**Zero-Knowledge Credibility Proof Protocol (ZKC2P)**

We propose to use the **identity management service** (IdM) to help TMS in measuring the credibility of a consumer’s feedback. however , processing the IdM information can breach the privacy users.

Thus, we propose a Zero –Knowledge Credibility Proof Protocol(ZKC2P) to allow TMS, to process IdM’s information(credentials) using the Multi-Identity Recognition factors.

In other words, TMS will prove the user’s credentials. TMS processes credentials without including the sensitive information.

**IDENTITY MANAGEMENT SERVICES:**

When users attempt to use TMS for the first time, TMS requires them to register their credentials at the trust identity registry in IdM to establish their identities. The trust

identity registry stores an identity record represented by a tuple I=(C,Ca,Ti) for each user.

* C is the user's primary identity (e.g., user name). Ca represents a set of credentials’ attributes (e.g., passwords, postal address, and IP address) and Ti represents the user's registration time in TMS.

**TRUST MANAGEMENT SERVICES**:

In a reputation-based TMS, a user either gives feedback regarding the trustworthiness of a particular cloud service or requests the trust assessment of the service.

**Tr(s)=∑F(c,s)∗Cr(c,s,t0,t)\*(χ\*Ct(s,t0,t))/|V(S)|**

WHERE,

* V(s) = trust feedbacks given to cloud services.
* |V(s)| represents the total number of trust feedbacks.
* F(c,s) are trust feedbacks from the c th user.
* F(c,s) is held in the invocation history record h .
* Ct(s,t0,t) is the rate of trust result changes in a period of time..

χ is the normalized weight factor for the rate of changes of trust results which

* increase the adaptability of the model.

**Cr(c,s,t0,t) is calculated as follows:**

**Cr(c,s,t0,t)=1/λ\*(ρ\*D(s)+ϕ\*Of(s,t0,t)+Ω\*Mid(c)+ι\*Oi(s,t0,t))**

WHERE,

* ρ and D(s) denote the Feedback Density factor's normalized weight and the factor's value respectively.
* ϕ and Of(s,t0,t) denote the parameter of the occasional feedback collusion factor and the factor's value respectively.
* Ω denotes the Multi-identity Recognition normalized weight and Mid(c) denotes the factor's value.
* ι denotes the occasional Sybil attacks’ normalized weight.
* Oi (s,t0,t) denotes the factor's value.
* λ represents the number of factors used to calculate Cr(c,s,t0,t).

If only feedback density is considered, λ will be 1. If all credibility factors are considered, λ will be 4.

**Assumptions and attack Models**

We also assume that TMS communications are secure because securing communication is not the focus of this paper.

Attacks such as Man-in-the-Middle (MITM) is therefore beyond the scope of this work,

We consider the following types of attacks:

**Collusion Attack :**

This type of attacks occurs when several users collaborate together to increase or to decrease the trust result of cloud services.

**Sybil Attack:**

This type of attacks occurs when malicious users exploit multiple identities to give numerous misleading feedbacks for a self-promoting or slandering attack.