


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

Olumide O. Malomo<sup>1</sup> · Danda B. Rawat<sup>1</sup>  · Moses Garuba<sup>1</sup>

© Springer Science+Business Media, LLC, part of Springer Nature 2018

**Abstract** Minimizing the breach detection gap (BDG) for cyber-attacks is a big concern for all organizations and governments. Cyber-attacks are discovered daily, many of which have gone undetected for days to years before the victim organizations detect and deploy the cyber defense. Cyber defense solutions are advancing to combat risks and attacks from traditional to next-generation advanced defense protection solutions. However, many individuals, organizations and businesses continue to be hit by new waves of global cyber-attacks. In this paper, we present a blockchain-enabled federated cloud computing framework that uses the Dempster–Shafer theory to reduce BDG by continuously monitoring and analyzing the network traffics against cyber-attacks. We evaluate the proposed approach using numerical results, and the proposed approach outperforms the traditional approaches.

**Keywords** Federated cloud · Blockchain · Breach detection gap · Federated blockchain cloud computing · Dempster–Shafer theory

---

✉ Danda B. Rawat  
db.rawat@ieee.org; danda.rawat@howard.edu

Olumide O. Malomo  
olumide.malomo@howard.edu

Moses Garuba  
mgaruba@howard.edu

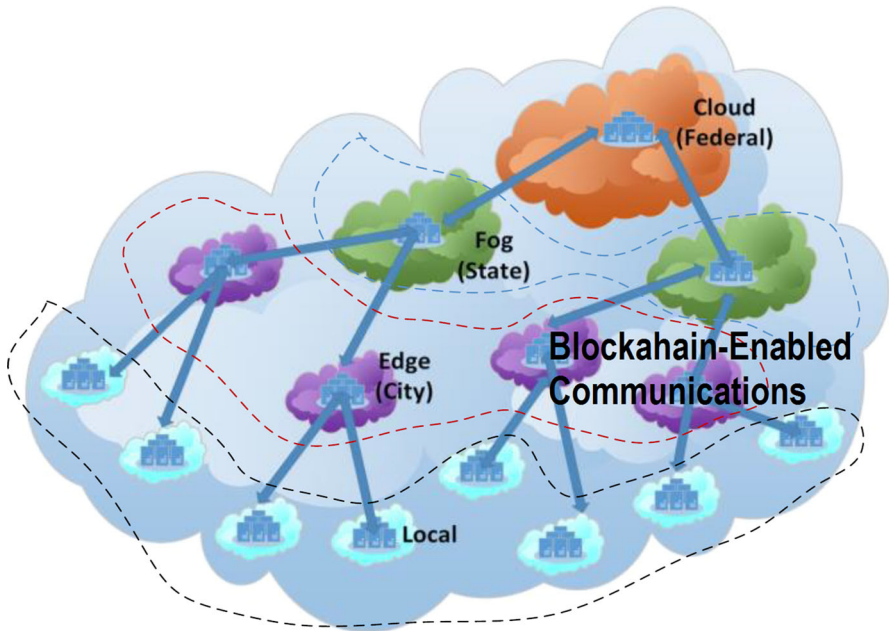
<sup>1</sup> Data Science and Cybersecurity Center (DSC<sup>2</sup>), College of Engineering and Architecture, Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA

# 1 Introduction

Cybersecurity is one of the major concerns for everyone including government and industry. There have been hundreds of billions of dollars spent on protecting and securing networked systems from malicious cyber-attacks. However, risks and vulnerabilities are growing exponentially in the Internet of Things (IoT) era [1–3]. The conventional security solutions have proven to be ineffective tools against the emerging cyber threats. Some improvements have been retrofitting security for the flaws in technologies and abstractions, which cyber criminals are taking advantage of for their nefarious acts. Newer technologies cannot be absolved, as some introduced vulnerabilities into the wild because of competition, urgency, and competitive advantage to develop market cutting edge business solutions. There are different cybersecurity solutions varying from antivirus to firewalls to intrusion detection/prevention system (IDS/IPS) [4–6]. 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) [7–12]. In recent times, attack vectors are similar against most organizations or industries across USA, Europe, South America and Asia in a new wave of global cyber-attacks, mainly because cyber criminals are aware of a wide variety of technology vulnerabilities common to consumers and enterprise technology. Reports are showing that the security risks are on the rise, with some executives sure that cyber intrusion will happen to them [13]. Businesses victims of cybercrime across the globe are left with damaged reputation, loss of customers trust, early termination of top executives' appointments, and security professionals' competencies are questioned for situations beyond their control. These are just a few of the consequences of cyber security breach [14].

In this paper, we design, develop and evaluate Blockchain-enabled federated cloud computing (BFC<sup>2</sup>) framework for next-generation cybersecurity to reduce data breaches and BDG. Figure 1 depicts a typical blockchain-enabled federated cloud framework where participating organizations use their block managers for sharing the information with other participants [48, 49].

The BFC<sup>2</sup> provides capabilities for promoting tighter security and restricted access control by using packet monitoring and traffic analysis. The BFC<sup>2</sup> framework consists of three basic components: block generator, block vault, and threatroscope. The block generator is central to the framework and handles all basic functions of BFC<sup>2</sup> operations such as generating blocks with transactions and signing them digitally to add in both distributed and centralized ledgers. The block vault is reserve vault operating as a secure storage for clients' offsite digital assets and access is through a chain of authorization. The threatroscope is designed to help customers enjoy continuously, real-time security monitoring, and robust analysis of network traffics before leaving the point of presence (POP) to reach their local networks and as such compensate for any weak or less advanced security mechanisms in any participating organizations that is within the federation. The threatroscope monitors and analyzes egress traffics for command and control servers using similar approach to detect egress attacks, existing exploit which may have occurred through social engineering Trojans or phishing email, or network traveling worms. The threatroscope is based on several factors using Dempster-Shafer theory (DST) as basis to track and build evidences of probable cyber-attacks. It sim-



**Fig. 1** Blockchain within federated cloud architecture

plifies security protection, manages risk exposure, eliminates unnecessary overheads [15–17] and is expected to reduce the cyber-attack significantly [18–20].

