说明书附图

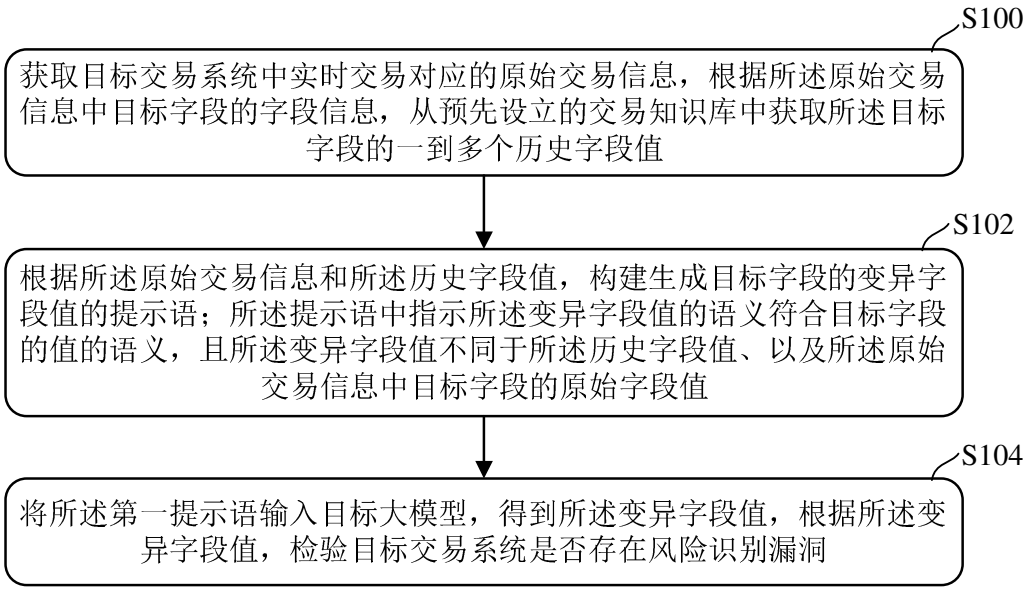
S100
获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值
S102
根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值
S104
将所述第一提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞

