Next-generation cybersecurity through a blockchain-enabled federated cloud framework

Advanced in Blockchain Technology

Seoul National University of Science and Technology

CIS (Cryptography and Information Security) Lab.

2018-05-28

Seonghyeon Gong

Contents

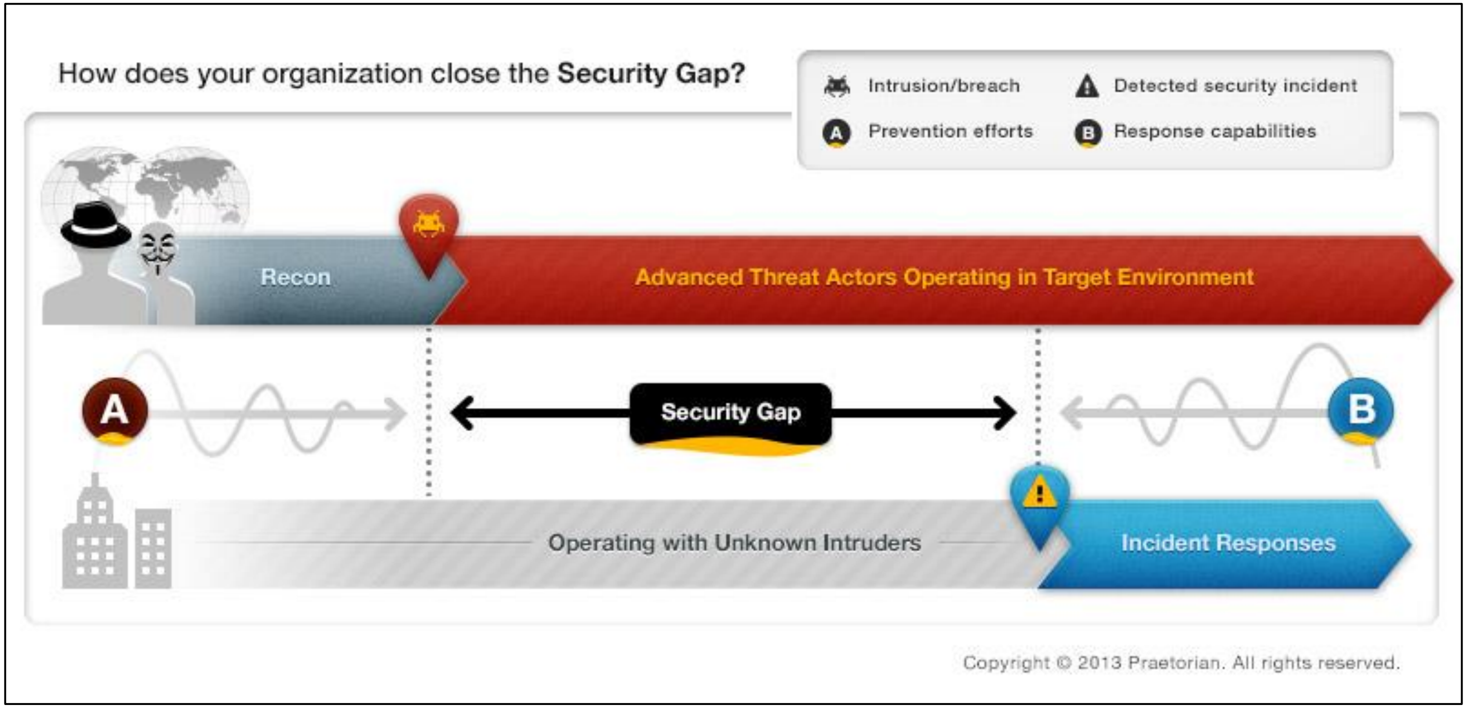
Introduction

Motivations – Breach Detection Gap

The risk and vulnerabilities are growing exponentially in Internet of Things (IoT) era.

There are different cybersecurity. solutions varying from antivirus to firewalls to IDS/IPS.

However, cyber-attacks are discovered daily, many of which have gone undetected for days and sometimes years before organizations detect and address attacks and raise concerns about breach detection gap (BDG).

