Cloud computing

Théo Demessance 621 2
Hugo Prevoteau 21 3
Christophe Haikal 9 084
Valentin Tassel 6219000085

Interest for security in cloud

- Cloud storage becomes more and more used and most of the organizations now use cloud based applications

- So there is a need to provide a robust and safe solution to authenticate the operations made on such an application.

Two main ways to answer this question

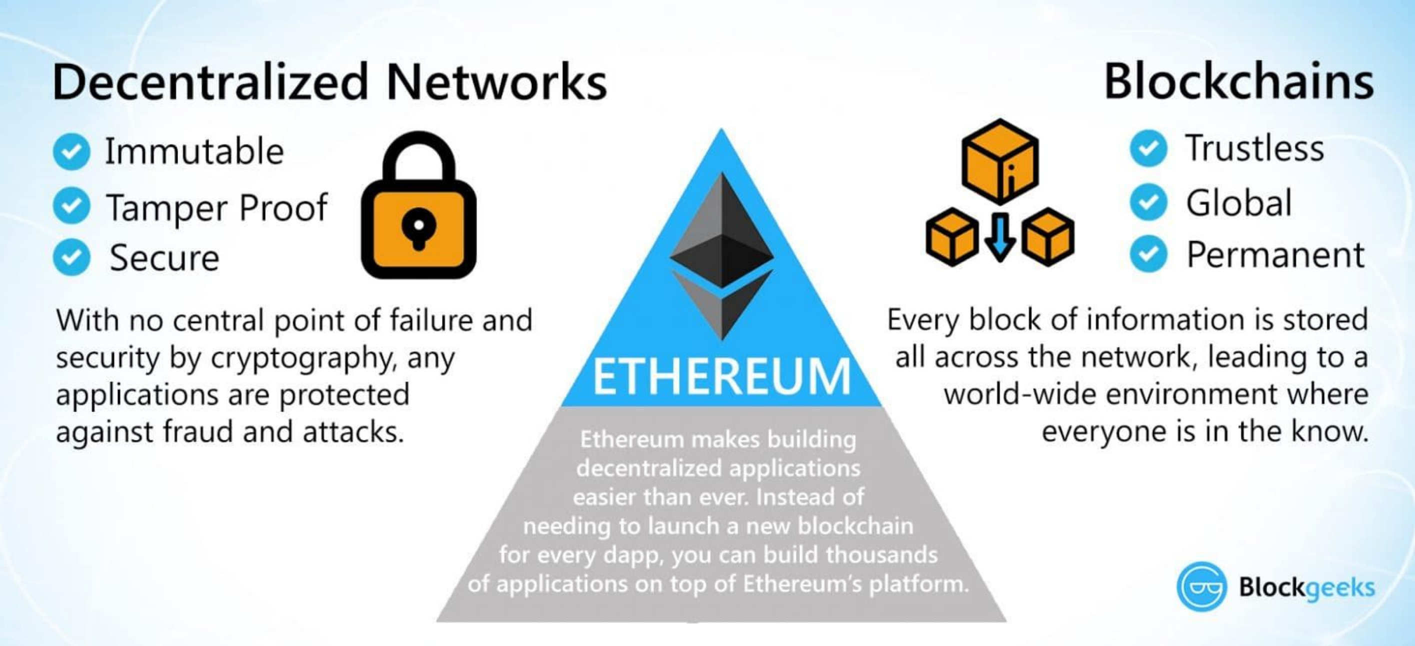
- Authenticate the user when he connects to the database, using **blockchain**

- Analysing the data traffic using **machine learning**

Using blockchain

- nowadays data is stored on the cloud server in the form of ciphertext
- To access data that are stored the user need an access key distributed by a third party, the the third party can be dishonest, the security of the system will be threatened.
- Instead of using a third party they use Ethereum.

What is Ethereum ?



Decentralized Networks

- ✓ Immutable
- ✓ Tamper Proof
- ✓ Secure

With no central point of failure and security by cryptography, any applications are protected against fraud and attacks.

