter and accurate in specifying user's trustworthiness as compared to the previous works. Therefore, based on the result, this study resolves the issue of specifying the user's trustworthiness. This study also indicates that the issue of protecting sensitive attributes has been resolved.**

***Keywords*—Access control; trust-based access control; quantification method; sensitive attributes; privacy; privacy protection**

I. Introduction

Nowadays, information technology is growing exponentially, with an increasing number of hardware and software designed to make it easier for people to do their everyday work. This technology helps people to preserve their data privacy by using a wide variety of applications. Data can be collected, stored, and used for personal use or for work purposes. By using information technology, people can exchange data with the same interested party without any constraint of the boundary.

Data privacy is rapidly becoming one of the most crucial concerns in data management. People or customer is now more conscious about how their data are being protected by the organization. This awareness has been more highlighted when sharing and collecting data become seamless and prevalent by the omnipresence of Internet connection. In general, the organization collected, stored, and used customers' data for various purposes, and according to the Federal Trade Commission, U.S, 97 percent of websites were collected at least one type of identifying information such as name, e-mail address, or postal address of customers [1]. This could lead to misuse of customer data and less control over their privacy information. It may create privacy violations and fear to the customer [2]. Thus, data privacy should be protected in such a way that only authorized users can access the data. To protect data privacy, a relevant mechanism needs to be introduced by the company to build a solid trust with customers. The mechanism should be equipped with minimum requirements of reasonable access for privacy and security as stipulated in the Health Insurance Portability and Accountability Act (HIPAA, 1996).

There are several ways to protect data, but access control is the most common approach. It prohibits unauthorized access to the system resources as permitted by the policy [3], [4], [5], [6], [7], [8], [9], [10]. Trust-Based Access Control (TBAC) model is a popular access control paradigm that is influenced by an essential feature of human life that is trust. A user that is highly trusted would be given access to more resources as a part of this principle. However, trust is inconsistent in adapting to changing circumstances [11], [12]. Therefore, it is crucial to formulate an efficient access control model capable of capturing the complex essence of the scenario.

This paper addresses the issues of preserving sensitive attributes and determining the trustworthiness of the user. The previous TBAC models [13], [14], [15], which generally protect data without specifically focusing on protecting sensitive attributes, are outlined in this paper. Data is sensitive in nature, but sensitive attributes must be kept safe [16]. In general, data is categorized into three categories of attributes: de-identified, quasi identifier, and sensitive [17]. De-identified are the obvious identifying records that need to be hidden, such as the social security number. On the other hand, quasi identifier is a non-key attribute that has to be generalized before being published, such as race, age, and zip code, and finally, sensitive attributes are confidential data that belongs to a consumer privately, such as medical status and wages. According to the definitions of the three attributes, sensitive attributes require extremely restricted access in the system, with only trusted users permitted access to this attribute. In the previous models [13], [14], [15], trusted user, i.e., senior role, were granted more data access than the untrusted user, i.e.,

junior roles. However, these previous models did not mention which data could be accessed or not by trusted and untrusted users. This may lead the administrator to simply select any categories of data to be permitted or prohibited access by each trust level of the user. In this case, by not knowing which categories of data that is sensitive, the administrator may have the risk to disclose sensitive attributes to the untrusted user. Therefore, an access control model based on trust needs to be proposed to protect sensitive attributes.

Next, to access the resources, certain user properties need to be quantified to specify the user's trustworthiness whether the user is trusted or not to access it. Existing TBAC models [13], [14], [15] have been proposed to permit access to the resources of the system and introduce quantification methods by quantifying certain user properties to specify user's trustworthiness. If authorized user achieves highly trusted based on the calculation of user properties, they are permitted to access the data. However, these previous works provide an inaccurate assessment to specify a user's trustworthiness, which may cause the user who is still untrusted to become a trusted user. Therefore, an accurate quantification method needs to be proposed to calculate user properties to specify the user's trustworthiness. The measurement of the user properties with the detailed elements is also proposed to understand the process of calculation to specify the user's trustworthiness.

In summary, the main contributions of this paper are as follows:

1) An access control model based on trust is proposed to protect sensitive attributes.
2) A quantification method to calculate user properties to accurately specify user's trustworthiness is proposed.
3) A comprehensive set of calculations of user properties is proposed to understand the calculation process to specify the user's trustworthiness.

The rest of this paper is organized as follows: Section 2 provides the related works, while the user properties are discussed in Section 3. In Section 4, the proposed TBAC model framework is presented, while the calculation of user properties is described in Section 5. The proposed quantification method process is presented in Section 6, while the methodology is described in Section 7. The findings of this paper are explained in Section 8, and finally, Section 9 concludes the work.

II. Literature Review

In this section, the TBAC models which are closely related to the proposed model are discussed.

In the previous work, a trust-based RBAC model for pervasive computing systems has been proposed. Users' trustworthiness is evaluated by using the user properties, namely: experience and recommendation before they are assigned to roles or functions, i.e., senior role. The role is associated with trust. If the user achieves the minimum requirement of trust level set by an organization, the user can be assigned to that specific role and permitted to access the resources. A class of TBAC models with a very formal semantic that is expressed in a graph theory has been developed [13]. However, this previous model does not provide in detail how to quantify the user properties to determine the user's trustworthiness.

Previous work also proposes a privacy protection model to integrate trust management into access control [14]. The trust value of each requester is evaluated based on histories and recommendations. This model also includes purposes, obligations, and conditions that meet the requirements of modern cooperation, regulations, and privacy laws. However, this approach also does not include a thorough measurement of histories and recommendations to specify the user's trustworthiness to access the data.

The issue highlighted in the previous study [15] is the unreliability of the delegatee can cause disclosure of the delegator's privacy. Therefore, a multi-level delegation model with trust management has been proposed where delegation trustworthiness is organized in three levels: low, medium, and high. The more trustworthy the delegatee is, the more sensitive the delegation task able to be accessed by the delegatee. High denotes the person that has a higher level of trust. The low level of trust denotes the person that is less trusted, and finally, the medium level is the intermediate state. In this study, the evaluation of trust is based on the two interpretations of trust. First, the trust is based on the individual history and behaviour, called reliability trust, while the next interpretation is to capture trust by predicting trust trends in the forthcoming future, called future trust. However, this approach offers a general estimate of histories and recommendations to specify the user's trustworthiness.

A novel trust-based access control model in the cloud environment has been proposed to authorize the user and select the most trusted resources for the user [18]. The user trust value is evaluated based on the user behaviour parameter, and the resource trust value is evaluated based on the Service Level Agreement (SLA) parameter or the quality of service provided to the users. This model is compared with the existing Quality of Service (QOS) model and shows that the model performs better than the QoS model. However, the user trust value applied in the previous work is different as compared to the proposed work.

TrustRBAC is proposed based on trust and traditional role-based access model for single and multi-domain cloud environments [19]. The model calculates the direct trust and recommendation trust with security policies for both domains. The result shows that the TrustRBAC model effectively protects cloud users and secures its platform, thus achieving both the security and efficiency of the trust model. However, TrustRBAC model calculates using different properties as compared to the proposed model due to both works proposed in different environments.