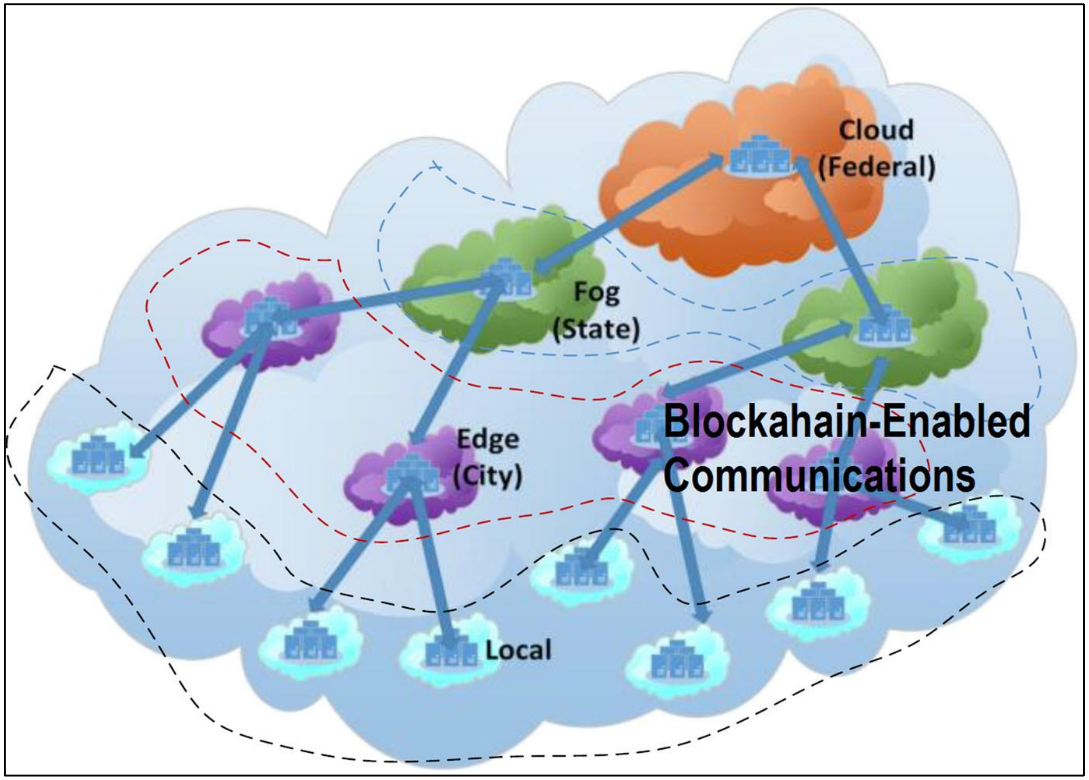


Introduction

Proposed Framework

Blockchain-enabled federated cloud computing (BFC^2) framework for next-generation cybersecurity to reduce data breaches and BDG.

The BFC^2 provides capabilities for promoting tighter security and restricted access control by using packet monitoring and traffic analysis.



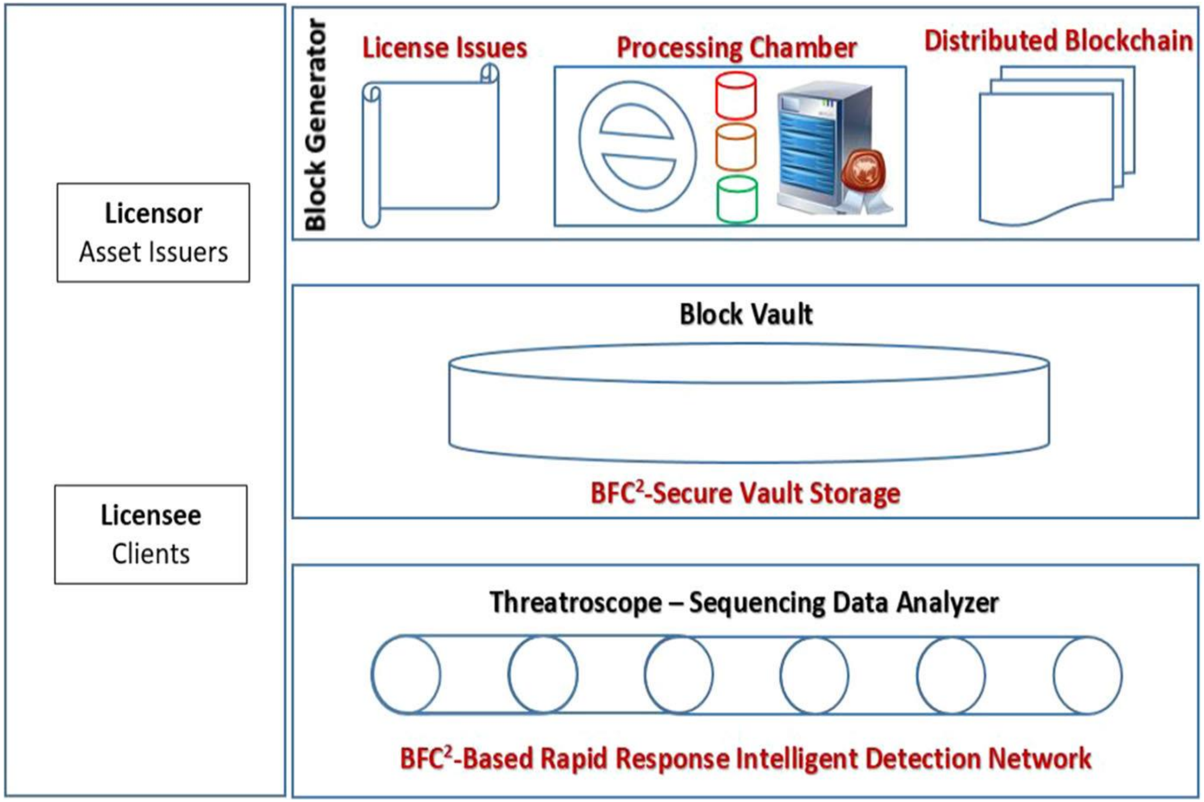
Proposed Framework

BFC^2 (Blockchain-enabled Federated Cloud Computing)

BFC^2 system model is permissioned blockchain (not permission-less public blockchain)

Three basic components of BFC^2

- Block generator - comprises of license issues, processing chamber, and distributed Blockchain
- Block vault - chained secure storage for transactions and blocks
- Threatroscope - designed for real-time network traffics monitoring and analysis of inbound and outbound traffics passing through participating organizations