ETHEREUM

Ethereum makes building decentralized applications easier than ever. Instead of needing to launch a new blockchain for every dapp, you can build thousands of applications on top of Ethereum's platform.

Blockchains

- ✓ Trustless
- ✓ Global
- ✓ Permanent

Every block of information is stored all across the network, leading to a world-wide environment where everyone is in the know.

Protocol

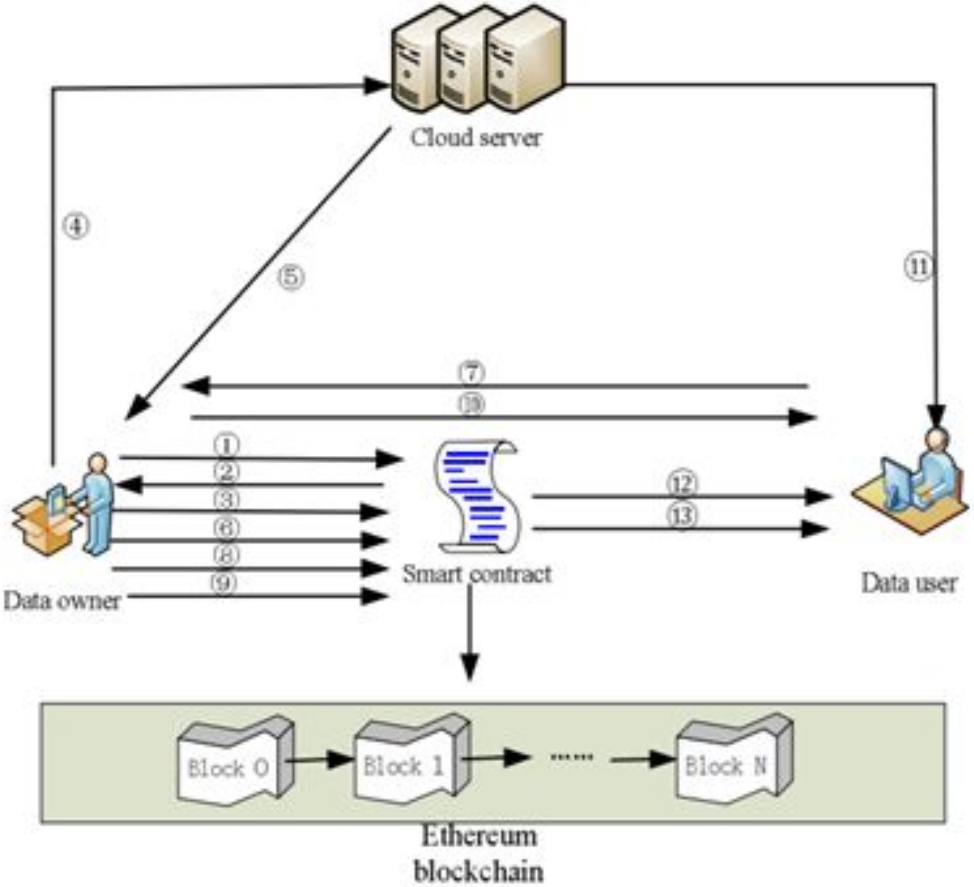


FIGURE 2. System Model

Protocol-System implementation

①The smart contract is deployed by the Data Owner in Ethereum

②After the smart contract is deployed successfully, the contract address is returned.

③ Data Owner stores the file in the smart contract.

④Data Owner package the contract address , file ID ,

and encrypted file and then upload to the cloud server.

⑤ Data Owner records file path returned by cloud server.

⑥ Data Owner stores the ciphertext of the encrypted document key in the Ethereum.