A TBAC model is proposed with a comprehensive policy to specify the user's trustworthiness to access sensitive attributes and two properties are used to specify it, namely: seniority and behaviour [20]. Based on the calculation of both properties, if an authorized user achieves a higher level of trust (senior-with-trust), they can access sensitive attributes, otherwise, they are permitted to access data without sensitive attributes. However, this paper does not provide any test and validate the quantification method to specify the user's trustworthiness.

Finally, an access control model based on trust is pro-

posed for accessing data via cloud [21]. The level of user trustworthiness is classified into three levels: full, partial, and no view. The user who is trusted and semi-trusted is permitted to access a full and partial view of data, while the user who is untrusted is denied accessing data or no view. However, this paper does not provided any information on the calculation of user's trustworthiness.

All these works propose different approaches to protect the privacy of individuals by measuring different properties to specify the user's trustworthiness. The objective of this study is to preserve the sensitive attributes by using an access control model based on trust, and a quantification method is applied that provides an accurate measurement of the user properties to specify the user's trustworthiness. With this aim, this paper extends the previous works [13], [14], [15] by introducing an access control model based on trust that explicitly protects sensitive attributes, and in order to protect it, the user is calculated by using the quantification method to accurately specify the user's trustworthiness.

III. User Properties

In the TBAC model, certain user properties are required to determine the user's trust to access the resources. In the previous works [13], [14], [15], quantification methods have been introduced by calculating certain user properties to specify the user's trustworthiness to access the resources. However, the previous quantification methods have the limitation that provides an inaccurate formula to specify a user's trustworthiness that may cause the unauthorized user to become a trusted user to access the resources. In this study, due to the limitation of the previous works, a quantification method is proposed which provides the accurate calculation of the user properties, namely, seniority and behaviour to specify the user's trustworthiness. The discussion on seniority and behaviour is in the following sections.

A. Seniority

Seniority refers to the level of rank or position earned by a user or staff, which higher rank owns more priority compared to low. Based on previous works [13], [14], [15], experience or history is used to specify seniority which refers to the set of events or number of user activities that had occurred in the past within a certain period in which the user or trustee was involved and that the trustee has a recollection about. Examples of user activities include seminars, workshops, courses, and publications. However, this study is not only referring to the activities involved by the user, but the evidence that is relevant to calculate the seniority is also considered, for example, years in service, as this evidence is stated under the staffing policy [22]. Therefore, the evidence which is referred to the activities and relevant evidence is used to specify the seniority in this study. Seniority can be set in the role status attribute at the user's personal details. Two levels of user seniority are involved, junior (less trust) and senior (highly trust).

B. Behaviour

Behaviour refers to the user attitude or characteristic shown during their substantive service. Recommendation or trusted third-parties who have the knowledge about the user performance in service can be assigned by the administrator to evaluate the user behaviour [13]. In this study, the recommendation is set in the role trust attribute at the user's personal details. Three levels of user behaviour are involved in the proposed quantification method, mistrust (junior), trust (senior), and uncertainty (senior performing negative behaviour).

C. User's Trustworthiness and Access to the Resources

This section discusses the influence of user's trustworthiness in accessing the data especially sensitive attributes in the proposed model. If a user's seniority is assigned as a junior, the proposed work will automatically assign behaviour as mistrust. This is due to a junior referring to new staff, and mistrust refers to the staff that cannot be trusted. In this case, a user is still not achieving the minimum requirement of the seniority and behaviour set in the proposed quantification method. It denotes that a user is untrusted and is only permitted to access data without sensitive attributes. Next, a user also can be assigned the seniority as a senior, and behaviour is uncertainty. Previously, a user is assigned as senior with trust, but due to the user performing negative activities, for example, committing fraud, ignorance of obligation, and dishonest behaviour, unfortunately, an administrator has the right to change manually a user behaviour from trust to uncertainty. In this situation, a user has achieved a minimum requirement set in the proposed quantification method to become a senior, but the behaviour is set as uncertainty, which refers to a punishment for the user who performs wrongdoing. Therefore, a user is not permitted to access the sensitive attributes. Administrators, in this case, are the people at the top management level that are highly trusted to protect users' and customers' privacy. Finally, if user seniority is senior and behaviour is trust, a user is considered as a trusted user, and permitted to access the sensitive attributes. The influence of seniority and behaviour levels to authorize access to sensitive attributes is as shown in Fig. 1.

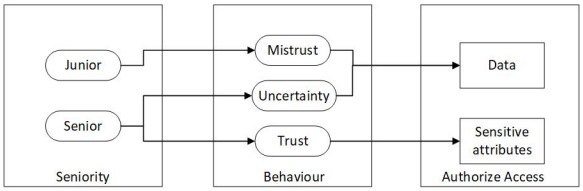

Fig. 1. User's Trustworthiness and Access to Sensitive Attributes

In this section, a proposed trust-based access control model is discussed. In general, to develop an access control model, three concepts are needed, access control model, policy, and mechanism [23], [10]. These three concepts are discussed in the proposed TBAC model framework as shown in Fig. 2.

The three main modules are discussed below.

1) Module 1: Access Control Policy
An access control policy is one of the concepts that need to be considered to implement access control. This policy is designed by organizations that are normally specific to their own use and may not be appropriate for other organizations [24]. In the

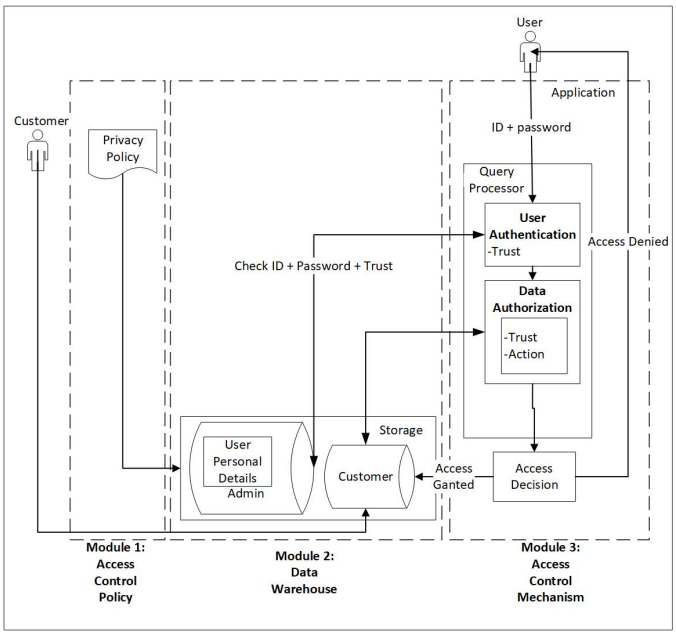

Fig. 2. The Proposed Trust-Based Access Control Model Framework

proposed model, access control policy issues are not part of the investigation.

2) Module 2: Data Warehouse
In this module, there are two databases involved in managing the proposed model, namely, the admin and customer database. These two databases are explained as follows:
   a) Admin database
   Admin database is used to collect the user data. In this database, the user personal details table is applied to store the user data. There are many particulars that can be collected from the user, but the user properties applied in the proposed model are the role status (user seniority) and role trust (user behaviour) attributes. These properties need to be identified before accessing sensitive attributes.
   b) Customer database
   Customer database store, maintain, and collect data from the customer. This database relates to the proposed model to permit authorized and trusted users only to access the customer data, particularly sensitive attributes.