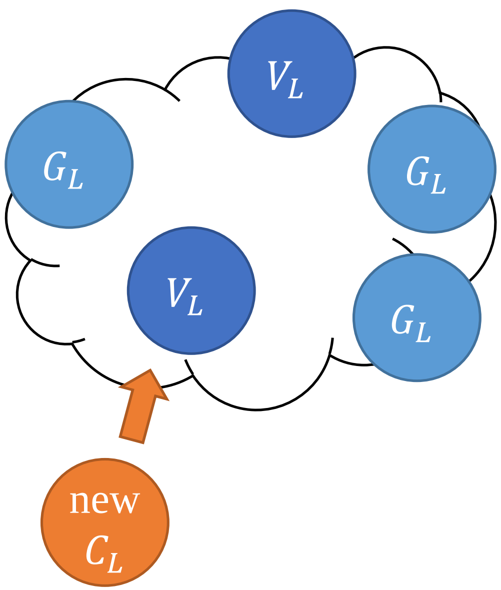


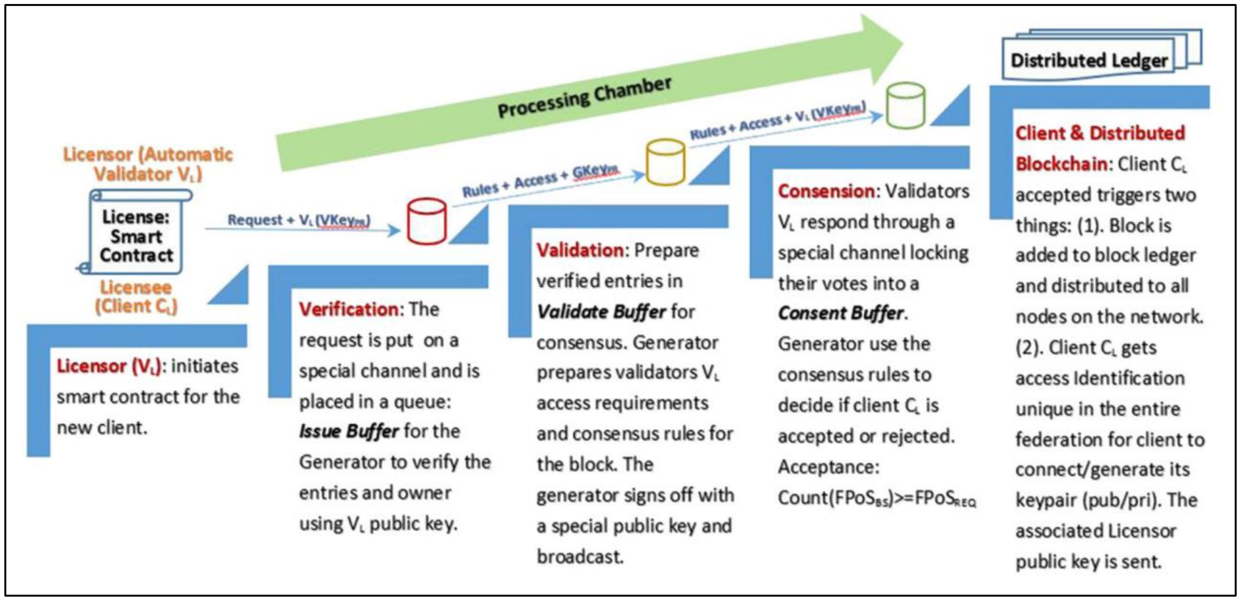
Proposed Framework

New client validation process of BFC^2 as a smart contract

Validator V_L, client C_L, block generator G_L

1. validator V_L raise new transaction request that is signed with its private key $VKey_{PR}$
2. signed requests are installed in $issue\ buffer$
3. block generator G_L verifies the owner of request using $VKey_{PUB}$
4. verified requests are installed in $validate\ buffer$
5. generators are signed that requests with their $GKEY_{PR}$ with timestamp, and store it into $consensus\ buffer$ for consensus
6. consent using Federated-Proof-of-Stake(FPoS)
7. other generators csheck the validity of consensus using $GKEY_{PUB}$





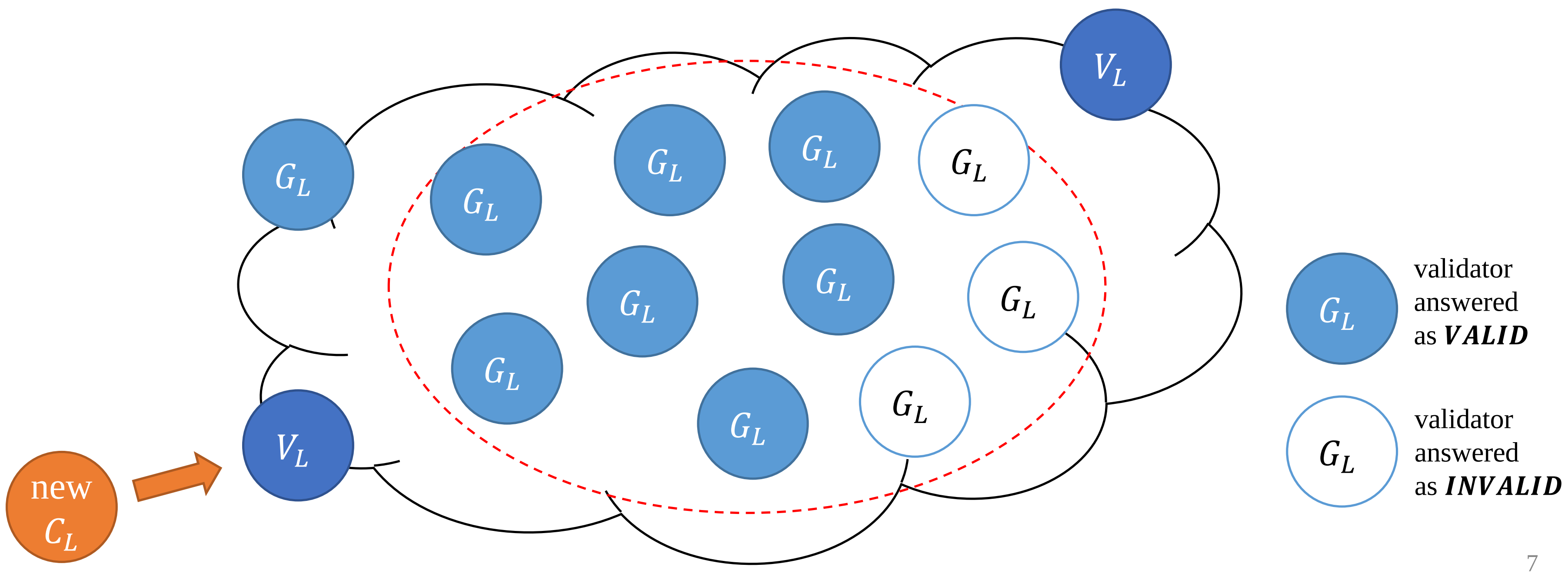
Proposed Framework

Federated-Proof-of-Stake (FPoS)

FPoS for consensus agreement is based on a threshold of number of Validators (Block Signers—BS) $FPoS_{BS}$ and the number of $FPoS_{BS}$ signatures that is required $FPoS_{REQ}$ to accept a block.