The rest of the paper is organized as follows: Sect. 2 describes our proposed framework BFC<sup>2</sup> (Blockchain-enabled federated cloud computing), with reference to blockchain technology. In Sect. 3, we present BFC<sup>2</sup>—threatroscope proposed approach for intelligence, strong and resilient cybersecurity using Dempster–Shafer methods as basis. Finally, conclusions are presented in Sect. 4.

## 2 The BFC<sup>2</sup> framework

BFC<sup>2</sup> system model is permissioned; meaning it's a Federated blockchain [21–25] suitable for enterprises that want privacy and restricted access control, which is not permissionless public Blockchain. The objective of having permissioned blockchain [26–30] is to have a tighter security, fraud-free environment, and management similar to Ethereum [31–42]. The proposed BFC<sup>2</sup> Architecture is shown in Fig. 2 which consists of three distinct systems that are interconnected: block generator, block vault, and threatroscope. Block generator comprises of license issues, processing chamber, and distributed Blockchain. Block vault is a chained secure storage for transactions and blocks. Threatroscope is designed for real-time network traffics monitoring and analysis of inbound and outbound traffics passing through participating organizations. The main goal of the threatroscope is to improve breach detection gap.

In BFC<sup>2</sup>, some participants are Validators  $V_L$  (licensor) and some are clients  $C_L$  (licensee). We start with smart contracts, which is a digital agreement that verifies that

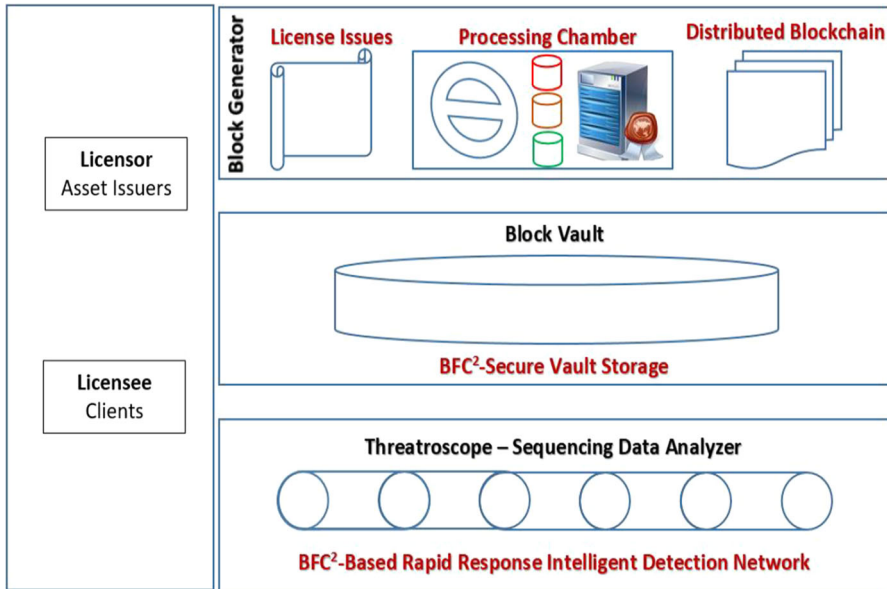


Fig. 2 BFC² architecture

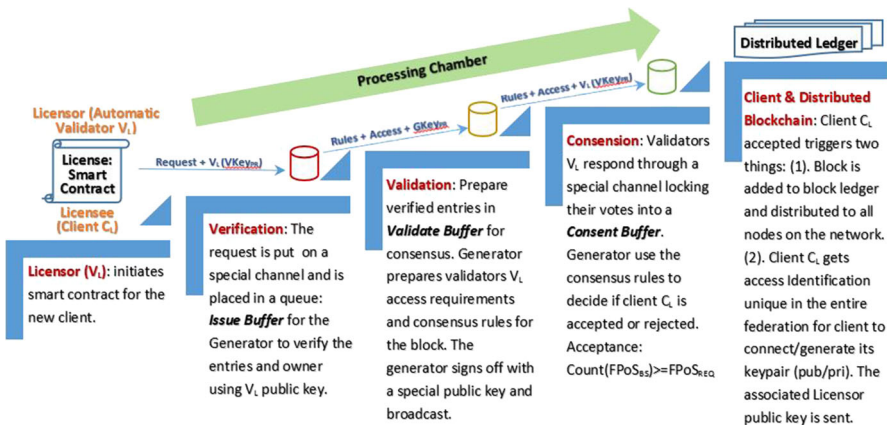


Fig. 3 BFC² block generator—process/stages progression

there is a legal license agreement between any of the Validators  $V_L$  and client  $C_L$ . This is important to the system and required any client  $C_L$  that needs to join the network to go through this process. In this contract, there will be rules for negotiating the terms of the agreement and what will govern client's transactions and future interactions within the network. It is the processing of the smart contract that initiates the client on-boarding process into the blockchain system. Figure 3 shows the steps.