3) Module 3: Access Control Mechanism
In access control, the data are protected by using two levels of access control mechanism, namely, user authentication and data authorization [25], [26], [27]. Normally, in the authentication stage, the user is authenticated based on username and password [28], [29]. However, due to privacy concerns by many parties, i.e., organization and customer, the expansion in terms of validating certain of the user properties must be considered to guarantee the correct user accesses the right data. As a result, the proposed model employs trust to authenticate the user to permit access to sensitive attributes.
In the next stage, the data are filtered based on certain user properties. If the user is trusted, sensitive attributes are rewarded to them, otherwise, the user is permitted to access data without sensitive attributes.

CALCULATION OF USER PROPERTIES

In order to specify the user's trustworthiness, a quantification method is required to quantify the user properties. In this section, the proposed quantification method is discussed to calculate the seniority and behaviour to specify the level of user's trustworthiness. The process of quantifying the seniority and behaviour in the proposed quantification method is described in the following sections.

D. Quantifying Seniority

In the proposed quantification method, the evidence is introduced to specify the user seniority. This evidence is stored in the user role history (URH) database and calculated by using the concept of weighing evidence [28] as shown in Fig. 3. The previous work [28] has suggested using weighing evidence to calculate the evidence that gives effect to the user's trustworthiness, however, the previous work has limitations to describe what is the user property used to be specified by the evidence. In this study, the weighing evidence is applied to calculate the evidence to specify the user seniority either senior or junior. The score of the evidence is stored in the URH database. The quantification of the evidence by using weighing evidence is discussed in the next section.

1) Weighing Evidence: In this study, weighing evidence is a method or decision process to quantify the evidence to specify the user seniority whether the user is senior or junior.

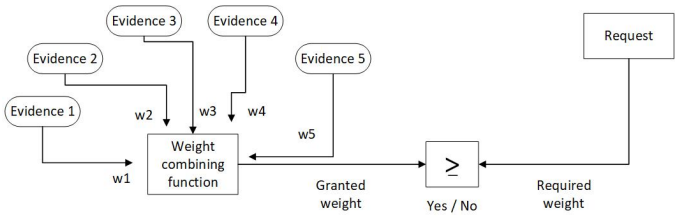

Fig. 3. Weighing Evidence

To quantify the evidence, the administrator needs to identify how many categories of evidence are to be set to calculate the seniority. However, the organization can determine the evidence as the different organization performs different evidence. For example, five categories of evidence are used to calculate the user Alice's seniority, i.e., years in service, seminars, workshops, courses, and publications. The value of calculating each category of evidence is between [0, 1] and the sum of this calculation is 1 [13]. In order to quantify the five categories of evidence, an administrator needs to decide the calculation on how to obtain the scores in each category. For example, the score of years in service can be based on how long a user works in an organization, e.g., a user obtains 0.1 mark for one year in service, and if a user has ten or more years in service, it means that the user obtains 1 mark or a full mark for years in the service category. The minimum required weight needs to be set by the administrator to specify whether the user is qualified to be a senior or not.

Let s denote the evidence and s needs to be calculated. The total sum of s is calculated as $(s_1 + \ldots + s_n)$. Then, the total sum of s is divided by a total number of evidence to obtain the result of user seniority us. The result is in the range of $[0, 1]$.

Hence, the administrator a must decide the minimum required weight of us. If the result of us is more than the required weight set by a, user u is assigned as a senior.

Assume the minimum required weight set by the administrator is 0.4. The calculation of user Alice's seniority is as follows: 1) Years in service = 0.5, 2) Seminars = 0.4, 3) Workshops = 0.6, 4) Courses = 0.3, 5) Publications = 0.7

The result of user Alice

```
   If seniority ≥ 0.4
   Result = senior
else
   Result = junior

(0.5 + 0.4 + 0.6 + 0.3 + 0.7) / 5 = 0.5
Result = senior
```

Based on the result, the user Alice's overall score is 0.5. This means that she is qualified as a senior.

E. Quantifying Behaviour

In this study, ten user behaviour categories are proposed to specify the user behaviour either trust or mistrust. Nine behaviour categories are proposed by Bruhn [30], and one category, self-discipline is proposed in this work as illustrated in Fig. 4. Self-discipline is included in this study as it is one of the user behaviour which is not included in the previous work [30], and it can be regarded as conscientiousness which implies a desire to do a task well and to take obligations to others seriously [31]. The justification for employing nine user behaviour categories in the proposed work is because they are based on a concept from prior work [30], and these categories were not undertaken in the computer domain. These categories are also used in the proposed work because the dataset collected and utilized in this model also uses the same categories. Subsequently, the reason for using self-discipline in the proposed work is because this category has been included in the dataset acquired from the Head of Studies Centers (HSCs). Therefore, these ten user behaviour categories are applied and quantified in the proposed quantification method to determine the user behaviour. The score of the ten user behaviour categories is stored in the recommendation database.

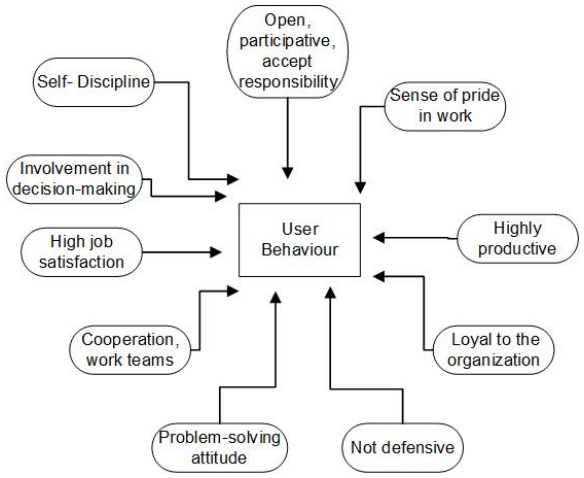

Fig. 4. User Behaviour Categories

The value of each category is between [0, 1] and the sum of these categories is 1 [13]. As mentioned earlier, the recommendation is applied in the previous works [13], [14], [15] to evaluate user behaviour. In this study, the recommendation is also used to evaluate the ten user behaviour categories. For example, if the mark of self-discipline is 0.1, the user obtains the lowest score, and if the score is 1 means the user obtains the highest score in that category. The minimum required weight needs to be set by the administrator to specify whether the user is qualified as trusted or mistrusted.

Let b denote the behaviour category and ten b needs to be quantified. The total sum of b is $(b_1 + \ldots + b_{10})$. Then, the total sum of b is divided by ten to obtain the result of a user behaviour ub. The result is in the range of $[0, 1]$. The ub is calculated as in Equation 1.

$$ub = \frac{1}{10} \sum_{i=1}^{10} b_i \tag{1}$$

Hence, the administrator a must decide the minimum required weight of ub. If the result of ub is more than the required weight set by a, user u is assigned as trust.