If $FPoS_{BS} \geq FPoS_{REQ}$, then that transaction becomes a blockchain ledger record.

1. Set $FPoS_{BS} = 10, FPoS_{REQ} = 7$
2. new client (new transaction raised)
3. select 10 validators from blockchain network randomly, and request validation to them
4. If the number of response as $VALID$ is bigger than or equal to 7, new transaction is stored in ledger
5. else, reject the transaction

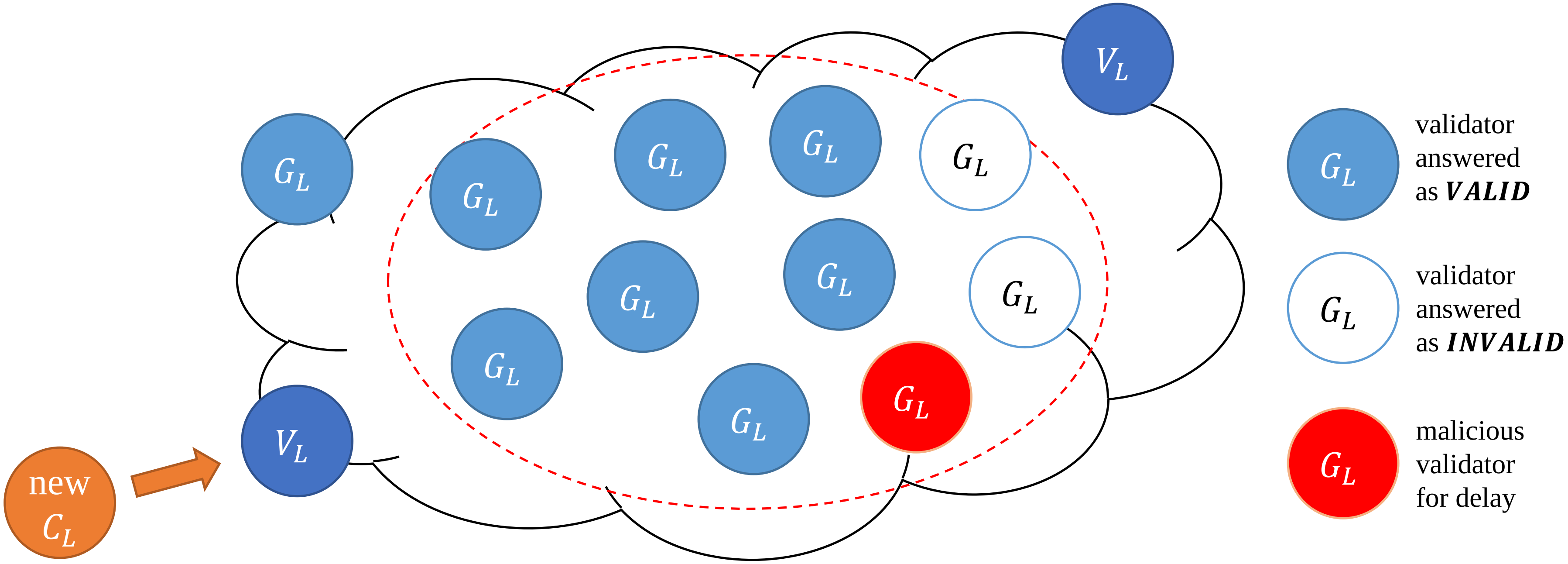


Proposed Framework

Attacks on FPoS

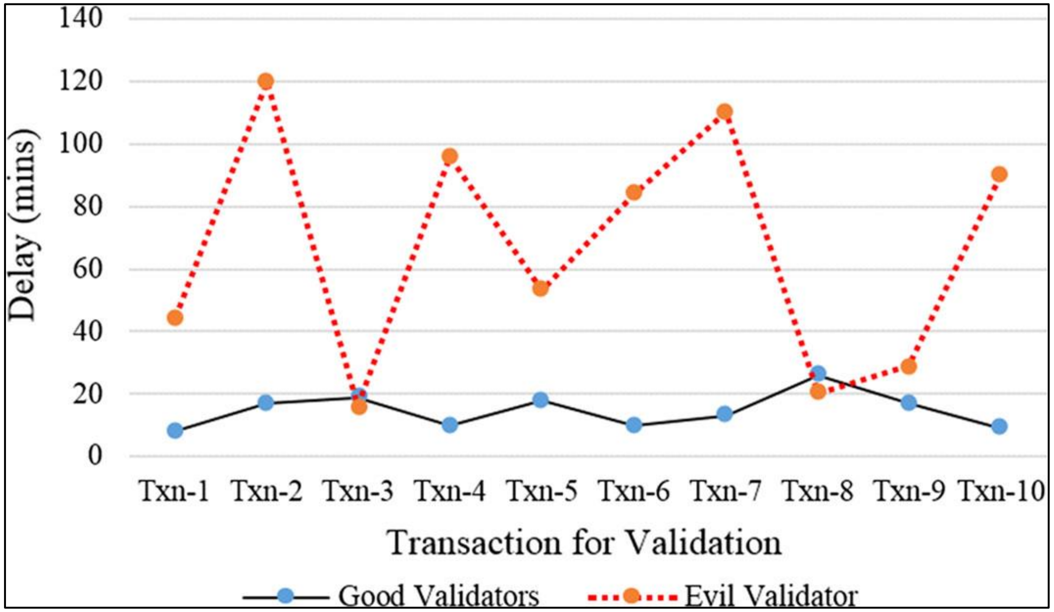
Sybil attack FPoS

- fake transaction – could be prevented systemically
- **delay** – malicious last response



Proposed Framework

Attacks on FPoS



	Txn-1	Txn-2	Txn-3	Txn-4	Txn-5	Txn-6	Txn-7	Txn-8	Txn-9	Txn-10
Good validator	**8**	**17**	**19**	**10**	**18**	**10**	**13**	**26**	**17**	**9**
Evil validator	**44**	**120**	**16**	**96**	**53**	**84**	**110**	**20**	**29**	**90**
Result	D-A	R	**P**	R	D-A	R	R	**P**	P	R

