CS6290 55323707 Reading Summary 4

Yu SU
Dept. of Computer Science
ID:55323707

I. Summary of Paper [1]

A. Problem statement

Nowadays, the trusted hardware systems, such as SGX are more and more popular in providing confidentiality and integrity of applications, but the cache attack, especially side-channel attack [2] seems giving users another concern. Side-channel attack is the malicious host could get lots of sensitive information through the memory access patterns with the physical side-channels. Therefore, the paper proposed a new cryptographic primitive based on transparent enclaves called Sealed-Glass proof, which could make the trsted hardware systems support trustworthy application even in the presence of the side channel.

B. Problem Significance

This paper is very meaningful. To defend the attack, most approaches are to limit the operation using long term secrets, because the total security is threatened by the private key. What's worse, it is hard to avoid the side-channel attack in a arbitrary computation without degradation of performance and with trust. And the SGP just could solve these problem by using a transparent enclaves and also proved it. Besides the theory, the paper also implemented the protocol to prove that works in practice.

C. State of the Art

Before the paper, the isolated execution environments rely on the confidentiality to protect data and code form the cloud and the paper fist proposed to forgo the enclaves confidentiality to protect the systems.

What's more, the zero knowledge proof is an active field in the cryptography community, but the limitation is they always require code in some specialized circuit representation which will restrict the function of the bug-bounty. And the paper proposed a kind of SGX-based bug bounty platform to simplify the setup.

D. Contributions

The paper try to prove the weaker model of trusted hardware useful. The key sight is the transparent enclaves could guarantee uni-directional resource asymmetry. And the paper also show it can be secure, powerful and general functional. What's more, the paper proposed SGPs for fair exchange of a secret for a monetary and combine it with smart contract to overcome its some limitation. Overall, there are three main contributions in the paper.

First, the paper introduced a novel notion of transparent enclave execution, which could capture the unbounded leakage of application data and thus arbitrarily powerful side-channel attacks. What's more, to make the system could fit more application in a efficient secure way, they formalize slight relaxation of the model. In detail, there are two relaxations. One is convert-channel resistance, which means a convert channel is a means for the host to pass data to a maliciously crafted enclave program. The other one is securing crptographic keys, which often used in efficiently setting up an authenticated channel to a remote party.

Second, the paper proposed the Sealed-Glass Proof, which is a primitive realizable with transparent enclaves. What's more, the proof encompassed and generalized the verifiable computing, commitment schemes and the zero knowledge proof. In the verifiable computing scheme, one sends the input to another and they will get a verification if the computation is correctly. And under the zero knowledge protection, the input could be confidential.

Last contribution is the paper proposed a protocol based on the SGPs and smart contracts and implemented it on the github. The protocol realizes knowledge marketplaces with strong fairness guarantee. What's more, the paper extend it for implementation on the ethereum. And there are also three example of bug bounties on its system. The first two correspond to exploits specified by a piece of data and the third one is a bug bounty for a general framework defined as code implementing a MITM attack.

E. Remaining Questions

Although the SGPs under the transparent enclaves works well, there still a lot of space to optimize the construction through the moderate relaxations or extensions to smart contract and trusted hardware platforms.

The other problem is the paper only focus on the security problem. For the performance, stability and scalability, there is no data analysis on it to prove the system is really as good as it said. However, the largest problem for the most research about blockchian is not the security problem. The largest problem is about performance, so I think maybe in the future, there need more experiment on the system.

II. Summary of Paper [3]

A. Problem Statement

The cloud computing has developed for many years, while all of them are based on the centralization computing, which will cause many problems. For example, with the data increase, the centralization will be a bottleneck for the data transfer and with the device increase, it is harder for the distant device communicate under a centralized network. What's more, the centralization will cause the concern for unfair such as the AWS, which controls up to 40 percent of the could market, so it is possible for AWS do something not fair like enforcing censorship of specific users of the cloud by removing its censorship-resistance property. So it is essential for us to have an alternative decentralized computing infrastructure. The paper proposed a novel scheme that enables users with CPUs that support Trusted Execution Environments and remote attestation to rent out computing time on secure enclaves to untrusted users, which is called Airtnt.