The Validator  $V_L$  can raise a new transaction request, if he has none pending in any of the pipeline, signs it with his private key ( $VKey_{PR}$ ), and broadcasts on a special channel over the network. The signed request goes through a processing chamber

pipeline into an *issue buffer* for the generator to process. Then the generator verifies the owner using a copy of the Validator's  $V_L$  public key ( $VKey_{PUB}$ ) and ensures that all necessary requirements are in place. If everything is in place, the transaction request progresses in the pipeline to the *validate buffer*. The generator prepares the entry in the validate buffer for consensus to vote using the validation rules. The generator prepares access credentials required by the Validators, a hash copy of the last block for security, some other data required pertaining to the process, timestamp, signs off using its special private key ( $GKey_{PR}$ ), and broadcasts on a special channel. The Validators can send their responses to the *consensus buffer*. The decision for acceptance or rejection is based on the consensus rules. The generator checks the validity of the votes in the *consensus buffer* using Validators' public keys ( $VKey_{PUB}$ ) and counts to determine whether the required number for acceptance is met. Otherwise, it is rejected, and Licensee is advised through the rejected transaction process special channel and reasons for rejection. The federated agreed procedure for rejected contract transaction for reprocessing would have to be followed. Acceptance implies consensus when  $\text{count}(FPoS_{BS}) \geq FPos_{REQ}$ . Federated-Proof-of-Stake (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. The threshold value of  $FPoS_{BS}$  and  $FPoS_{REQ}$  is decided by the federation. For example, if the number of block signers ( $FPoS_{BS}$ —Validators that participate in consensus agreement)  $FPoS_{BS}$  that are agreeing to the validity of a block equals or exceed the required signature to accept block  $FPoS_{REQ}$  such that  $\text{count}(FPoS_{BS}) \geq FPos_{REQ}$ , then the transaction becomes a blockchain ledger record and it is propagated. The generator adds the new contract to the block ledger and completes everything that will make the new block (previous hash + new) and distribute to all nodes (Licensors/Validators) on the network. The generator checks if client  $C_L$  (Licensee) already exists in the system, and if not, update CIM (Client-Intro-Manager) showing the Licensors and Licensee associativity, and assign the new client unique federated access identification ( $C_L\text{-ID}$ ). For new client or existing, the generator finalizes client's on-boarding and forwards the Licensors public key ( $VKey_{PUB}$ ) for the new contract, signed by its own private key ( $GenKey_{PR}$ ).

The one major concern is the Sybil attack which can be carried out by just a single Validator in the system that wants to be generating fake new transactions or delay consensus, making it impossible to agree on transaction validation. The system can expose such malicious Validator and defend against these issues based on the policies adopted by the federation. The issue of generating fake new transaction is controlled by having one new transaction only that can be raised at a time provided there is no pending transaction in any of the buffers in the processing chambers. The special channel to broadcast request is available only if this condition is met. The channel is locked once request is turned for processing and unlocks, free for any new transaction. This is very important and must be enforced, because any transaction that has gone through the due diligence process/activities to become a block, which may have been either raised by an attacker or genuine Validator, is treated as a legitimate transaction block. There is provision for any Validator in the consortium to request for audit in accordance with the policy. However, a high rate of transactions from one source being rejected will draw attention for auditors/regulators to investigate which can easily lead

to identifying a malicious attacker. The other issue is consensus problem which can only be detected based on the number of times (frequency) a malicious Validator is randomly picked/selected to vote on transactions. Since acceptance of transaction to block is determined by Consensus count( $\text{FPoS}_{\text{BS}} \geq \text{FPoS}_{\text{REQ}}$ ). Let us assume that the policy says 10 Validators are randomly selected as  $\text{FPoS}_{\text{BS}}$  (block signers) and only 7 ( $\text{FPoS}_{\text{REQ}}$ ) Validators' signature with same value can decide either to accept or reject a transaction. Technically, it will require over  $\geq 40\%$  malicious attackers to always decide the fate of any transaction. However, the 40% attackers would first have to be selected to validate that transaction. The probability will depend on the size of the pool of potential Validators available to select from, and what the algorithm for the selection takes into account: at least in the minimum, randomization as best as possible. Since privacy is protected on the network, they would have to be in communication to know that they are all selected, and their votes are required before any attack can be successful. However, a greater concern is having one attacker (delayed attack), whose vote matters most when it is required as the last count to make decision either to reject or accept transaction. Let's say we have 6 Validators' acceptance votes and 3 rejection votes (or there may be one or two of the three that did not respond). To best illustrate the point, let us use the data in Table 1, which is generated using random variables showing the time in minutes when Validators voted on transactions.

Please note that an average time was computed for the 6 good Validators and the last row is the decision that can be made by the evil Validator. Figure 4 shows how the attacker can hurt the system in two ways: by voting acceptance but delayed response (D-A). More painfully is delaying response and eventually voting rejection (R) which will force rejection process and cost the Licenser time to go through the reprocessing all over again. We can see how the attacker can make it difficult to avoid being detected by voting earlier in Txn-3 and Txn-8.

The attacker progress and impact to the network may be for a while. But through Poisson distribution, when the probability expectations for processed transactions for a period begin to drop, and rejection is high, it won't be long before auditors get to the root of the problem. One good policy that can help to mitigate this problem will be to reduce voting response time to an acceptable time frame in minutes, which can be based on transactions processed daily.