图 1

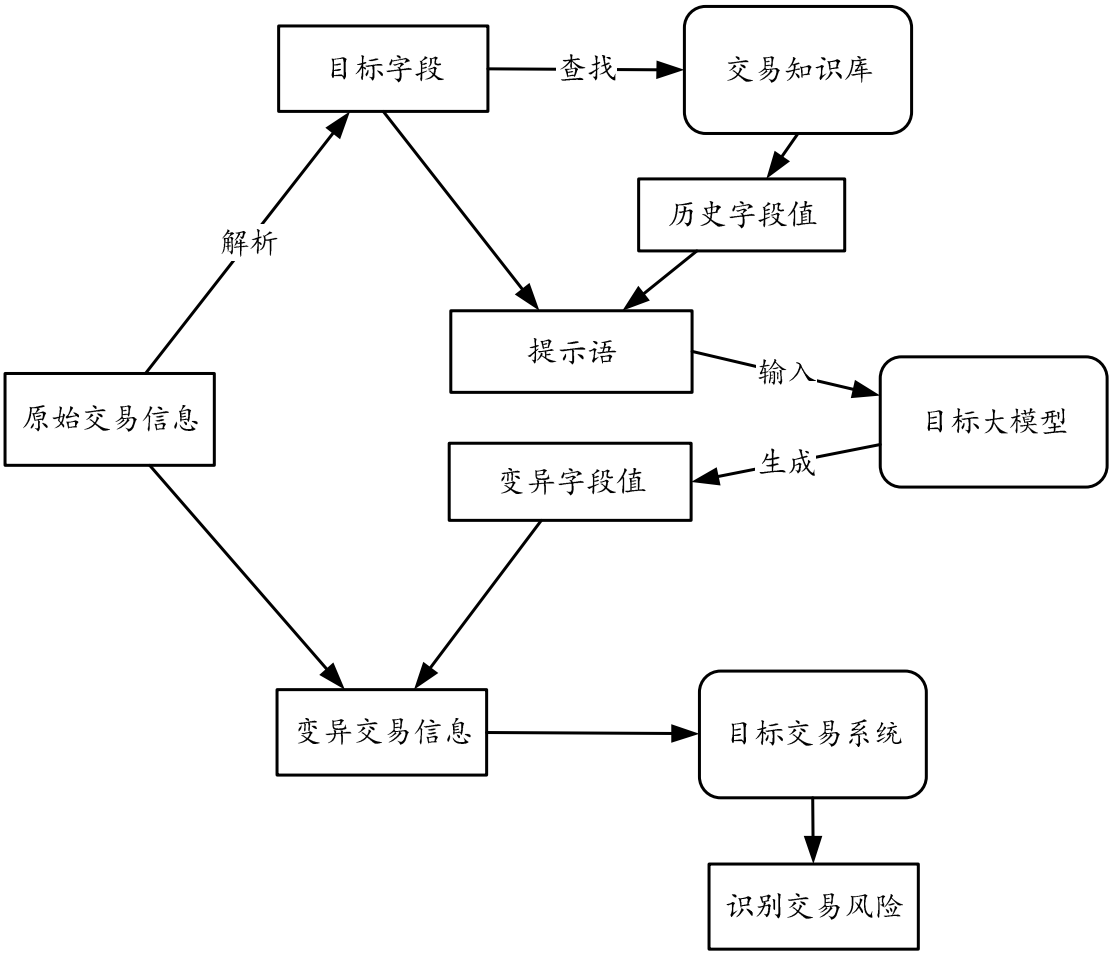

图 2

键	值
字段信息特征1(字段名称)	历史交易1
字段信息特征2	历史交易2
字段信息特征3	历史交易3
...	...

图 3

5

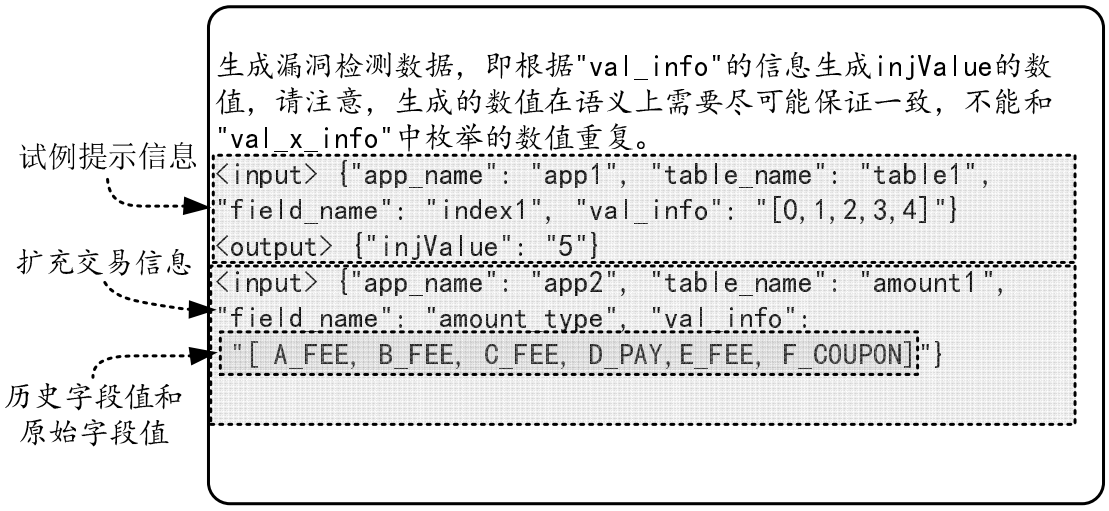
生成漏洞检测数据，即根据"val_info"的信息生成injValue的数值，请注意，生成的数值在语义上需要尽可能保证一致，不能和"val_x_info"中枚举的数值重复。
试例提示信息
<input> {"app_name": "app1", "table_name": "table1", "field_name": "index1", "val_info": "[0,1,2,3,4]"}
<output> {"injValue": "5"}
扩充交易信息
<input> {"app_name": "app2", "table_name": "amount1", "field_name": "amount_type", "val_info":
"[A_FEE, B_FEE, C_FEE, D_PAY,E_FEE, F_COUPON]"}
历史字段值和原始字段值