D-A: delated acceptance, R: reject, P: perfect

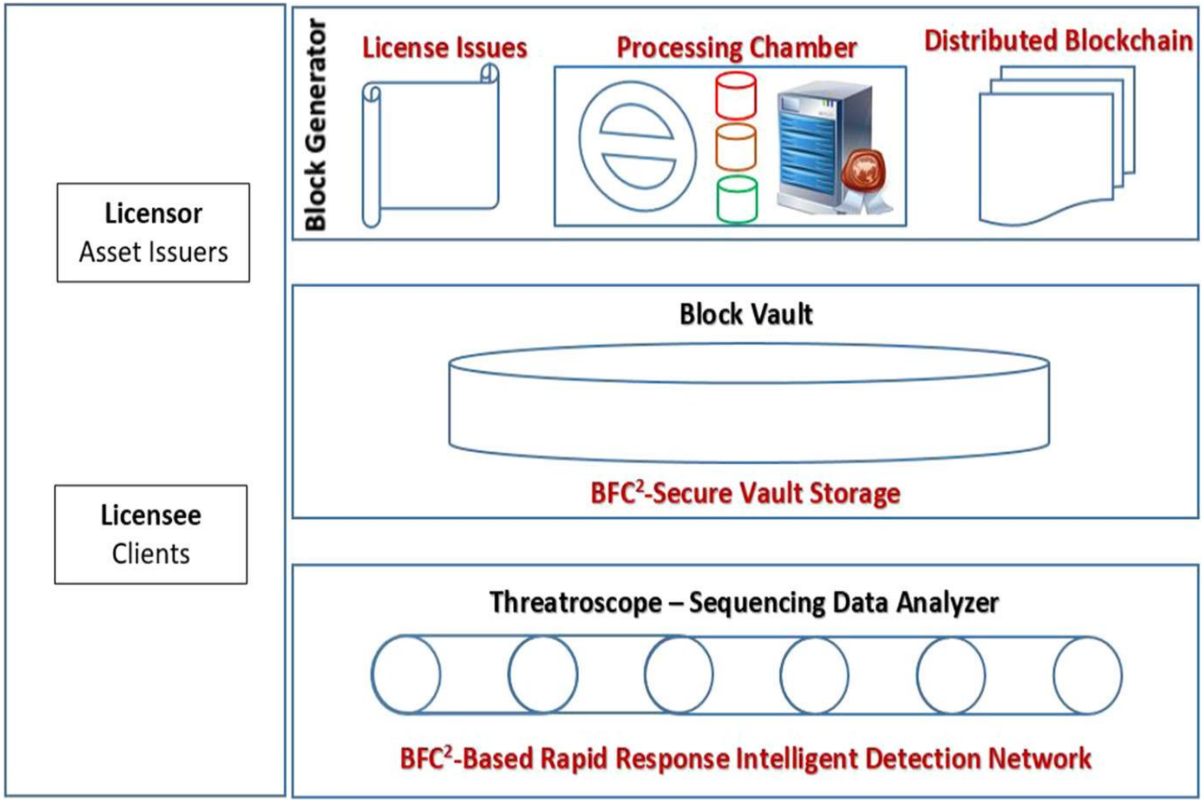
BFC^2 threatroscope and Dempster-Shafer

Threatroscope

Our system wants to bring real-life policing into technology.

A crime is resolved by bringing all the pieces of evidence together which could be from multiple sources including monitoring public surveillance cameras.

Threatroscope is designed for **continuous monitoring, coordination, cooperation and information sharing** among hubs at the edges, fogs and the federal clouds.



BFC^2 threatroscope and Dempster-Shafer

Integration of Dempster–Shafer with probability and threatroscope

Dempster–Shafer is the mathematical discipline for our threat detection as the theory potentially allows the combination of separate pieces of the network data packet (**evidence**) obtained from multiple hubs within the federated cloud and modeling them.

For example, email event in our model can have two discrete random variables X and Y.

- X represents "Riskware"
  - value of 0: genuine
  - value of 1: malicious email
- Y represents "Belief"
  - value of 0: no evidence
  - value of 1: there is evidence

Evidence (Y)	Belief–riskware (X)	
	Genuine (0)	Malicious (1)
No Evidence (0)	0.5	0.1
Evidence (1)	0.1	0.3

- $\sum_{x,y} P(X = x, Y = y) = 1$
- $P(X = 1, Y = 1) = 0.3$ ... Joint probability
- $P(X = x) = \sum_{y} P(X = x, Y = y)$ ... Marginal probability
- $P(X = 1|Y = 1) = P(X = 1, Y = 1)/P(Y = 1)$ ... Conditional probability.
- $P(X = 0|Y = 1) + P(X = 1|Y = 1) = \frac{0.1}{0.4} + \frac{0.3}{0.4} = 1$ ... Nomalization

