

Ecommerce Data Vault

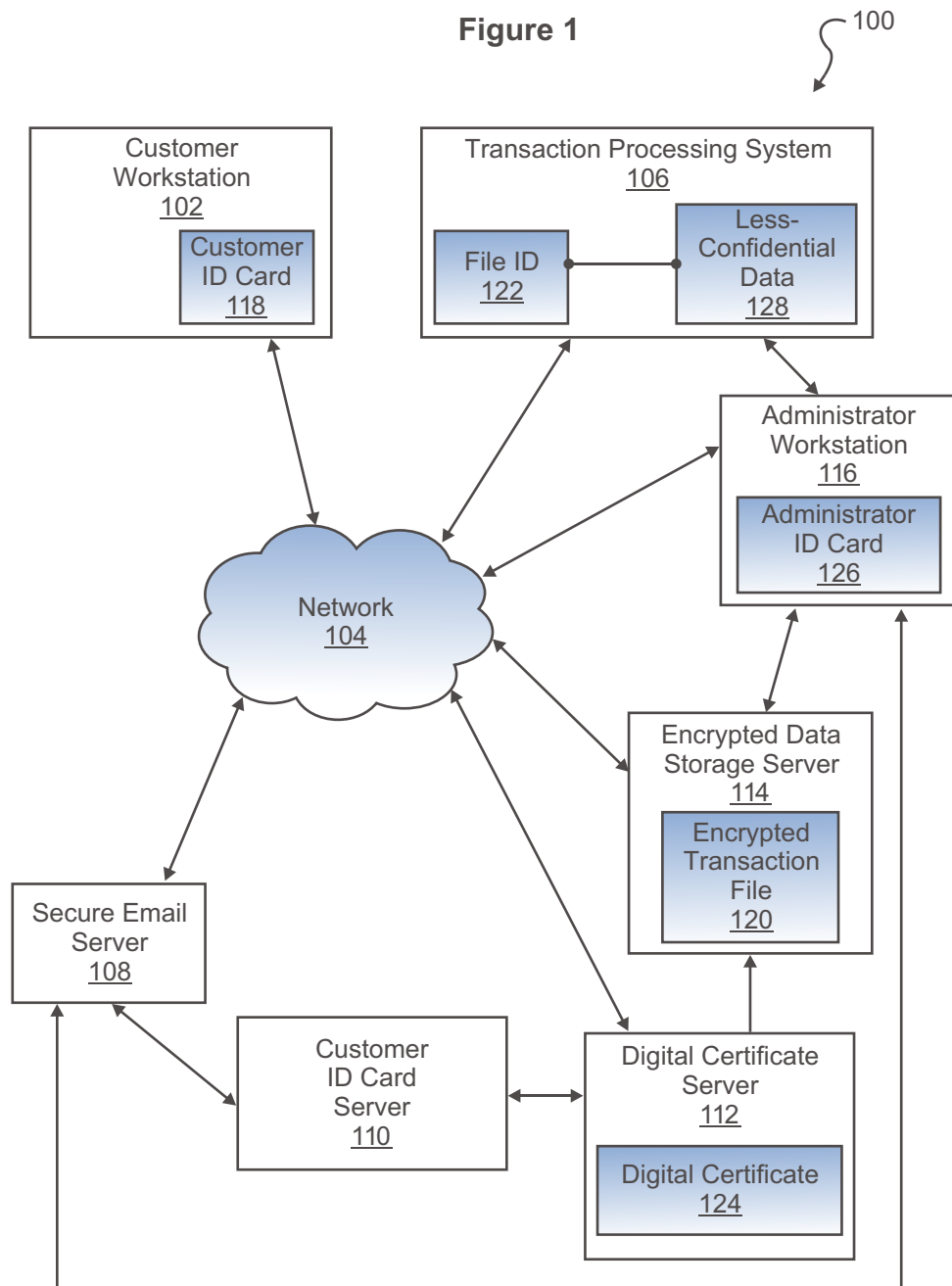


It seems as though every week we hear about a major theft of consumer information from a corporate or government computer network. In the last four years, approximately 250 million records containing personal identifying information of United States residents stored in government and corporate databases was either lost or stolen. Since little attention was given to database breaches prior to 2005, it is safe to assume that every man, woman and child has had their personal information exposed at least once statistically. In fact, many citizens have received multiple notification letters informing them that their personal information has been placed in jeopardy. One of the most recent stories in the news reported that a computer hacker stole thousands of credit card numbers from two U.S. grocery store chains resulting in nearly 2,000 cases of credit card fraud. Personal information, credit card and debit card numbers, corporate data - all this information is under constant threat by aggressive, highly motivated cyber criminals bent on breaking and exploiting any network weakness they can find. Businesses seeking to protect their sensitive systems and data must be just as aggressive as the hackers and solidify their approach to network security practices, systems and management. Confidential data stored on mass storage devices is at risk to be disclosed to persons getting physical or administrator access to the device. Just about any network, no matter how well protected, can be breached if hackers invest enough time and effort (and money) to break in.

The key to a successful security strategy is to make your systems so time-consuming and difficult to break, with no weak points and fresh layers of protection added consistently, that the hackers conclude it's not worth their time and search for easier targets.

We have presented the components of the present system in **Figure 1**.

Figure 1



Ecommerce Data Vault provides a way to encrypt each data file belonging to the consumer as a separate capsule. The file is encrypted using the consumer's digital certificate and assigned a unique alphanumeric I.D to each data file. The Alpha numeric ID is also linked to the digital certificate of the consumer. The encrypted file is stored in the Ecommerce Data Vault while the indexing attributes along with the Unique file ID are stored in a searchable index database. This approach helps in creation of Ecommerce Data Vault that could store critical consumer information that can be extracted during an Ecommerce transaction and stored in a shared place for entire enterprise and can be accessed by an administrator or staff only if the administrator or staff has access to the unique alphanumeric ID that is linked to digital certificate and can allow decryption of the Ecommerce data and have access to the searchable index database. This approach restricts even the administrator or staff to decrypt only one data file at a time and an outsider will have a lot difficult time getting hold of data as they will have to have a digital certificate issued to them and even after that they get only one transaction record.