An Efficient Privacy-Preserving Credit Score System Based on Non interactive Zero-Knowledge Proof

ABSTRACT

Credit system is generally associated with the banking and financial institutions, although it has far reaching implications for residents of countries, such as U.S., particularly for those with a poor credit history. Specifically, a credit score computation (CSC) quantifies an individual’s credit value or credit risk, which is used by banking and financial institutions, as well as other entities (e.g., during purchasing of insurance policies and application of rental properties), to facilitate their decision-making (e.g., whether to approve the insurance policy purchase or the level of premium). Although a number of CSC models have been proposed in the literature for supporting different application scenarios, privacy protection of CSC is rarely considered despite the potential for leakage of user private information (e.g., registration, hobbies, credit, relationships, and inquiry). Such information can then be abused for other nefarious activities, such as identity theft and credit card fraud. Thus, in this article, we first analyze the privacy strength of existing CSC models, prior to presenting the formal definition of a privacy-preserving CSC system alongside its security requirements. Then, we propose a concrete construction based

on Paillier encryption with three proposed non interactive zero knowledge schemes. To demonstrate feasibility of our proposal, we evaluate both its security and performance.

**EXISTING SYSTEM**

* Non-interactive zero-knowledge proofs and non-interactive witness-indistinguishable proofs have played a significant role in the theory of cryptography. However, lack of efficiency has prevented them from being used in practice. One of the roots of this inefficiency is that non-interactive zero-knowledge proofs have been constructed for general NP-complete languages such as Circuit Satisfiability, causing an expensive blowup in the size of the statement when reducing it to a circuit.
* The contribution of this paper is a general methodology for constructing very simple and efficient non-interactive zero-knowledge proofs and non-interactive witness-indistinguishable proofs that work directly for groups with a bilinear map, without needing a reduction to Circuit Satisfiability. Groups with bilinear maps have enjoyed tremendous success in the field of cryptography in recent years and have been used to construct a plethora of protocols.
* An existing system provides non-interactive witness- indistinguishable proofs and non-interactive zero-knowledge proofs that can be used in connection with these protocols. An existing system is to spread the use of non-interactive cryptographic proofs from mainly theoretical purposes to the large class of practical cryptographic protocols based on bilinear groups.

Disadvantages

1) .The system doesn’t have more security on Credit score computation.

2). There is no trusted authority to trust credit data and finalize the credit scores.

**PROPOSED SYSTEM**

* In this article, we model a PCSC system designed to support the credit system. Unlike prior works that consider the design of risk models, we focus on its privacy protection instead. Specifically, our main contributions are summarized as follows.
* The system proposes the first formal description of a PCSC system alongside its security goals (i.e., weight confidentiality and credit confidentiality). This definition can be used in CSC, as well as other computations, such as digital asset settlement.
* The system introduces a concrete construction of PCSC, where the CSC is based on the weight. In the construction, we use Paillier encryption to hide the credit data and weights, and design three NIZK schemes to prove the validity of three statements mentioned earlier.

**Advantages**

1. . The system has developed with privacy-preserving CSC (PCSC) system tp give more security in credit card transactions.
2. . An efficient model to analyze credit score and credit card transactions from large data sets.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 7 Ultimate.
* **Coding Language :** Python.
* **Front-End :** Python.
* **Back-End :** Django-ORM
* **Designing :** Html, css, javascript.
* **Data Base :** MySQL (WAMP Server).