BFC2 threatroscope and Dempster-Shafer

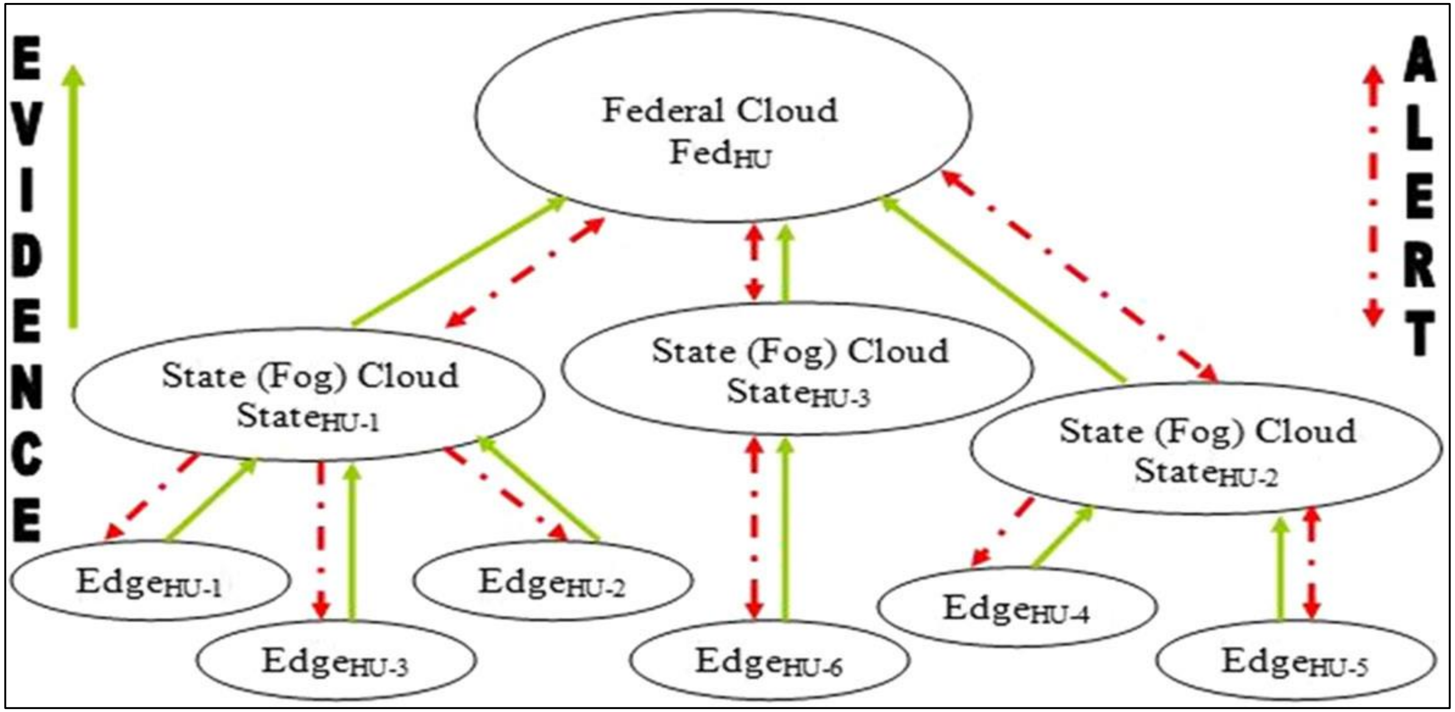
Threatroscope in BFC^2

The threatroscope operates through edge cloud centers referred to as hubs at different levels of the federation.

The hubs collect intelligent information from passing network packet traffics and disseminate important information to all service hubs/stations within.

Themodel is based on several factors using Dempster–Shafer theory (DST) to build **evidences** that can help to reach a logical conclusion from an initial state of uncertainty about packet being a threat.

We achieved the goal of closing breach detection gap using quantitative method based on the information gathered from the network traffic at the edge hub stations.



BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

The constant evidence used for monitoring and analysis is: S ={IP, SP, DP, BY, PR}.

1. IP Address (IP source for ingress and destination for egress packets)
2. Source Port (SP)
3. Destination Port (DP)
4. Bytes (BY)
5. Protocol (PR)

The two possible outcomes for these emails before the threatroscope process are:

- p = Probability of defense certified packets that are clean (to be processed by threatroscope).
- q = Probability of blocked packet with malicious email attachment (detected by layer defense).

Let us consider that the Binomial distribution independent Bernoulli trials and x =number of packets that are clear certified by $defense_M$, which will now go through threatroscope scrutiny, can be represented as

$$P(X = x) = p^x q^{n-x}$$

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

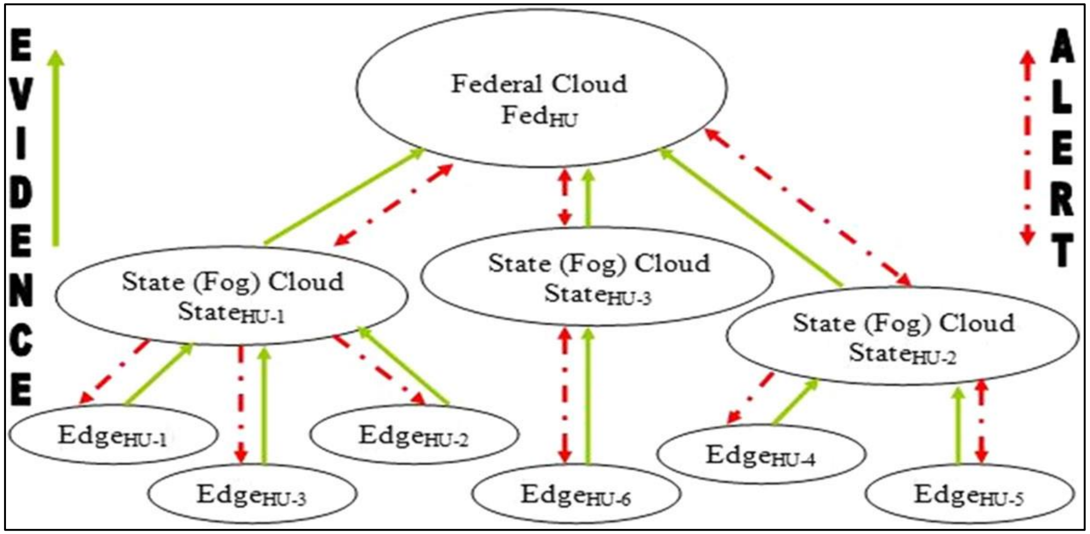
Phase 1 Dempster–Shafer theory allows belief states representation and reasoning with uncertainty. It startswith an exhaustive set ofmutually exclusive singleton hypotheses (universe) under consideration called the Frame of Discernment Ω.

Determining the Frame of Discernment: The **Edge Hub Stations are data collection points for evidential sets**.