For example, assume the minimum required weight set by the administrator is 0.4. The user Alice's scores of behaviour is calculated as follows: 1) Open, participative, accept responsibility = 0.5, 2) Highly productive = 0.5, 3) Loyal to the organization = 0.5, 4) Not defensive = 0.5, 5) Cooperation, work teams = 0.5, 6) High job satisfaction = 0.5, 7) Problem-solving attitude = 0.5, 8) Involvement in decision-making = 0.5, 9) Sense of pride in work = 0.5, 10) Self-discipline = 0.5 The result of user Alice

```
   if behaviour ≥ 0.4
   Result = trust
else
   Result = mistrust

(0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 +
0.5 + 0.5 + 0.5) / 10 = 0.5
Result = trust
```

As a result, Alice's overall score is 0.5 and entitled as trust. In the previous work [32], the level of trust is introduced to identify the level of user's trustworthiness. However, each of the values is not set with the trust range, but the trust range is introduced in the notion of Vidyalakshmi et al. (2013). Therefore, in this proposed quantification method, the level of trust is introduced based on a combination of the previous works [32], [33] to identify the user level of trust, and this level of trust is as shown in Table I. This table indicates that the overall score of user Alice's behaviour is in Level 3, which is average.

TABLE I. LEVEL OF TRUST

Value	Meaning	Explanation	Trust Range
Level 0	Distrust Completely	Untrustworthy	0
Level 1	Ignorance	Cannot decide	0.1-0.19
Level 2	Minimal	Lowest trust	0.2-0.39
Level 3	Average	Mean trustworthiness	0.4-0.59
Level 4	Good	Trusted by major population	0.6-0.79
Level 5	Fully trust	Fully trustworthy	0.8-1

As mentioned earlier, three levels of user behaviour are proposed in this study, trust, mistrust, and uncertainty. Based on the quantification of user behaviour, only two levels of user behaviour are involved, trust and mistrust. As explained earlier, uncertainty is changed manually from the trust by an administrator. Previously, the user is set as a senior-with-trust, and as the user is performing negative activities, the user is set as a senior-with-uncertainty. Therefore, the user is not allowed to access sensitive attributes.

F. Computation of Trustworthiness

In this study, the user's seniority and behaviour are quantified to determine the level of user's trustworthiness. If the calculation of seniority attains the minimum required weight set by the administrator, but the calculation of behaviour does not achieve minimum requirement or vice versa, the user is not assigned as senior-with-trust. In this case, both properties should achieve the minimum requirement set by the administrator to become a trusted user, or else the user is still set as a junior-with-mistrust. For example, based on the previous sections (refer Section III - D1 & E), the user Alice's trustworthiness needs to be specified. The result of the user that is trusted is set as 1, while the untrusted user is stated as 0. The calculation to specify Alice's trustworthiness is as follows:

The result of user Alice

```
   if (Seniority ≥ 0.4) & (Behaviour ≥
0.4)
   Result = 1
else
   Result = 0

(Seniority = 0.5) & (Behaviour = 0.5)
Result = 1
```

As a result, both properties of user Alice has achieved the minimum requirement and she has qualified to become a trusted user. Based on the result, Alice is allowed to access sensitive attributes in the proposed model. In the next section, the function and process in the proposed quantification method to specify the user's trustworthiness are discussed.

IV. PROPOSED QUANTIFICATION METHOD

In this section, the framework of the proposed quantification method is designed to discuss each function and process. The framework is composed of two main modules, and it is shown in Fig. 5. The two main modules are as follows:

1) Data Warehouse
2) Request and Calculation

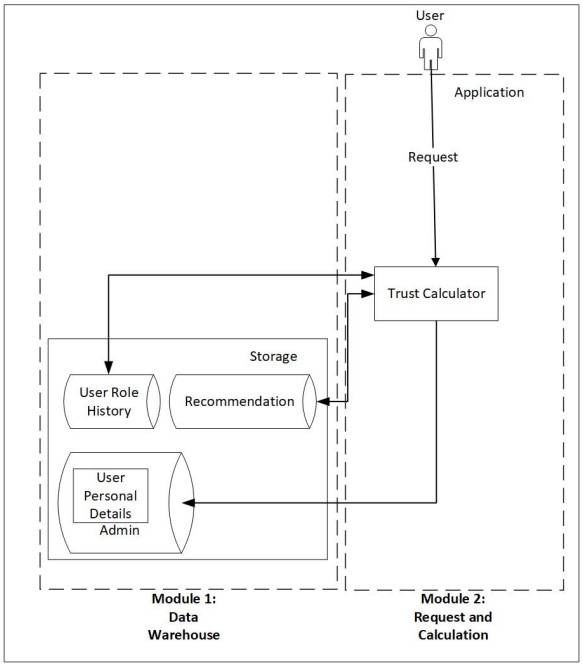

Fig. 5. The Proposed Quantification Method Framework

Now, the two main modules are discussed.

1) Data Warehouse
This module refers to the three databases, user role history (URH), recommendation, and admin database. These databases are used to collect different types of

data. The explanation of these three databases is as follows:

a) User role history (URH) database
In the previous works [14], [15], [13], the URH database is applied to store the score of activities. In the proposed quantification method, the score of evidence is stored in the same database to quantify the evidence to specify the user seniority whether the user is senior or junior. If a user requested to be a trusted user, the score of a user's evidence is calculated in the trust calculator to specify the user seniority. After specifying the user seniority, the result is stored in the admin database.

b) Recommendation database
In the previous works [14], [13], a recommendation database is introduced to store the score of user's behaviour. This score is supplied by the recommendation or evaluator who knows the user. In the proposed quantification method, the recommendation database is also used to store the score of the user behaviour based on the ten user behaviour categories to specify whether the user is trusted or mistrusted. If a user requests to become a trusted user, the score of ten user behaviour categories is calculated in the trust calculator to specify the user behaviour. The result is stored in the admin database after specifying the user behaviour.

c) Admin database
After the user seniority and behaviour are quantified, the result is stated in this database at the user personal details table. The user personal details table includes the user information and some of the attributes are assigned for user authentication. In the proposed quantification method, role status and role trust attributes are used to state the result based on the quantification of the user seniority and behaviour. The role status attribute is used to state the user's seniority whether the user is junior or senior, while the role trust attribute is used to state the result of user behaviour either trust, mistrust, or uncertainty. Based on both attributes, the results can be used in the proposed model to identify user's trustworthiness to access sensitive attributes.

2) Request and Calculation
In this module, the request to calculate user's trustworthiness and calculation of the user properties is discussed as follows:

a) User: Refers to new staff or a user who requested to become a trusted user. A new user is set as a junior-with-mistrust or untrusted user and requested to be set as a senior-with-trust or trusted user. A user needs to request from the system to quantify user properties to specify the user's trustworthiness. The quantification procedure will then be carried out automatically. A senior-with-uncertainty user can also be requested to be set as a senior-with-trust where the proposed work will re-evaluate user behaviour by re-calculating the ten user behaviour categories to specify whether the user is trusted or maintained to uncertainty. However, if the user performs wrongdoing, the administrator is responsible for manually changing user trust from senior-with-trust to senior-with-uncertainty. The proposed quantification method obtains the score of user evidence at the URH database to calculate the user seniority, while the score of ten user behaviour categories is taken from the recommendation database to calculate the user behaviour. Based on the calculation of both properties, the result is stored in the admin database.

b) Trust calculator: In this process, the user seniority and behaviour are quantified to specify the user's trustworthiness. If the result of user seniority is senior, but the user behaviour is mistrust, or the user seniority is junior, but the user behaviour is trust, the user is still considered as an untrusted user. The user is considered trusted if the user is set as a senior-with-trust.