图 4

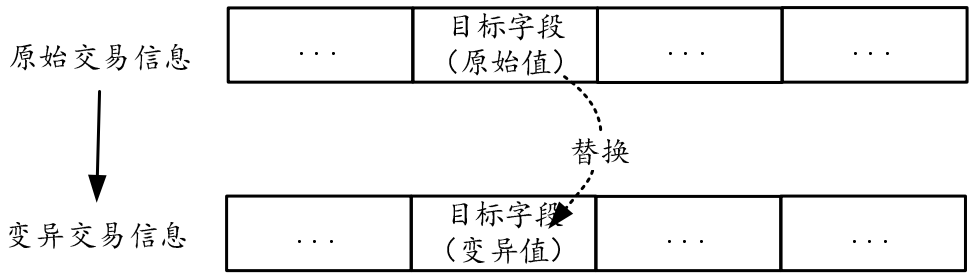
原始交易信息
...
目标字段（原始值）
...
...
替换
变异交易信息
...
目标字段（变异值）
...
...

图 5

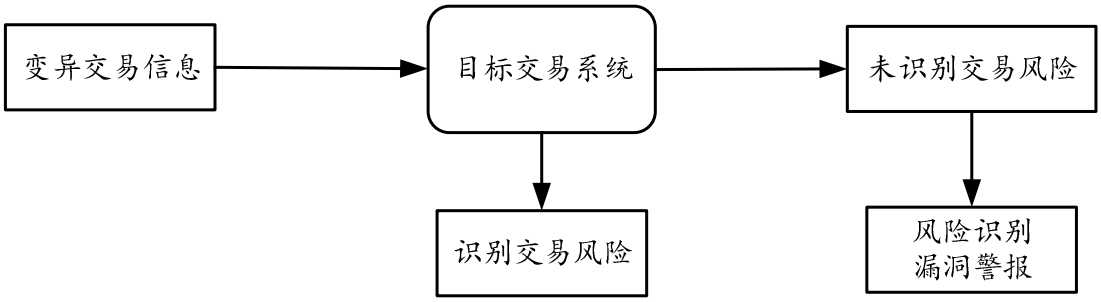
变异交易信息
目标交易系统
未识别交易风险
识别交易风险
风险识别漏洞警报

图 6

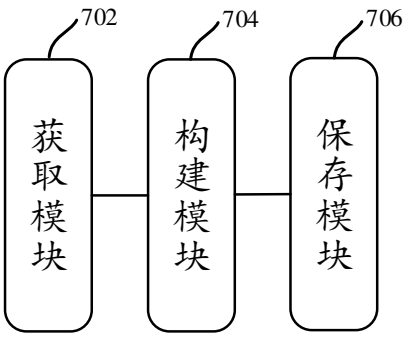
702
704
706
获取模块
构建模块
保存模块

图 7

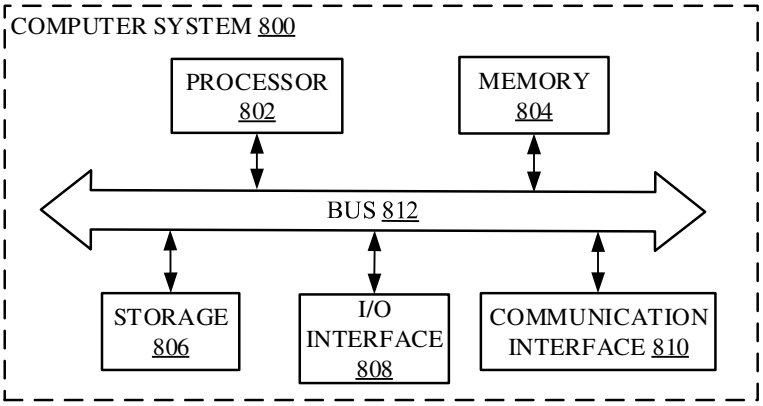
COMPUTER SYSTEM 800
PROCESSOR 802
MEMORY 804
BUS 812
STORAGE 806
I/O INTERFACE 808
COMMUNICATION INTERFACE 810

图 8