HB-1 $\{Edge_{HU}^{1}\}$; HB-2 $\{Edge_{HU}^{2}\}$;

HB-3 $\{Edge_{HU}^{3}\}$; . . . ;HB-N $\{Edge_{HU}^{N}\}$

Ω ={HB-1, HB-2, HB-3, . . . , HB-N}



Ω represents the set (universe) where we can draw our possible conclusions from and it is exhaustive.

As packets are passing through the hubs' networks, the network flow fields (IP, SP, DP, BY, PR) are extracted and forwarded to their respective State Hub Center $State_{HU}$ and a copy to the Federated Cloud Hub Center Fed_{HU}.

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

Phase 2 Dempster–Shafer theory **assigns a mass**, called the mass function (denoted by $m(A)$) or Basic Probability Assignment (BPA), to each element of the power set, which is defined as a function $m\colon\ 2^{\Omega} \rightarrow [0, 1]$. The BPA or mass for the empty set Ø is 0, while other elements have BPA between 0 and 1, and their masses sum up to 1.

$$Belief(A) = \sum_{A \in 2^{\Omega}} m(A) = 1$$

Evidential proof	Belief			Total
	$X=1$ Genuine	$X=2$ Malicious	Uncertainty:(G, M)	
$Y=0$: None	0.3	0.1	0.1	0.5
$Y=1$: Evidence	0.1	0.3	0.1	0.5
Total	0.4	0.4	0.2	

let's assume that the first packet is from $Edge_{HU-1}$ to $State_{HU-1}$, which means evidential proof is no evidence; none existing elements of the subset $P(X = x|Y = 0)$ for now.

$Edge_{HU-1}$: HB-1={IP=162.243.149.0/24, SP=2525, DP=445, BY=12 KB, PR=TCP}.

$$m_1(HB1 - A) = \{G = 0.6, M = 0.2, U = 0.2\}$$

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC[2]

$Edge_{HU-1}$: HB-1={IP=162.243.149.0/24, SP=2525, DP=445, BY=12 KB, PR=TCP}

$$m_1(HB1 - A) = \{G = 0.6, M = 0.2, U = 0.2\}$$

$Edge_{HU-2}$: HB-2={IP=162.243.149.0/24, SP=2525, DP=445, BY=12 KB, PR=TCP} (same with 1)

⇒ we already know about IP, Byte size of it

⇒ source port, destination port, protocol type could be different even though the IP address is same

⇒ We have evidence about IP, BY

HB-2	$(X=1)$ Genuine (G)	$(X=2)$ Malicious (M)	$(1-G-M)$ Uncertainty (G, M)	Comments
Degree of belief				
IP $(X=x\|Y=1)$	0.20	0.60	0.20	Same IP with HB-1
SP $(X=x\|Y=0)$	0.60	0.20	0.20	
DP $(X=x\|Y=0)$	0.60	0.20	0.20	
BY $(X=x\|Y=1)$	0.20	0.60	0.20	Same BY with HB-1
PR $(X=x\|Y=0)$	0.60	0.20	0.20	
Total	2.20	1.80	1.00	
Normalize	0.44	0.36	0.20	

$$m_2(HB2 - A) = \{G = 0.44, M = 0.36, U = 0.20\}$$

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

Phase 3 combine two independent sets of probability mass assignments in specific situations.

$$m3 = m1 \oplus m2$$

Combination: $m_1 \backslash m_2$	$\{G\}$:0.44	$\{M\}$:0.36	$\{G,M\}$:0:20
$\{G\}$:0.60	0.264	Ø : 0.216	0.120
$\{M\}$:0.20	Ø:0.088	0.072	0.040
$\{G,M\}$:0.20	0.088	0.072	0.040

$$Dempster's\ rule\ factor\ \boldsymbol{\alpha} = \frac{1}{1 - \sum_{B \cap C \neq \emptyset} m_1(B) m_2(C)} = \frac{1}{1 - (0.088 + 0.216)} = 1.4367$$

$$m3(\{G\}) = m1(\{G\}) \oplus m2(\{G\}) = 1.4367 \times (0.264 + 0.088 + 0.120) = 0.678$$

$$m3(\{M\}) = m1(\{M\}) \oplus m2(\{M\}) = 1.4367 \times (0.072 + 0.072 + 0.040) = 0.264$$

$$m3(\{G, M\}) = m1(\{G, M\}) \oplus m2(\{G, M\}) = 1.4367 \times 0.040 = 0.057$$

$$\because m_3 = (\{G\}: 0.678, \{M\}: 0.264, \{G, M\}: 0.057)$$

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

Phase 4

$$A = \{h_1, h_2\}$$

$$Belief(A) = m(h_1) + m(h_2) + m(h_1, h_2)$$

...

$$when\ B = \{h_1, h_2, h_3\}$$

$$Belief(B) = m(h_1) + m(h_2) + m(h_3) + m(h_1, h_2) + m(h_1, h_3) + m(h_2, h_3) + m(h_1 h_2, h_3)$$

Phase 5

$$m_5 = m_4 \oplus m_3$$
$$m_6 = m_5 \oplus m_4$$
$$m_7 = m_6 \oplus m_5$$
$$\dots$$
$$m_n = m_{n-1} \oplus m_{n-2}$$

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

Packet	Pieces of evidence from edge hub stations						
	HB-1	HB-2	HB-4	HB-6	HB-5	HB-3	HB-1
IP	1.1.1.0/24	1.1.1.0/24	1.1.1.0/24	1.1.1.0/24	1.1.1.0/24	1.1.1.0/24	1.1.1.0/24
SP	2525	135	25	2525	135	134	25
DP	445	138	445	445	138	136	445
BY	12 KB	12 KB	12 KB	12 KB	12 KB	12 KB	12 KB
PR	TCP	UDP	TCP	TCP	UDP	UDP	TCP