### 3 The BFC<sup>2</sup> threatroscope and Dempster–Shafer

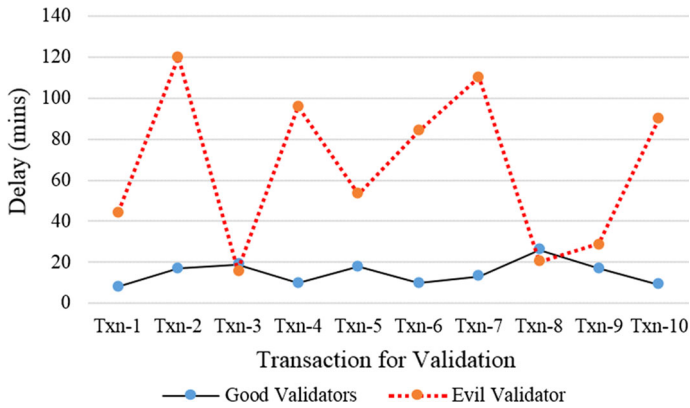
#### 3.1 BFC<sup>2</sup> threatroscope

Today, there are many systems and networks that seem secured just because there has not been DDoS. Some Administrators would be shocked to know their servers are being under command and control, communicating with some external botnets or with some sorts of Internet relay chat bot. 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. If public cameras can help to deter crime and solve high profile criminal cases,

Table 1 Transactions for consensus with results

Transactions for consensus (average time for 6 good Validators with acceptance and 1 evil validation)										
	Txn-1	Txn-2	Txn-3	Txn-4	Txn-5	Txn-6	Txn-7	Txn-8	Txn-9	Txn-10
Good Validators	8	17	19	10	18	10	13	26	17	9
Evil Validator	44	120	16	96	53	84	110	20	29	90
	D-A	R	P	R	D-A	R	R	P	P	R

Table keys *D-A* Delay and Accept, *R* Reject, *P* Perfect



**Fig. 4** Possible consensus attack (6-3-1) from a malicious Validator

then threatroscope is novel; it is designed for continuous monitoring, coordination, cooperation and information sharing among hubs at the edges, fogs and the federal clouds. ComputerWeekly.com on their website [43] reported that 30% of malware are zero-day exploits which are new in the wild. They said “companies could be missing up to third of malware that is targeting them, according to a report by WatchGuard”. Those missing undetected malwares by security mechanisms are our interest. For better understanding, if we can just focus on emails to illustrate our point. Let us take the report of Digital Guardian [44] and Faronics blog report on a study that “91% of all cyber-attacks start as phishing email”. Figure 5 gives a graphical representation of hypothetical situation with randomly generated numbers to buttress the point computerweekly.com was making. Say we have a device that inspect packets and can detect malicious packet especially for emails with attachment,  $M$  number of emails (100 within 10 min) passed through the security device and were inspected,  $K$  number (63) had attachment, and out of these we know that  $X$  number (37) were actually emails with malicious attachment, but unfortunately, the device could only detect  $Y$  number (15), so the issue is what about the  $Z$  number ( $Z = X - Y = 22$ ) that passed through the system undetected which in our table we term zero-day. This is one clear digital security risk organizations face on daily basis. Malicious threats like these that have managed to pass through the security systems undetected, waiting for any vulnerability to cause damage or loss which may result to both serious tangible and non-tangible consequences. The longer they stay undetected, the greater the risk which is why the breach detection gap (BDG) or prevention gap is very important, and our system can reduce BDG time including the time it takes to detect zero-day threats.

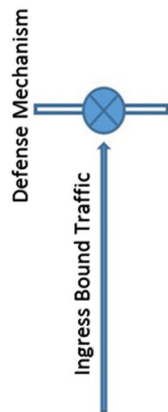
We shall briefly cover Dempster–Shafer theory by way of introduction and show its basis to threatroscope design concepts.

### 3.2 Dempster–Shafer theory

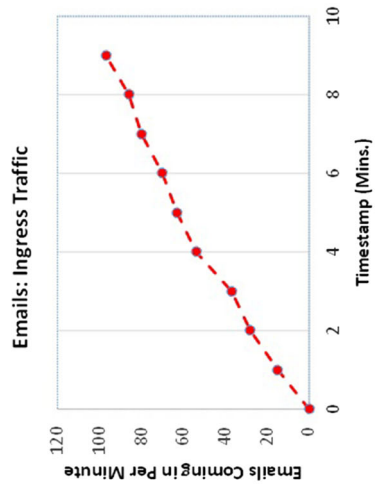
Dempster–Shafer’s theory (DST) is a mathematical theory that is referred to as theory of evidence or belief functions based on degree of belief. The theory is the contribution



**Fig. 5** Sample digital security risk hypothetical analysis



Timestamp (Mins.)	Cumulative Emails	No. of Emails/Mins.	Attachment	Infected	Detected	Zero Day
0	0	0	0	0	0	0
1	15	15	8	4	3	1
2	28	13	10	3	2	1
3	37	9	7	4	3	1
4	54	17	5	3	2	1
5	63	9	6	4	3	1
6	70	7	7	4	3	1
7	80	10	5	5	4	1
8	86	6	4	2	1	1
9	97	11	9	6	5	1
10	100	3	2	2	1	1
Total:		100	63	37	27	10



of Dempster and Shafer. First developed by Dempster (1967) and later, Shafer (1976) refined the method of obtaining degree of belief from weights of evidence, which is different from traditional probability density function and is a better alternative for risk evaluation. The states of evidence and beliefs are mathematically represented by belief functions and Dempster's rule of combination applied to process belief interval and plausible reasoning to determine the degree of certainty of belief [wiki]. Dempster–Shafer is the right mathematical discipline for our model as the theory potentially allows the combination of separate pieces of network data packet (evidence) obtained from multiple hubs within the federated cloud and modeling them by using associative and commutative methods to logically determine whether an exploit is underway without resorting to assumptions. However, how related the evidence from multiple sources can have great impact on the computation time and information obtained from their combination [wiki]. Dempster–Shafer framework has connections to other frameworks such as probability, possibility and imprecise probability theories [wiki]. However, there are five concepts that are basis to Dempster–Shafer theory and three of them are important functions:

- Frame of discernment.
- Basic probability assignment function (BPA) or mass function (m).
- Dempster rule of combination.
- Belief function (Bel).
- Plausibility function (Pl).