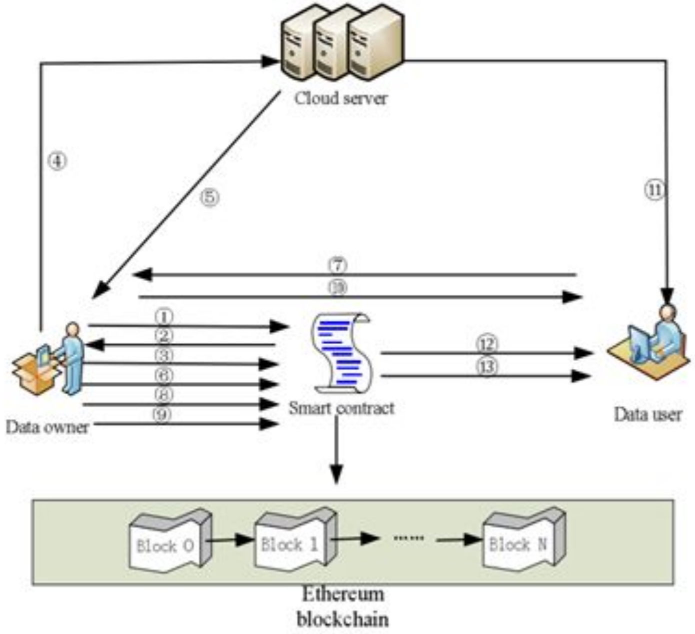


FIGURE 2. System Model

Protocol-An access request

⑦ Data User sends an access request to Data Owner.

⑧ Data Owner adds the effective period to Data User and stores it in the smart contract .

⑨ Data Owner encrypts the secret key of Data User and stores it in the smart contract .

⑩ Data Owner sends the contract address with user information through a secure channe

⑪ Data User downloads encrypted file from the cloud server.

⑫ Data User obtains effective period from the smart contract.

⑬ Data User obtains his secret key ciphertext from the smart contract.

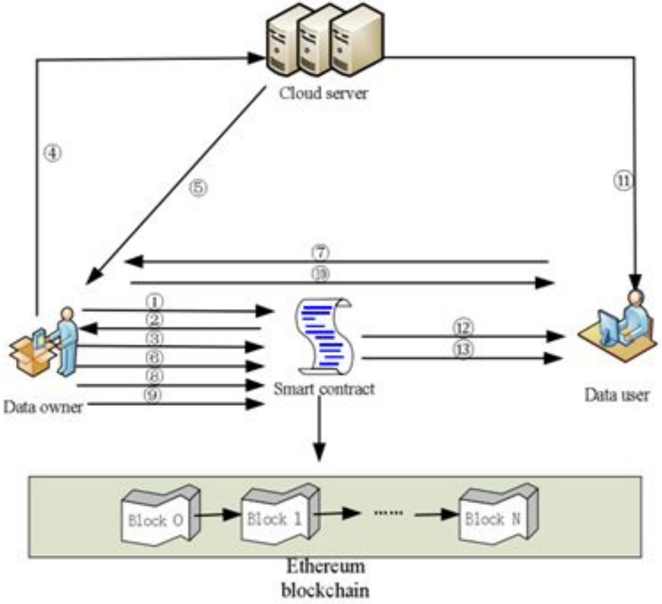


FIGURE 2. System Model

Conclusion

ethereum

Using machine learning

- Robust enough to detect any form of anomalies
- Highly accurate when it’s well trained
- Easily adaptable to evolving changes
- Efficient with a large training dataset

The features

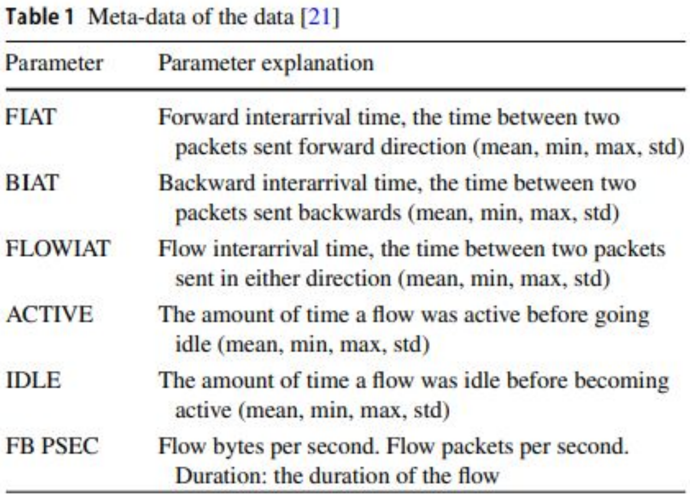


Table 1 Meta-data of the data [21]