V. Methodology

The proposed quantification method needs to be developed to test whether it can be used to specify or not a user's trustworthiness by quantifying the user properties, seniority, and behaviour. Both properties are quantified by using a dataset. Next, the proposed quantification method needs to be validated by comparing the calculation of the user properties to specify the user's trustworthiness with the previous quantification methods [13], [14], [15]. The proposed quantification method shows the calculation of the user seniority and behaviour, while the previous quantification methods present the quantification of the user history | experience and recommendation. The dataset is explained in the following section.

A. Dataset

To test the proposed quantification method, the dataset is required to calculate the user seniority and behaviour to specify the user's trustworthiness. This study uses a dataset that contains staff data that refer to their performance assessment, and the data need to be prepared every year-end. This dataset is applied in this study due to containing the data of user seniority and behaviour to evaluate the lecturer's performance. It is acquired from the Head of Studies Centers (HSCs) at Universiti Teknologi MARA, Sarawak who are responsible to assess the performance of the lecturer under the HSC's responsibility.

In this study, 48 original user data (refer to Appendix) are collected from the HSCs. The data are then expanded as synthetic data to show the variety of results from the different numbers of user data. The function of random between (RANDBETWEEN) is applied to increase the amount of data

until 500 users. Then, this study shows the pattern of the proposed quantification method results between the original and synthetic data. Next, the proposed quantification method is compared with the previous works [13], [14], [15] to highlight the differences of results between the proposed work and the previous works.

B. Proposed Quantification Method

This section discusses the proposed quantification method in quantifying the user seniority and behaviour to specify the user's trustworthiness. To show the result of user's trustworthiness, four tests are conducted where the first test used 48 original data, while, the following three tests [7], [34] are conducted by using synthetic data with a different number of users, i.e, 100, 300, and 500 to understand the pattern of the result between the original and synthetic data in the proposed and previous works. The calculation results of both user properties to quantify user's trustworthiness are discussed in the following sections.

1) Test on Quantification of Seniority: In this study, to test the quantification of user seniority, the result is in the range of [0, 1]. Since the total score of activities in the dataset is set as 10 marks, therefore it needs to be calculated as follows: (score of user's seniority / 10). The minimum requirement to be a senior is set at 0.8 marks based on the pattern that the majority of the users attain that minimum score. To calculate the user seniority, the score of **User 3** as shown in Table II is used as an example. It shows that User 3 has reached the minimum requirement and qualified as a senior.

TABLE II. LEVEL OF USERS' SENIORITY

No.	Name	Activity / Contribution	Total	Rolestatus
1	User 1	8	0.8	senior
2	User 2	9	0.9	senior
3	User 3	8	0.8	senior
4	User 4	6	0.6	junior
5	User 5	7	0.7	junior
6	User 6	8	0.8	senior
7	User 7	8	0.8	senior
8	User 8	8	0.8	senior
9	User 9	8	0.8	senior
10	User 10	9	0.9	senior

As mentioned earlier, four tests are conducted to obtain the results of the quantification of users' seniority in the proposed work. These results of the four tests are applied to specify the user's trustworthiness in the following section. The results are as shown in Table III.

2) Test on Quantification of Behaviour: To test the quantification of user behaviour, the result is set in the range of [0, 1]. The total score of each category is set as 10 marks. This study has ten categories of user behaviour, therefore, the total score of all categories is set as 100 marks. The calculation of the user behaviour is set as follows: (sum of all categories / 100). The minimum requirement to attain a level of trust is set at 0.8 marks due to the majority of users attaining that minimum score. The score of **User 3** as shown in Table IV is applied as an example to calculate the user behaviour. It shows that User 3 has accomplished the minimum requirement where the score is 0.9. Based on Table I, User 3 is in level 5 means the user is fully trusted.

TABLE III. RESULT OF THE USERS' SENIORITY

Test	Senior	Junior	Total
1	36	12	48
2	54	46	100
3	138	162	300
4	229	271	500

Four tests are conducted to quantify the user behaviour in the proposed work. These tests are utilized to specify the user's trustworthiness in the next section. The results of the four tests are shown in Table V.

3) Result of User's Trustworthiness: In the previous sections (refer Section V - B1 & B2), four tests are conducted to calculate the users' seniority and behaviour and the results of both properties have been specified. Then, this section enlightens how to specify the users' trustworthiness. The result of the user that is trusted is set as 1, while the untrusted user is stated as 0. The result of users' trustworthiness is shown in Table VI. For example, in Table VI, the score of **User 3** are as follows:

The result of User 3

```
if (Seniority ≥ 0.8) & (Behaviour ≥ 0.8)
   Result = 1
else
   Result = 0

(Seniority = 0.8) & (Behaviour = 0.9)
Result = 1
```

As a result, both properties of User 3 have achieved the minimum requirement and are qualified to become trusted user. Based on the result, User 3 is allowed to access sensitive attributes in the proposed model.

Based on the four tests to specify the users' seniority and behaviour, the results are utilized to specify the user's trustworthiness in the proposed quantification method. The result of the four tests to specify the users' trustworthiness are as shown in Table VII.

Next, the discussion is on the calculation of the previous quantification methods [13], [14], [15], and later validate the proposed quantification method by comparing the result of the calculation with the previous quantification methods.

C. Existing Quantification Methods

The calculation of the previous quantification methods is as shown in Table VIII. By using the same score of both properties as in the proposed quantification method, then the combination of both properties in the previous quantification methods is calculated as follows: (Experience + Recommendation) / 2. The result of the user that is trusted is set as 1, while the untrusted user is stated as 0. For example, in Table VIII, the score of **User 3** are as follows:

The result of User 3

```
   if (Average [Experience | History +
Recommendation] 0.8)
   Result = 1
```

TABLE IV. QUANTIFICATION AND LEVEL OF USERS' BEHAVIOUR

No	Name	open	productive	loyalty	not defensive	cooperation	job satisfaction	problem solver	decision maker	sense of pride	discipline	Total	Activity	Total
1	User 1	9	9	9	9	9	9	9	9	9	9	0.9	8	0.8
2	User 2	9	9	9	9	9	9	9	9	9	9	0.9	9	0.9
3	User 3	9	9	9	9	9	9	9	8	9	9	0.9	8	0.8
4	User 4	8	8	8	8	9	8	9	8	8	9	0.8	6	0.6
5	User 5	8	8	9	9	8	9	9	8	9	9	0.9	7	0.7
6	User 6	9	8	9	9	9	9	9	8	9	9	0.9	8	0.8
7	User 7	9	8	9	9	8	9	9	8	9	9	0.9	8	0.8
8	User 8	9	8	9	9	9	9	9	8	9	9	0.9	8	0.8
9	User 9	8	8	9	9	8	8	9	8	9	9	0.9	8	0.8
10	User 10	9	9	9	9	9	9	9	8	9	9	0.9	9	0.9