Each of these concepts would be explained in phase as we discuss threatroscope framework and highlight other concepts that may be relevant to DST in the course of our discussion. We start with Dempster–Shafer framework connections to probability and the connection probability has to threatroscope.

### 3.3 Integration of Dempster–Shafer with probability and threatroscope

The basis of Dempster–Shafer theory has relationship with probability. Marginal, joint and conditional probabilities are three distinct probabilities that are useful to help produce the result of probabilities of events occurring based on the combinations of other events (intersection of events, union of events, dependent and independent events, and complement event) that may be known to have occurred and also determine the relationships between these events. Their concepts we would use to introduce normalization which is also very relevant to DST. Marginal probability deals with a single event occurrence  $P(X=x)$ ; joint probability deals with two events that can occur at the same time  $P(X=x, Y=y)$  and; conditional probability deals with a particular event occurring given that there is a supporting evidence that another event has occurred  $P(X=x|Y=y)$ . For example, email event in our model can have two discrete random variables  $X$  and  $Y$ .  $X$  represents “Riskware” state of email and takes on a value of 0 if an email is genuine and 1 if an email is malicious.  $Y$  represents “Belief” and takes a value 0 if our belief is with no evidence and a value of 1 if there is evidence. We used the binomial relationships that exist in these random variables to represent multivariate of at least four possible cases [as shown in the Table of Probabilities (Table 2)]. Let us assign probability values to the possibility of the cases occurring:

**Table 2** Table of probabilities

Evidence (Y)	Belief–riskware (X)		
	Genuine (0)	Malicious (1)	
No Evidence (0)	0.5	0.1	Row 1
Evidence (1)	0.1	0.3	Row 2
	Column 1	Column 2	

The probability (Uncertainty-belief) that an email is “genuine” with “no evidence”=0.5.

The probability (belief) that an email is “genuine” with “evidence”=0.1.

The probability (Uncertainty-belief) that an email “malicious” with “no evidence”=0.1.

The probability (belief) that an email “malicious” with “evidence”=0.3.

*Note* The probability is 0.3 because the sum of all the probability must equal to 1.

$$\sum_{x,y} P(X = x, Y = y) = 1 \quad (1)$$

*Joint probability* Let’s say we want the probability of an email belief to be malicious, and we have evidence:  $P(X = 1, Y = 1) = 0.3$  [Implies: joint probability is the intersection  $P(X_1 \text{ and } Y_1)$ ].

*Marginal probability* Let’s say we want the probability of an email belief to be genuine:  $P(X = 0) = 0.5 + 0.1 = 0.6$ .

Also, if we want the probability of an email belief to be malicious:

$$P(X = 1) = 0.1 + 0.3 = 0.4.$$

And if we want the probability that we have evidence on an email (which in this case could be genuine or malicious):

$$P(Y = 1) = 0.1 + 0.3 = 0.4$$

It implies marginal probability operates down columns in the  $X$  cases and across rows in the  $Y$  case. In relation to Joint probability:

$$P(X = x) = \sum_y P(X = x, Y = y) \quad (2)$$

*Conditional probability* Let’s say we want the probability at random an email belief to be malicious given that we have the evidence to support our belief  $P(X_1 \text{ given } Y_1)$ : To compute this, we can use both knowledge of marginal and joint probability.

$$P(X = 1 | Y = 1) = P(X = 1, Y = 1) / P(Y = 1) \quad (3)$$

From joint probability, we know the result of  $(X = 1, Y = 1) = 0.3$ .

From marginal probability, we know also the result of  $P(Y = 1) = 0.4$ .

Therefore,  $P(X = 1|Y = 1) = P(X = 1, Y = 1)/P(Y = 1) = 0.3/0.4 = 0.75$ .

The result  $P(X = 1|Y = 1) = 0.75$  is noteworthy because earlier, before we had our evidence, the marginal probability  $X_1$  was 0.4 and with the evidence to support our belief that the email is malicious  $Y_1$  has changed the probability of  $X_1$  to 0.75. These two events are called dependent events because they are related. This aspect of changes is very important to DST as there would be independent (one event cannot be influenced/affected given that another event occurred) or related and dependent events, when new information and more evidence are made available, belief interval and plausible reasoning for determining the degree of certainty of belief could be impacted.

*Normalization* This is another aspect that is important to DST and can impact the belief and plausible results. Let's focus on row 2 and conditional probability, given that we have evidence to support our belief. Whatever probability we are looking for in row 2 will mean all possible outcomes in row 2 have to sum up to 1. There are two possibilities, and the sum of their probabilities must equal to 1: That is:  $P(X = 0|Y = 1) + P(X = 1|Y = 1)$  which does not equal 1. Part of the solution requires normalization, which is simply dividing with the marginal probability  $Y_1$  (0.4):

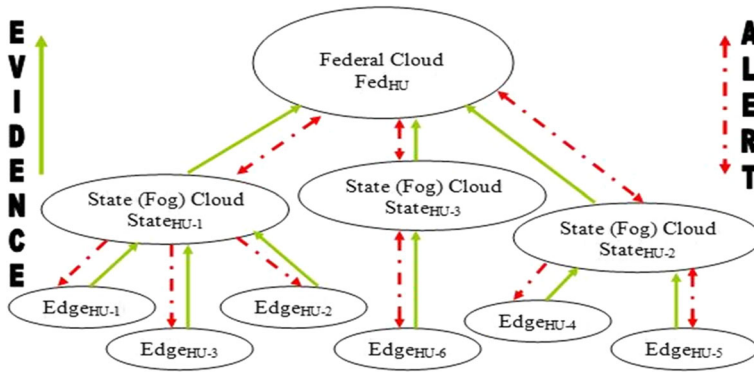
$$P(X = 0|Y = 1) + P(X = 1|Y = 1) = 0.1/0.4 + 0.3/0.4 = 1 \quad (4)$$

The idea of this aspect to DST is to ensure there is a ratio that is proportion and relevant to the entire sampling data. However, we should point out that probability requires all sum to 1, but in DST, there is a degree of support between 0 (fact is not supported) and 1 (fact is supported). This section is good for statistical analysis of the sample and population variables. We can now breakdown threatroscope framework into DST phases.

