OFFLINE HANDWRITTEN CHARACTER RECOGINITION SYSTEM

ABSTRACT:

A fair contract-signing protocol allows two potentially mistrusted parities to exchange their commitments (i.e., digital signatures) to an agreed contract over the Internet in a fair way, so that either each of them obtains the other's signature, or neither party does. Based on the RSA signature scheme, a new digital contract signing protocol is proposed in this paper. Like the existing RSA-based solutions for the same problem, our protocol is not only fair, but also optimistic, since the trusted third party is involved only in the situations where one party is cheating or the communication channel is interrupted. Furthermore, the proposed protocol satisfies a new property abuse-freeness. That is, if the protocol is executed unsuccessfully, none of the two parties can show the validity of intermediate results to others. Technical details are provided to analyze the security and performance of the proposed protocol. In summary, we present the first abuse-free fair contract signing protocol based on the RSA signature, and show that it is both secure and efficient.

EXISTING SYSTEM:

As electronic commerce is becoming more and more important and popular in the world, it is desirable to have a mechanism that allows two parties to sign a digital contract via the Internet. However, the problem of contract signing becomes difficult in Existing setting the simultaneity has to be mimicked in order to design a digital contract-signing protocol. According to the involvement degree of a trusted third party (TTP), contract-signing protocols can be divided into three types:

1) Gradual exchanges without any TTP;
2) Protocols with an on-line TTP; and
3) Protocols with an off-line TTP.

In existing, such protocols are inefficient because the costs of computation and communication are extensive.

DRAWBACKS OF EXISTING SYSTEM:-

- The disadvantages are contract-signing protocols with an on-line TTP could be designed more easily since the TTP facilitates the execution of each exchange, but may be still expensive and inefficient because the TTP needs to be paid and must be part of every execution (though maybe not involved in each step).
- In practice, the on-line TTP is prone to become a bottleneck in the whole system, especially in the situation where many users rely on a single TTP. Cheating may occurs between two parties.

PROPOSED SYSTEM:-

In this paper, based on the standard RSA signature scheme, proposed a new digital contract-signing protocol that allows potentially mistrusted parties to exchange their digital signatures on a contract in an efficient and secure way. Furthermore, different from all previous RSA-based contract-signing protocol, the proposed protocol is further *abuse-free*. The reason is that we integrate an interactive zero-knowledge protocol, proposed for confirming RSA undeniable signatures into our scheme to prove the validity of the intermediate results. Moreover, we exploit trapdoor commitment schemes to enhance this zero-knowledge protocol so that the abuse-freeness property can be fully achieved.

ADVANTAGES OF PROPOSED SYSTEM:-

- The advantages are two parties get or do not get the other's digital signature simultaneously, and the TTP is only needed in abnormal cases that occur occasionally.
- To settle potential disputes between users, the TTP is not required to maintain a database to searching or remembering the state information for each protocol instance, so the overhead on the side of the TTP is reduced greatly, compared with the previous schemes.
- Like the existing RSA-based solutions, the new protocol is fair and optimistic.

SYSTEM SPECIFICATION:-

HARDWARE REQUIREMENTS:

- Hard disk : 40 GB
- RAM : 512mb
- Processor : Pentium IV
- Monitor : 17''Color Monitor

SOFTWARE REQUIREMENTS:

- Front End : Java
- Operating System : Windows XP.
- Back End : SQL SERVER 2005