TABLE V. RESULT OF THE USERS' BEHAVIOUR

Test	Trust	Mistrust	Total
1	46	2	48
2	79	21	100
3	207	93	300
4	343	157	500

TABLE VI. RESULT OF USERS' TRUSTWORTHINESS

No	Name	**TOTAL**	rolestatus	**TOTAL**	roletrust	**RESULT**
1	User 1	0.8	senior	0.9	trust	1
2	User 2	0.9	senior	0.9	trust	1
3	User 3	0.8	senior	0.9	trust	1
4	User 4	0.6	junior	0.8	trust	0
5	User 5	0.7	junior	0.9	trust	0
6	User 6	0.8	senior	0.9	trust	1
7	User 7	0.8	senior	0.9	trust	1
8	User 8	0.8	senior	0.9	trust	1
9	User 9	0.8	senior	0.9	trust	1
10	User 10	0.9	senior	0.9	trust	1

```
else
   Result = 0

(0.8 + 0.9) / 2 = 0.9
Result = 1
```

Based on the result of User 3 in the previous quantification methods, by merging the score of both properties, the user has achieved the minimum requirement to become a trusted user.

Similar to the proposed quantification methods, the four tests are conducted to determine user's trustworthiness in the previous quantification methods. These results are used to compare with the proposed quantification method in the next section. The results of the four tests are shown in Table IX.

VI. FINDINGS

In this section, the proposed quantification method needs to be validated by comparing the calculation with the previous methods. Table X shows the comparison of the result between the proposed and previous quantification methods [13], [14], [15]. Based on the results of the previous examples (refer Section V - B3 & C), User 3 in the proposed quantification method and previous quantification methods achieve the same result which is 1 or qualified as a trusted user. In this case, there is no difference between both methods because both of them achieve the same results, even the calculation of both methods is different. However, the result of User 5 is different as compared to User 3. The discussion on **User 5** are as follows:

TABLE VII. RESULT OF THE USERS' TRUSTWORTHINESS IN THE PROPOSED QUANTIFICATION METHOD

Test	Trusted User	Untrusted User	Total
1	36	12	48
2	45	55	100
3	101	199	300
4	166	334	500

TABLE VIII. RESULT OF USERS' TRUSTWORTHINESS DATA FOR THE PREVIOUS QUANTIFICATION METHODS

No	Name	Experience / history / seniority	Recommendation / behaviour	TOTAL	RESULT
1	User 1	0.8	0.9	0.9	1
2	User 2	0.9	0.9	0.9	1
3	User 3	0.8	0.9	0.9	1
4	User 4	0.6	0.8	0.7	0
5	User 5	0.7	0.9	0.8	1
6	User 6	0.8	0.9	0.8	1
7	User 7	0.8	0.9	0.8	1
8	User 8	0.8	0.9	0.8	1
9	User 9	0.8	0.9	0.8	1
10	User 10	0.9	0.9	0.9	1

TABLE IX. RESULT OF THE USERS' TRUSTWORTHINESS IN THE EXISTING QUANTIFICATION METHODS

Test	Trusted User	Untrusted User	Total
1	40	8	48
2	66	44	100
3	171	129	300
4	298	202	500

Result in the **Previous Quantification Methods**:

```
   if (Average [Experience | History +
Recommendation] ≥ 0.8)
   Result = 1
else
   Result = 0

(0.7 + 0.9) / 2 = 0.8
Result = 1
```

Result in the **Proposed Quantification Method**:

```
   if (Seniority ≥ 0.8) & (Behaviour ≥
0.8)
   Result = 1
else
```

```
   Result = 0

(Seniority = 0.7) & (Behaviour = 0.9)
Result = 0
```

Based on the results of User 5, both methods show different results where the previous quantification methods achieve the minimum requirement to become a trusted user, while the proposed work shows the result is 0 or untrusted user. In the previous quantification methods, by combining the amount of both properties, User 5 achieves the minimum requirement to become a trusted user even the user seniority is still a junior. However, in the proposed quantification method, the rule is both user properties must achieve the minimum requirement, but unfortunately, User 5 in the proposed work does not achieve the minimum requirement of seniority to become a senior. Therefore, the result of User 5 is the untrusted user. These comparisons show the calculation in the proposed quantification method is stricter and accurate as compared to the previous quantification methods to be a trusted user.

In order to validate the proposed work, the results of the four tests of specifying the users' trustworthiness in the proposed work and previous works need to be compared. Based on Tables VII and IX, the results in Test 1 show the previous works and proposed work have many trusted users as compared to untrusted users. However, previous works have more trusted users, which are 40 people or 83.3% than the proposed work is only 36 people or 75%.

In Test 2, the result of a trusted user in the previous works and proposed work is different as compared to Test 1. The previous works show 66 people or 66% are trusted users, while the proposed work shows untrusted users are more than trusted users where trusted users recorded as only 45 people out of 100 or 45%. Although the percentage of the trusted users in the previous works declined as compared to Test 1, the previous works maintain records as a higher number of trusted users than the proposed work.

Test 3 also shows the same trend where the number of trusted users in the previous works and proposed work which are 171 people or 57% and 101 people or 33.7% decreasing as compared to Test 1 and Test 2. However, the previous works show the same pattern with more trusted users as compared to the proposed work.

Finally, in Test 4, the previous quantification methods show 298 users or 59.6% with an increase in the number of trusted users as compared to Test 3, while the proposed quantification method shows the same trend of decreasing number of trusted users that is only 166 users or 33.2%. However, Test 4 also shows the same trend with the proposed quantification method obtaining a smaller number of trusted users as compared to previous works.

To compare the pattern of the trusted user in Test 1 (original data) and three tests by using synthetic data, the results show the same pattern which the number of trusted users in the original and synthetic data is smaller in the proposed work as compared to the previous works. The reason for a smaller number of trusted users in the proposed work is because the proposed work provides strict rules which to ensure both properties achieve a minimum requirement to be a trusted user. The rule in the proposed work is accurate as compared to previous works because the proposed work ensures only the user who achieves the minimum requirement of both properties is qualified as a trusted user. As compared to the previous works, both properties are combined without considering both properties have achieved the minimum requirements or not. If achieves the minimum requirement, the user is entitled as a trusted user. Therefore, this comparison shows that the proposed quantification method is stricter and accurate in specifying user's trustworthiness as compared to the previous works.

The proposed method's strict rule achieves the notion of privacy by restricting data access to only authorized users [35], [36]. Even while previous work restricted access to authorized users in this scenario, the technique is insufficient to properly identify trusted users as compared to the proposed method, which allowed only trusted users to access sensitive attributes. Therefore, a strict rule is required in the proposed method to produce an accurate result.

In this study, there are three differences between the proposed quantification method and previous quantification methods [13], [14], [15].