Parameter	Parameter explanation
FIAT	Forward interarrival time, the time between two packets sent forward direction (mean, min, max, std)
BIAT	Backward interarrival time, the time between two packets sent backwards (mean, min, max, std)
FLOWIAT	Flow interarrival time, the time between two packets sent in either direction (mean, min, max, std)
ACTIVE	The amount of time a flow was active before going idle (mean, min, max, std)
IDLE	The amount of time a flow was idle before becoming active (mean, min, max, std)
FB PSEC	Flow bytes per second. Flow packets per second. Duration: the duration of the flow

Datasets

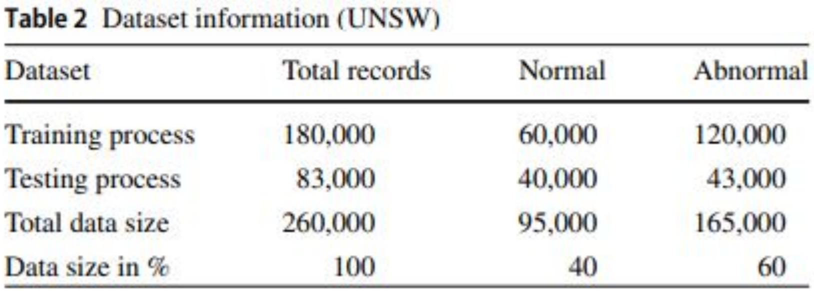


Table 2 Dataset information (UNSW)

Dataset	Total records	Normal	Abnormal
Training process	180,000	60,000	120,000
Testing process	83,000	40,000	43,000
Total data size	260,000	95,000	165,000
Data size in %	100	40	60

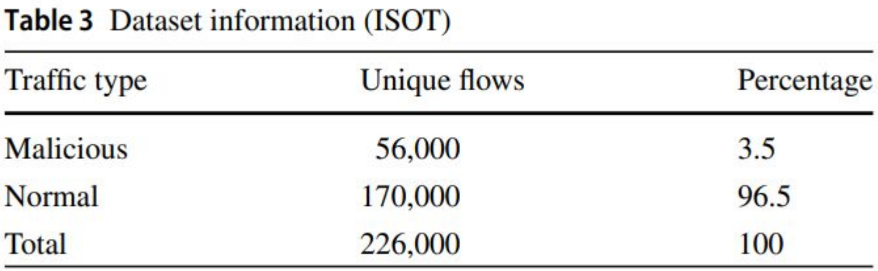


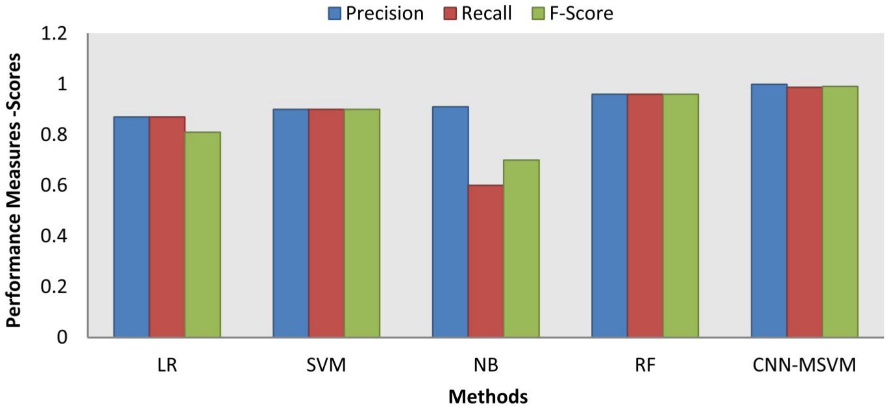
Table 3 Dataset information (ISOT)