### 3.4 Threatroscope in BFC<sup>2</sup>

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 without breach of confidentiality or integrity, process, analyze and disseminate important information accordingly in an effective intelligent fashion to all service hubs/stations within the federation. Figure 6 depicts the concepts.

The model 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. Some parameters/metrics were determined qualitatively. The system can operate as hybrid and work with any existing layered defense infrastructures. It operates on packets that have passed through all the layers of security mechanism infrastructures. For example, let's say our interest is on emails with attachment (emails<sub>att</sub>) and assume at this point, the packets we are interested in have



**Fig. 6** Evidence and alert signal flow

passed through front layers of defense mechanisms (defense<sub>M</sub>) and certified clean. A solution's filter has helped to classify the packets which are now routed to a functional unit in the threatroscope that handles emails with attachment. This marks the beginning of threatroscope process of validating the defense<sub>M</sub> action. We can characterize the flow of traffic at the defense<sub>M</sub> using the Bernoulli distribution. A Bernoulli trial or binomial trial can give us the expression with two mutually exclusive and exhaustive outcomes.

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

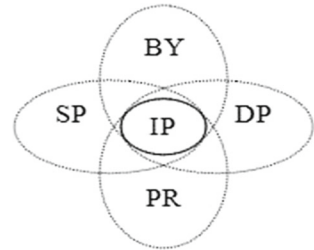
$p$  = Probability of defense certified packets that are clean (to be processed by threatroscope).

$q$  = 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<sub>M</sub>, which will now go through threatroscope scrutiny, can be represented as  $P(X = x) = p^x q^{n-x}$ .

The system applies the DST about belief on the  $x$  number of packets cleared by the defense mechanisms by combining several parameters as independent sets of probability which create rules guiding specific message block of interest. Evidence is very important to the ideas Dempster–Shafer theory is based upon and in fact, Shafer theory's degree of belief is based on evidence with great emphasis. Evidence is what support outcomes. However, the type of evidence is equally very important, especially when the theory's approach is combining evidences from multiple sources, there might be some conflicting beliefs, higher number of possible outcomes, and computation complexity could increase significantly.

Threatroscope uses consistent evidence type (as shown in Fig. 7) because IP address (regardless of masked IP through proxy server or regular IP address) is a piece of evidence that is definitely required and is common to all subsets  $S$  of our hypotheses (frame of discernment) in the universal set. There are other types of evidence that can be used in DST, such as: disjoint evidence, consonant evidence and arbitrary evidence [45]. The constant evidence used for monitoring and analysis is: IP Address (IP—source for ingress and destination for egress packets), Source Port (SP), Destination

**Fig. 7** Consistent evidence type

Port (DP), Bytes (BY), and Protocol (PR) [46].  $S = \{IP, SP, DP, BY, PR\}$ . Note IP is constant piece of evidence in every subset  $S$ . We can add to the evidence subset, any uniquely or additional packet field fit (e.g.,  $\{U\}$ ). While the IP is a constant evidence, there is the possibility that other elements of similar kind of evidence may differ from what is obtained from multiple sources (e.g., Protocol— $PR = \{TCP, UDP\}$ ). We used the IP address range (e.g., 107.170.230.0/24) to allow more packets from similar subnet. However, the scope can be narrowed down to single IP address.

**Phase 1** Dempster–Shafer theory allows belief states representation and reasoning with uncertainty. It starts with an exhaustive set of mutually exclusive [46, 47] singleton hypotheses (universe) under consideration called the Frame of Discernment  $\Omega$ .

**Determining the Frame of Discernment:** The Edge Hub Stations ( $Edge_{HU-1}$ ,  $Edge_{HU-2}$ ,  $Edge_{HU-3}, \dots, Edge_{HU-N}$ ) are data collection points for evidential sets required in modeling to reach logical possible conclusions on belief. The events that occur at  $Edge_{HU-1}$  are independent of the events that occur at  $Edge_{HU-2}$  and any other hub stations. However, having an IP address within the same subnet range is what associate two or more events for modeling. These hub stations are singleton hypotheses of the frame of discernment  $\Omega$ . Figure 6 depicts the hypotheses:

$$\begin{aligned} HB-1 &= \{Edge_{HU-1}\}; HB-2 = \{Edge_{HU-2}\}; \\ HB-3 &= \{Edge_{HU-3}\}; \dots; HB-N = \{Edge_{HU-N}\} \\ \Omega &= \{HB-1, HB-2, HB-3, \dots, HB-N\} \end{aligned}$$

$\Omega$  represents the set (universe) where we can draw our possible conclusions from and it is exhaustive. Any singleton of the hypotheses (HB-1 or HB-2 or ... HB-N) is mutually exclusive that is, at most there must be one of the hypotheses that have to be true.

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  $Fed_{HU}$ ; with a time stamp and tagged with station identity code (e.g., HB-1). These data become admissible evidence at the  $State_{HU}$  and  $Fed_{HU}$  levels in the federated cloud. This part of the process is significant to a piece of the evidence (IP) because depending on network traffic flow direction, packet's originating source IP address is for determining the possibility of an ingress network traffic attack in the direction of client's network. While destination IP address

is an egress packets for detecting servers that are under “command and control” attack by external botnets. Evidences captured are model based on the direction of network traffic (ingress/egress). Thus, evidences received at the State<sub>HU</sub> are stored and index on IP address range for phase 2 of the process. A concatenation of the IP address with port number would have been good to be used as the index; unfortunately, any service can be configured to run on any port, which makes it difficult to use port numbers to determine the actual service. One other restrain on live operating network is capturing full packet, which would be desirable for more analyses, but could result to issues:

- Security and privacy of organizations with sensitive data which by law must be protected on the network could be breached. It is very important to avoid confidentiality breach.
- Storage throughput and analysis complexity can increase significantly creating a problem.