1) Previous works applied the quantification methods to quantify certain properties to specify the user's trustworthiness to access data. While the proposed work uses a comprehensive set of quantification method which use the user seniority and behaviour to specify the user's trustworthiness, and later in the proposed access control model, the user's trustworthiness can only be identified to access sensitive attributes.
2) Previous works have a limitation which provides inaccurate calculation to quantify the user properties. However, this study proposes the quantification method with stricter and accurate calculations to specify the user's trustworthiness.
3) The score of experience and recommendation [13] and history and recommendation [14], [15] have been calculated and merged to specify the user's trustworthiness. However, the proposed work does not combine the score of seniority and behaviour to specify the user's trustworthiness. Therefore, the proposed work provides better calculation because the proposed work has to make sure both properties achieve a minimum requirement to become a trusted user.

VII. Conclusion

In this paper, a TBAC model has been proposed to protect sensitive attributes. A quantification method also has been proposed by providing accurate measurement of the two user properties, namely: seniority and behaviour to specify the user's trustworthiness. A detailed measurement of user properties is also proposed to understand the process of specifying the user's trustworthiness. Test and validation of the proposed quantification method have been conducted to prove that it can be used to specify the user's trustworthiness and compare it with the previous quantification methods. The result shows that the proposed quantification method is stricter and accurate in specifying user's trustworthiness as compared to the previous

TABLE X. RESULT OF THE PROPOSED AND PREVIOUS QUANTIFICATION METHODS

No	Name	Experience / History / Seniority	Rolestatus	Recommendation / Behaviour	Roletrust	RESULT - Proposed Method	TOTAL - Previous Methods	RESULT - Previous Methods
1	User 1	0.8	senior	0.9	trust	1	0.9	1
2	User 2	0.9	senior	0.9	trust	1	0.9	1
3	User 3	0.8	senior	0.9	trust	1	0.9	1
4	User 4	0.6	junior	0.8	trust	0	0.7	0
5	User 5	0.7	junior	0.9	trust	0	0.8	1
6	User 6	0.8	senior	0.9	trust	1	0.8	1
7	User 7	0.8	senior	0.9	trust	1	0.8	1
8	User 8	0.8	senior	0.9	trust	1	0.8	1
9	User 9	0.8	senior	0.9	trust	1	0.8	1
10	User 10	0.9	senior	0.9	trust	1	0.9	1

works. Based on the result, the issue of the previous works [13], [14], [15] have limitation which provides inaccurate calculation to specify user's trustworthiness has been solved. The issue of the previous access control models based on trust which focuses on generally protecting data without considering specifically protecting sensitive attributes also has been solved.

In future work, further development needs to be considered. First, many different types of access control models are employed to preserve privacy, such as blockchain-based access control [37], cloud-based access control [38], provenance-based access control model [39], and situation-based access control [40]. Therefore, this is an opportunity for researcher to develop alternative access control models to address the challenge of keeping privacy, particularly sensitive attributes. Next, the suggested quantification method may be adapted to specify authorized users or subjects to access resources in another environment, such as blockchain or cloud.

REFERENCES

[1] ANSI, "American national standard for information technology role based access control," *ANSI INCITS*, pp. 359–2004, February 2004.

[2] J.-W. Byun, E. Bertino, and N. Li, "Purpose based access control of complex data for privacy protection," in *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '05. New York, NY, USA: ACM, 2005, pp. 102–110. [Online]. Available: http://doi.acm.org/10.1145/1063979.1063998

[3] C. Bertolissi and M. Fernández, "A metamodel of access control for distributed environments: Applications and properties," *Information and Computation*, 2014.

[4] J. Crampton and J. Sellwood, "Path conditions and principal matching: A new approach to access control," in *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*. ACM, 2014, pp. 187–198.

[5] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role-based access control: Towards a unified standard," in *ACM Workshop on Role-based Access Control*, vol. 2000, 2000.

[6] P. C. Hung, "Towards a privacy access control model for e-healthcare services." in *Third Annual Conference on Privacy, Security and Trust, October 12-14, 2005, The Fairmont Algonquin, St. Andrews, New Brunswick, Canada, Proceedings*, 2005.

[7] A. Kayes, J. Han, and A. Colman, "A semantic policy framework for context-aware access control applications," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*, July 2013, pp. 753–762.

[8] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," *Computer Science Review*, vol. 4, no. 2, pp. 81–99, 2010.

[9] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," in *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*. IEEE, 2012, pp. 556–563.

[10] P. Samarati, "Protecting respondents identities in microdata release," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 13, no. 6, pp. 1010–1027, 2001.

[11] S. Vahabli and R. Ravanmehr, "A novel trust-based access control for social networks using fuzzy systems," *World Wide Web*, vol. 22, no. 6, pp. 2241–2265, 2019.

[12] B. Zhao, C. Xiao, Y. Zhang, P. Zhai, and Z. Wang, "Assessment of recommendation trust for access control in open networks," *Cluster Computing*, vol. 22, no. 1, pp. 565–571, 2019.

[13] M. Toahchoodee, R. Abdunabi, I. Ray, and I. Ray, "A trust-based access control model for pervasive computing applications," in *Data and Applications Security XXIII*. Springer, 2009, pp. 307–314.

[14] M. Li, H. Wang, and D. Ross, "Trust-based access control for privacy protection in collaborative environment," in *e-Business Engineering, 2009. ICEBE'09. IEEE International Conference on*. IEEE, 2009, pp. 425–430.

[15] M. Li, X. Sun, H. Wang, and Y. Zhang, "Multi-level delegations with trust management in access control systems," *Journal of Intelligent Information Systems*, vol. 39, no. 3, pp. 611–626, 2012.

[16] N. Maheshwarkar, K. Pathak, and N. S. Choudhari, "K-anonymity model for multiple sensitive attributes," *International Journal of Computer Applications (IJCA)*, 2012.

[17] L. Sweeney, "K-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[18] P. K. Behera and P. M. Khilar, "A novel trust based access control model for cloud environment," in *Proceedings of the International Conference on Signal, Networks, Computing, and Systems*. Springer, 2017, pp. 285–295.

[19] C. Uikey and D. Bhilare, "TrustRBAC: Trust role based access control model in multi-domain cloud environments," in *Information, Communication, Instrumentation and Control (ICICIC), 2017 International Conference on*. IEEE, 2017, pp. 1–7.

[20] M. R. Salji, N. I. Udzir, M. I. H. Ninggal, N. F. M. Sani, and H. Ibrahim, "Performance-aware trust-based access control for protecting sensitive attributes," in *International Conference on Soft Computing and Data Mining*. Springer, 2016, pp. 560–569.

[21] A. Singh, U. Chandra, S. Kumar, and K. Chatterjee, "A secure access control model for e-health cloud," in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, 2019, pp. 2329–2334.

[22] S. Ganesan and B. A. Weitz, "The impact of staffing policies on retail buyer job attitudes and behaviors," *Journal of Retailing*, vol. 72, no. 1, pp. 31–56, 1996.

[23] S. Castano and E. Ferrari, "Protecting datasources over the web: Policies, models and mechanisms," in *Web-Powered Databases*. IGI Global, 2003, pp. 299–330.

[24] N. Abdul Ghani, "Credential purpose-based access control for personal data protection in web-based applications," Ph.D. dissertation, Universiti Teknologi Malaysia, Faculty of Computing, 2013.