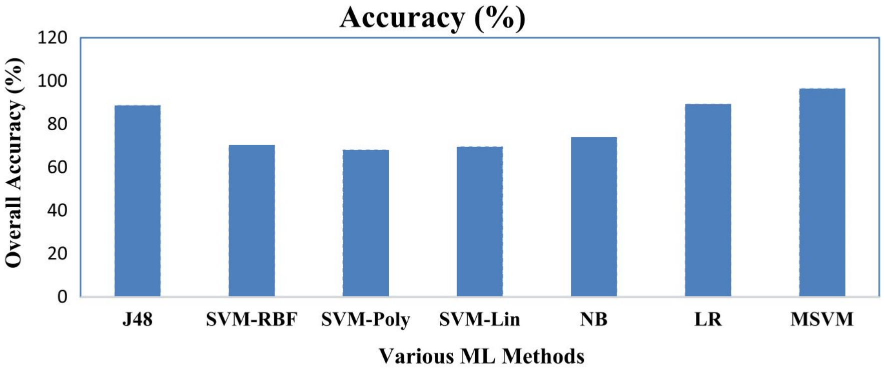
Traffic type	Unique flows	Percentage
Malicious	56,000	3.5
Normal	170,000	96.5
Total	226,000	100

Used Algorithms

- CNN with 5 layers to convert the data as vectors
- Identifying the classes with a multi SVM

Results


Precision
Recall
F-Score
Performance Measures -Scores
1.2
1
0.8
0.6
0.4
0.2
0
LR
SVM
NB
RF
CNN-MSVM
Methods


Accuracy (%)
Overall Accuracy (%)
120
100
80
60
40
20
0
J48
SVM-RBF
SVM-Poly
SVM-Lin
NB
LR
MSVM
Various ML Methods

Limits of the model

- Requires a lot of memory space
- Anomalies may occur while running the algorithm

EIDC Firewall scheme

- Detects and classifies the received traffic packets
- Most frequent decision technique
- The nodes past decisions are combined with the current decision of the ML algorithm
- Estimate the final attack category classification

Firewall scheme EIDC

- Improves the detection and the classification of malicious users

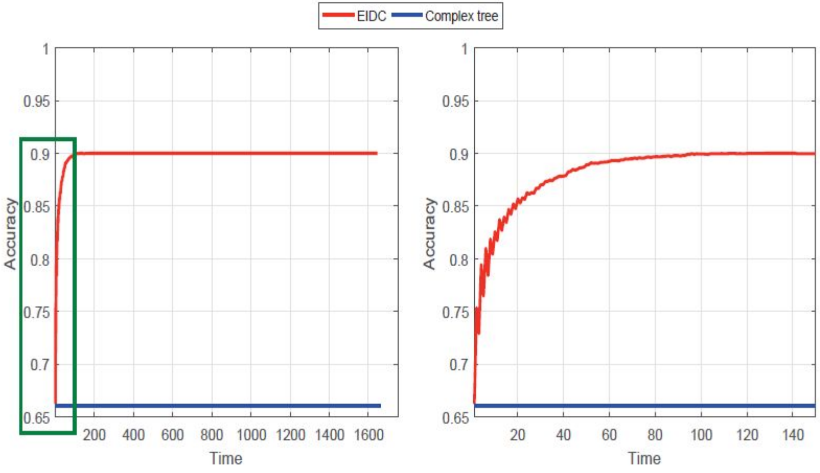


Fig. 4. The accuracy of the proposed model compared to complex tree as a function of time

Conclusion

- Extended supervised machine learning methods are highly suitable and applicable in real-time cloud applications.
- Efficiency is verified by experiment on various datasets

Papers

A focus on future cloud: machine learning-based cloud security
E. K. Subramanian · Latha Tamilselvan
7 june 2019

A Secure Cloud Storage Framework with Access Control based on Blockchain
SHANGPING WANG , XU WANG , and YALING ZHANG
2019

A Combined Decision for Secure Cloud Computing based on Machine Learning and Past Information
Zina Chkirbene, Aiman Erbad and Ridha Hamila
2019

谢谢