**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  $m: 2^\Omega \rightarrow [0, 1]$ . The BPA or mass for the empty set  $\emptyset$  is 0, while other elements have BPA between 0 and 1, and their masses sum up to 1.

$$Bel(A) = \sum_{A \in 2^\Omega} m(A) = 1 \quad (4)$$

Assigning mass, Basic Probability Assignment (BPA) –  $m(A)$ : This is the first of the three important functions. Phase 2 of threatroscope has three separate cases and processes in which two are closely related (cases 2 and 3). From Fig. 6 and apart from genuine network packets, there are three cases (classify as exploits) that may occur as evidences flow from edge cloud to higher level cloud centers in the federation:

1. Attack against Edge Cloud: A State<sub>HU</sub> is continuously receiving similar evidence from the same Edge<sub>HU</sub>. For example, State<sub>HU-1</sub> continues to receive same (or almost similar) evidence from Edge<sub>HU-3</sub> with an IP address within the same range. This case is managed through threshold value that must be exceeded within defined time frame before action is taken. Computation of BPA function is only required once in this case, which implies there is little or no additional computational complexity. However, the threshold value and time frame (e.g., say 256 within some reasonable time) must be agreed by the federation. If the number of packets received exceeded the threshold within the set time frame, then this is a flag; either probe attack is in progress or possible Denial of Service Attack (DoS/DDoS). Information is disseminated to block generator for consensus decision; the entire federation is put on alert. This way breach time is reduced significantly; client/business under attack is alerted by CIM (Validator that initiated client’s smart contract) and saved from possible damaging reputation and financial loss, risk is managed, and the entire federation benefits.
2. Attack against State Cloud: State<sub>HU</sub> received related evidence (IP address within same range) from multiple sources under its state (Edge<sub>HU-1</sub> and Edge<sub>HU-2</sub>). For example, let’s say in phase 1, Edge<sub>HU-1</sub> forwarded evidence:

**Table 3** Threatroscope table of conditional probabilities

Evidential proof	Belief			Total
	$X=1$	$X=2$	Uncertainty:(G, M)	
	Genuine	Malicious		
$Y=0$ : 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	

$S = \{IP = 162.243.149.0/24, SP = 25, DP = 445, BY = 12 \text{ KB}, PR = TCP\}$  to State<sub>HU-1</sub>, then sometime Edge<sub>HU-3</sub> received packet within the same IP address range:

$S^I = \{IP = 162.243.149.0/24, SP = 135, DP = 138, BY = 12 \text{ KB}, PR = UDP\}$  and forwarded to State<sub>HU-1</sub>; computation of Basic Probability Assignment function (BPA) is required and BPA computation is triggered.

- Attack against Federation: This is a case where by Fed<sub>HU</sub> handles the computation of BPA for evidences from multiple sources involving different State<sub>HU</sub>. For example, evidences coming from Edge<sub>HU-1</sub> and Edge<sub>HU-2</sub> of State<sub>HU-1</sub>, Edge<sub>HU-4</sub> of State<sub>HU-2</sub>, and Edge<sub>HU-6</sub> of State<sub>HU-3</sub> are to be combined. However, Fed<sub>HU</sub> starts with an updated BPA function from State<sub>HU</sub>. For example, State<sub>HU-1</sub> had already computed BPA function for Edge<sub>HU-1</sub> and Edge<sub>HU-2</sub> before new evidence from another state is forwarded to the Fed<sub>HU</sub> for processing.

We continue with phase 2 computation of Basic Probability Assignment function (BPA) or mass function  $m(A)$  and its broken down as follows. Basic Probability Assignment (BPA): Based on the case, BPA is assigned either at the State<sub>HU</sub> or Fed<sub>HU</sub> using conditional probability with threatroscope table of probabilities (Table 3). Belief is strengthened by evidential proof of an element in a subset that is already known. Data are held as admissible evidence accessible to both State<sub>HU</sub> and Fed<sub>HU</sub> centers.

To assign BPA, let's assume that the first packet is from Edge<sub>HU-1</sub> to State<sub>HU-1</sub>, which means evidential proof is no evidence; none existing elements of the subset  $P(X=x|Y=0)$  for now.

Edge<sub>HU-1</sub>: HB-1 =  $\{IP = 162.243.149.0/24, SP = 2525, DP = 445, BY = 12 \text{ KB}, PR = TCP\}$ .

The BPA is assigned to the set:  $m_1(HB1-A) = \{G \text{ Genuine}, M \text{ Malicious}, G-M \text{ Uncertainty}\}$ , using threatroscope table of conditional probabilities and computation of the evidence to BPA  $m_1(HB1-A)$  is shown in Table 4.

As shown in the table  $m_1(HB1-A) = \{G \text{ Genuine} = 0.60, M \text{ Malicious} = 0.20, G, M \text{ Uncertainty} = 0.20\}$ . Our belief function for example of  $M$  (malicious) is the minimum belief of  $M$  that is based on the evidence we have, which is the local belief of  $M$  for now. As evidences flow to the State<sub>HU</sub>, they are built up to check for match with subsequent events with data within the same IP address range. Suppose State<sub>HU-1</sub>, received data from:

Edge<sub>HU-2</sub>: HB-2 =  $\{IP = 162.243.149.0/24, SP = 2525, DP = 445, BY = 12 \text{ KB}, PR = TCP\}$ .