[25] T. Ercan and M. Yıldız, "Semantic access control for corporate mobile devices," in *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2010, pp. 198–207.

[26] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in distributed systems: Theory and practice," *ACM Transactions on Computer Systems (TOCS)*, vol. 10, no. 4, pp. 265–310, 1992.

[27] T. Singh and R. Kumar, "Database and information security concerns," *International Journal of Computer Science & Technology.*, vol. 4, no. 2, pp. 211–215, 2011.

[28] D. Gollmann, "From access control to trust management, and back–a petition," in *IFIP International Conference on Trust Management*. Springer, 2011, pp. 1–8.

[29] S. Harris, *Mike Meyers' CISSP Certification Passport*. McGraw-Hill/Osborne, 2002.

[30] J. G. Bruhn, *Trust and the Health of Organizations*. Springer Science & Business Media, 2001.

[31] S. Bai, B. Hao, A. Li, S. Yuan, R. Gao, and T. Zhu, "Predicting big five personality traits of microblog users," in *Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)-Volume 01*. IEEE Computer Society, 2013, pp. 501–508.

[32] M. Kim, J. Seo, S. Noh, and S. Han, "Identity management-based social trust model for mediating information sharing and privacy enhancement," *Security and Communication Networks*, vol. 5, no. 8, pp. 887–897, 2012.

[33] B. Vidyalakshmi, R. K. Wong, and C.-H. Chi, "Decentralized trust driven access control for mobile content sharing," in *Big Data (BigData Congress), 2013 IEEE International Congress on*. IEEE, 2013, pp. 239–246.

[34] A. Kayes, J. Han, and A. Colman, "An ontological framework for situation-aware access control of software services," *Information Systems*, 2015.

[35] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[36] C. S. Powers, P. Ashley, and M. Schunter, "Privacy promises, access control, and privacy management. enforcing privacy throughout an enterprise by extending access control," in *Proceedings. Third International Symposium on Electronic Commerce,*. IEEE, 2002, pp. 13–21.

[37] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "Authprivacychain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70 604–70 615, 2020.

[38] A. A. Almtrf, "Cloud-based access control to preserve privacy in academic web services," Ph.D. dissertation, Oakland University, 2020.

[39] A. Bates, B. Mood, M. Valafar, and K. Butler, "Towards secure provenance-based access control in cloud environments," in *Proceedings of the third ACM conference on Data and application security and privacy*. ACM, 2013, pp. 277–284.

[40] D. Beimel and M. Peleg, "Using owl and swrl to represent and reason with situation-based access control policies," *Data & Knowledge Engineering*, vol. 70, no. 6, pp. 596–615, 2011.

APPENDIX

No	Name	open	productive	loyalty	not defensive	cooperation	job satisfaction	problem solver	decision maker	sense of pride	discipline	Total	Activity	Total
1	User 1	9	9	9	9	9	9	9	9	9	9	0.9	8	0.8
2	User 2	9	9	9	9	9	9	9	9	9	9	0.9	9	0.9
3	User 3	9	9	9	9	9	9	9	8	9	9	0.9	8	0.8
4	User 4	8	8	8	8	9	8	9	8	8	9	0.8	6	0.6
5	User 5	8	8	9	9	8	9	9	8	9	9	0.9	7	0.7
6	User 6	9	8	9	9	9	9	9	8	9	9	0.9	8	0.8
7	User 7	9	8	9	9	8	9	9	8	9	9	0.9	8	0.8
8	User 8	9	8	9	9	9	9	9	8	9	9	0.9	8	0.8
9	User 9	8	8	9	9	8	8	9	8	9	9	0.9	8	0.8
10	User 10	9	9	9	9	9	9	9	8	9	9	0.9	9	0.9
11	User 11	8	8	9	9	9	8	9	8	9	9	0.9	6	0.6
12	User 12	9	9	9	9	9	9	9	8	9	9	0.9	8	0.8
13	User 13	7	6	8	9	6	8	8	6	8	9	0.8	5	0.5
14	User 14	8	8	9	9	8	8	9	8	9	9	0.9	6	0.6
15	User 15	8	8	9	9	9	9	9	8	9	9	0.9	8	0.8
16	User 16	8	8	9	9	9	9	9	8	9	9	0.9	9	0.9
17	User 17	8	8	9	9	9	9	9	8	9	9	0.9	8	0.8
18	User 18	8	8	9	9	9	9	9	8	9	9	0.9	8	0.8
19	User 19	8	8	9	9	8	8	9	8	8	9	0.8	6	0.6
20	User 20	8	8	9	9	9	8	9	8	9	9	0.9	8	0.8
21	User 21	8	6	9	8	6	8	8	6	8	9	0.8	6	0.6
22	User 22	7	6	8	9	6	8	7	6	8	9	0.7	5	0.5
23	User 23	6	6	8	9	6	8	7	6	8	9	0.7	4	0.4
24	User 24	10	7	10	10	8	10	7	7	10	9	0.9	8	0.8
25	User 25	9	7	10	10	8	9	8	8	9	10	0.9	8	0.8
26	User 26	10	8	9	10	9	9	8	9	9	10	0.9	8	0.8
27	User 27	10	9	10	10	9	10	7	8	10	10	0.9	8	0.8
28	User 28	10	9	10	10	9	9	8	8	10	10	0.9	8	0.8
29	User 29	10	7	10	10	8	9	7	7	9	10	0.9	8	0.8
30	User 30	10	7	10	10	8	9	8	8	9	10	0.9	8	0.8
31	User 31	9	7	9	10	8	9	7	8	9	10	0.9	8	0.8
32	User 32	10	7	10	10	8	9	8	8	9	10	0.9	8	0.8
33	User 33	8	7	9	10	7	8	7	7	8	10	0.8	7	0.7
34	User 34	9	7	10	10	9	10	8	9	10	10	0.9	8	0.8
35	User 35	9	9	10	10	8	10	9	8	10	10	0.9	8	0.8
36	User 36	9	7	10	10	7	10	9	9	10	10	0.9	9	0.9
37	User 37	9	7	9	10	8	9	9	8	9	10	0.9	9	0.9
38	User 38	9	7	10	10	9	9	9	8	9	10	0.9	9	0.9
39	User 39	9	7	10	10	8	9	8	8	9	10	0.9	8	0.8
40	User 40	9	7	10	10	9	10	8	8	10	10	0.9	9	0.9
41	User 41	10	7	10	10	9	9	7	7	9	10	0.9	8	0.8
42	User 42	9	7	9	10	7	7	7	7	7	10	0.8	7	0.7
43	User 43	9	7	9	10	7	7	7	7	7	10	0.8	7	0.7
44	User 44	9	7	9	10	8	9	8	8	9	10	0.9	8	0.8
45	User 45	9	7	10	10	8	9	8	8	9	10	0.9	8	0.8
46	User 46	9	7	10	10	9	10	9	9	9	10	0.9	8	0.8
47	User 47	9	7	8	10	8	9	8	8	9	10	0.9	8	0.8
48	User 48	9	7	7	10	7	7	8	7	7	10	0.8	10	1.0