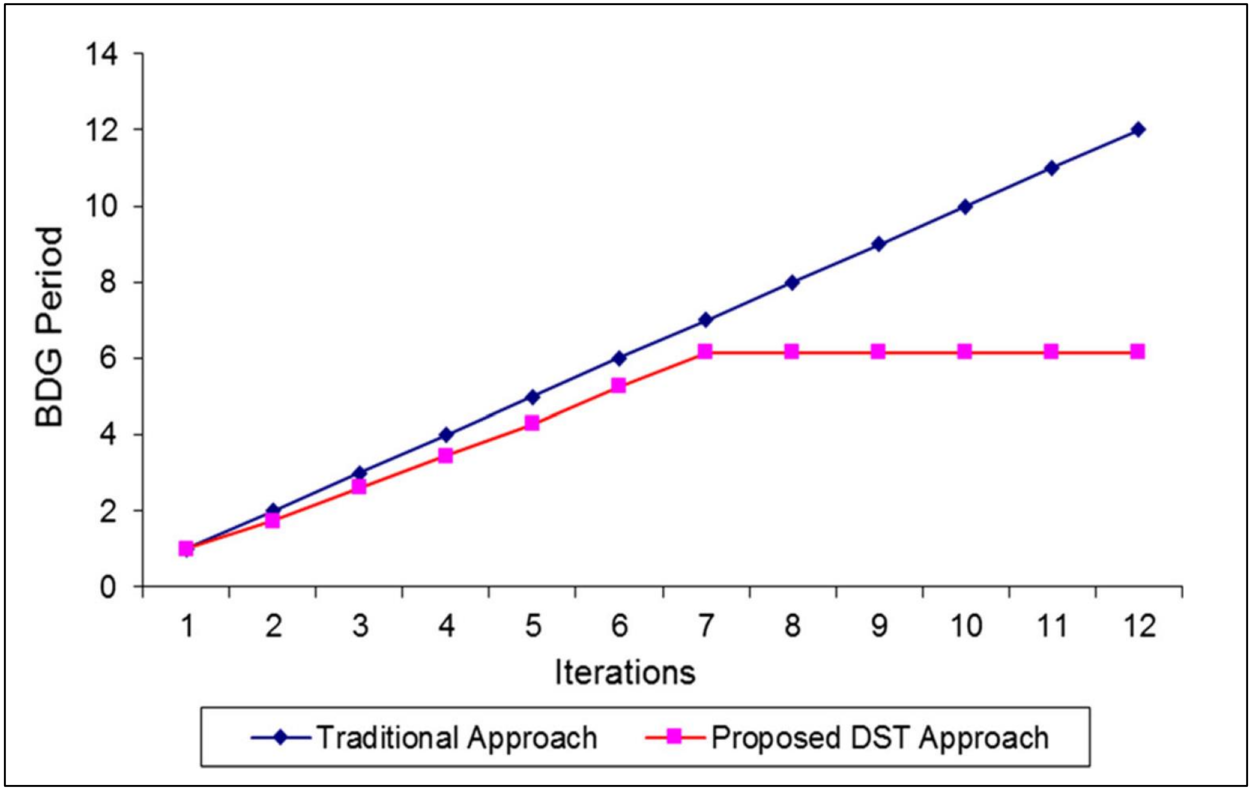
Hypotheses	Basic probability assignments $m(A)$						
	$\text{State}_{\text{HU-1}}$		$\text{State}_{\text{HU-2}}$	$\text{State}_{\text{HU-3}}$	$\text{State}_{\text{HU-2}}$	$\text{State}_{\text{HU-1}}$	
	$\text{Edge}_{\text{HU-1}}$ m_1	$\text{Edge}_{\text{HU-2}}$ m_2	$\text{Edge}_{\text{HU-4}}$ m_4	$\text{Edge}_{\text{HU-6}}$ m_6	$\text{Edge}_{\text{HU-5}}$ m_8	$\text{Edge}_{\text{HU-3}}$ m_{10}	$\text{Edge}_{\text{HU-1}}$ m_{12}
Genuine	0.60	0.44	0.28	0.20	0.20	0.36	0.20
Malicious	0.20	0.36	0.52	0.60	0.60	0.44	0.60
Uncertainty	0.20	0.20	0.20	0.20	0.20	0.20	0.20

Hypotheses	Rule of Combination						Conclusion
	$m_3 = m_1 \oplus m_2$	$m_5 = m_3 \oplus m_4$	$m_7 = m_5 \oplus m_6$	$m_9 = m_7 \oplus m_8$	$m_{11} = m_9 \oplus m_{10}$	$m_{13} = m_{11} \oplus m_{12}$	
Genuine	0.678	0.596	0.428	0.274	0.249	0.143	
Malicious	0.264	0.384	0.565	0.724	0.750	0.857	Threat!
Uncertainty	0.057	0.020	0.007	0.002	0.001	0.0002	

BFC2 threatroscope and Dempster-Shafer

Threatroscope in BFC^2

Hypotheses	Rule of Combination						Conclusion
	$m_3 = m_1 \oplus m_2$	$m_5 = m_3 \oplus m_4$	$m_7 = m_5 \oplus m_6$	$m_9 = m_7 \oplus m_8$	$m_{11} = m_9 \oplus m_{10}$	$m_{13} = m_{11} \oplus m_{12}$	
Genuine	0.678	0.596	0.428	0.274	0.249	0.143	
Malicious	0.264	0.384	0.565	0.724	0.750	0.857	Threat!
Uncertainty	0.057	0.020	0.007	0.002	0.001	0.0002	



Conclusion & Opinion

This research demonstrated how to reduce BDG for cyber-attacks using the proposed blockchain-enabled federated cloud computing framework for monitoring the data traffic.

This research have evaluated the proposed approach using numerical results, and results have shown that the proposed framework can reduce the BDG for cyber-attacks.

My Opinion

- In the real environment, BPA (Basic Probability Assignment) could not fit well because of the **dramatically unbalanced probability** of malicious behaviors.
- This study used **dichotomy** to address the state of the attack.
- Using the **kill-chain** model to consider the attack state further and applying a timeline analysis method such as the **Markov chain model** may result in a higher level of security analysis.

Thank you