B. Problem Significance

This paper is very meaningful, because there is much difference for the centralized computing infrastructure between the decentralized one. One of the challenge is it is hard to realize the trust and reputation environment in the decentralized system. Although we could rely on the trusted execution environment, there is still problem that they do not allow for exchange for the fair exchange of payment and result for two mutually distrusting parties. What's more, although the smart contract could be facilitated, the key challenge is to realize the large range of verification because the blockchain is related to the high transaction fees. So what the paper research on is very meaningful.

C. State of the Art

At that moment, there are two group of technique for the result verification. One focus on the constructing cryptographic proof of computation, which has the problem that the overhead of the pre-computation and creation of proof is too high. The other technique is based on multiple servers and the overhead is also increased with repeated computation.

And for the fairness, most of research focus on the incentivising fairness and timely delivery of the results using cryptocurrencies, which could be used with the micro-payment to reduce the cost and overhead of transactions.

And there are some attempts on the computation verification on the system, but they are limited in a specific type of task, such as the easy computation for the polynomial computations.

And there are also some attempts on the vision of the decentralized computer. However, the functions are all restricted and the result for the automatic verification is even worse.

D. Contributions

The paper proposed a protocol which has two function. One is allowing the requesters to execute tasks on node with TEE-enabled CPUs. Second is allow the executing node to receive payment without creating any trust connection. And applying smart contracts as the mediator for fair exchange and applying checkpoint micro payment to make computation constant. What's more, the paper use Game of Life and OCR to show the performance of the protocol. Specifically, there are four main contributions in the paper.

First, the paper proposed Airtnt, a fair exchange system, which realize the definite fair. The definite fair means not only the malicious user cannot make others lose money, even if they want to lose money is also forbidden. In detail, there are three parts in Airtnt. The requester send request to the executing node and it send back the result after computation. And the smart contract does the fair exchange job.

Second contribution is to realize the execution integrity, the paper proposed some protocols to make sure the execution will always be correct. The first two contributions are realized under the trusted execution environment.

Besides the fairness and integrity, the paper also realize the executing node counterparty risk resistance and execution transferability. They use the payment channels to realize a micropayment system. In detail, they use many state to lead the micro payment execute the computation and under this scheme, the computation can continue on a different executing node that the original node has gone offline.

Last, the paper also implement and evaluate one prototype to prove the practical works of their theory. In detail, for the implementation part, the paper implemented two types of applications, which have different properties. One is state-based programs, which is a simulation of the program that needs to remember intermediate state. The other is the pure program, which do not need to record the state. This type of program will be negligible in size compared to the state-based programs because of the discarding of the state. By comparing this two different application the paper got a better evaluation. The paper pointed out the advantage and disadvantage of the state-based programs and pure programs.

E. Remaining Questions

One of the problem is the dependency of the Airtnt. Although the Airtnt could solve many problems, at the same time, they are under a lot of restriction, such as SGX, smart contracts and the ethereum. Each of them has some problem will influence the performance and even the security of the protocol. For example, the cache attack for the SGX is effective to Airtnt or not. There is no optimization about this and also no prove. Therefore, the researchers still need to increase the scalability of the Airtnt to make it perform well in different environment. And there are also needs for more evaluation on it.

References

[1] T. Florian, Z. Fan, L. Huang, H. Jean, J. Ari, and S. Elaine, "Sealed-glass proofs: Using transparent enclaves to prove and sell knowledge."

[2] W. Jinwen, C. Yueqiang, L. Qi, and J. Yong, "Interface-based side channel attack against intel sgx."

[3] A.-B. Mustafa, S. Alberto, K. Michal, and P. Ioannis, "Airtnt: Fair exchange payment for outsourced secure enclave computations."