**Table 4** BPA  $m_1$ (HB-1A)

HB-1	IP	SP	DP	BY	PR	Total	Normalize
Degree of belief							
Genuine ( $G$ ) $P(G)=P(X=1 Y=0)$	0.60	0.60	0.60	0.60	0.60	3.00	0.60
Malicious ( $M$ ) $P(M)=P(X=2 Y=0)$	0.20	0.20	0.20	0.20	0.20	1.00	0.20
Uncertainty ( $G/M$ ) $(1-P(G)-P(M))$	0.20	0.20	0.20	0.20	0.20	1.00	0.20

**Table 5** BPA  $m_2(\{HB2-A\})$

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	

From this set, there is an intersection ( $HB-1 \cap HB-2$ ); the elements (IP and BY) in HB-1 will now be used as evidence since they also belong to HB-2. The computation of BPA assigned to  $m_2(\{HB2-A\})$  is shown in Table 5.

As shown in the table, BPA is assigned to  $m_2(\{HB2-A\}) = \{G: \text{Genuine} = 0.44, M: \text{Malicious} = 0.36, G, M: \text{Uncertainty} = 0.20\}$ . Because there are evidences from multiple sources, we need to apply the Dempster rule of combination on BPA  $m_1$ (HB-1) and the new BPA  $m_2$ (HB-2) to update our belief.

**Phase 3** Dempster–Shafer theory uses the rule of combinations as fusion operator to combine two independent sets of probability mass assignments in specific situations. The reason being that there might be a case of different sources expressing their beliefs over the frame of discernment in terms of belief; therefore, the rule of combinations derives common shared belief between all the multiple sources and all the conflicting beliefs are ignored through a normalization factor [wiki]. It will be an interesting research to study fusing separate beliefs estimates from multiple sources as there are some criticisms.

*Dempster’s Rule of Combination* This aspect of the theory is very important because the combination of independent evidences determines the belief interval by showing the validity and associative of the evidences, and also both their minimum (Belief) and maximum share (plausible). The belief interval is the difference between the belief and plausible, and the smaller it gets, shows strong indication of certainty about the

**Table 6** BPA  $m_1(\{\text{HB1-A}\}) \oplus \text{BPA } m_2(\{\text{HB2-A}\})$ 

Combination: $m_1 \setminus m_2$	$\{G\}:0.44$	$\{M\}:0.36$	$\{G,M\}:0.20$
$\{G\}:0.60$	0.264	$\emptyset:0.216$	0.120
$\{M\}:0.20$	$\emptyset:0.088$	0.072	0.040
$\{G,M\}:0.20$	0.088	0.072	0.040

$\alpha = 1/1 - (0.088 + 0.216) = 1.4367$  (we applied Eq. 7)

belief. The rule of combination is the conjunctive operation of masses and has two properties:

$$\text{Given two masses } m_1 \text{ and } m_2 : m_{1,2}(A) = m_1 \oplus m_2(A) = \alpha \sum_{B,C:A=B \cap C} m_1(B) m_2(C) \quad (6)$$

where  $\text{BPA } m_1(B) \neq 0$  and  $\text{BPA } m_2(C) \neq 0$

$$\alpha = \frac{1}{1 - \sum_{B \cap C \neq \emptyset} m_1(B) m_2(C)} \quad (7)$$

We need to apply the rule of combination on the two evidences  $m_1(\{\text{HB1-A}\})$  and  $m_2(\{\text{HB2-A}\})$ . The computation result is shown in Table 6:

$$m_1 \oplus m_2(\{G\}) = 1.4367 \times (0.264 + 0.088 + 0.120) = 0.678$$

$$m_1 \oplus m_2(\{M\}) = 1.4367 \times (0.072 + 0.072 + 0.040) = 0.264$$

$$m_1 \oplus m_2(\{G, M\}) = 1.4367 \times 0.040 = 0.057$$

Denote as a new mass:  $m_3 := m_1 \oplus m_2 = m_3(\{G\}:0.678, \{M\}:0.264, \{G, M\}:0.057)$

**Phases 4 and 5** Dempster–Shafer theory wants to define upper and lower bounds of a belief probability interval from the mass assignments. “This interval contains the precise probability of a set of interest (in the classical sense), and is bounded by two non-additive continuous measures called belief (or support) and plausibility” [wiki].

**Belief Function (Bel) and Plausibility Function (Pl):** These are the other two important functions in Dempster–Shafer. Thus, phase 4 starts from after assigning/determining the BPA  $m(A)$ ; the next assignment is to compute the Belief function which is denoted as  $\text{Bel}(A)$ . Suppose given a set  $A = \{h_1, h_2, h_3\}$ . Belief  $\text{bel}(A)$  is the sum of all masses of elements which are subsets of  $A$ , and  $A$  inclusive.

$$\begin{aligned} \text{Bel}(A) = & m(h_1) + m(h_2) + m(h_3) + m(h_1, h_2) \\ & + m(h_1, h_3) + m(h_2, h_3) + m(h_1 h_2, h_3) \end{aligned} \quad (8)$$

**Table 7** BPA  $m_4(\{HB4-A\})$

HB-4	( $X=1$ ) Genuine (G)	( $X=2$ ) Malicious (M)	( $1-G-M$ ) Uncertainty (G,M)	Comments
Degree of belief computed and assigned by Fed <sub>HU</sub>				
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 ( $X=x Y=1$ )	0.20	0.60	0.20	Same DP with HB-1
BY ( $X=x Y=1$ )	0.20	0.60	0.20	Same BY with HB-1
PR ( $X=x Y=1$ )	0.20	0.60	0.20	Same PR with HB-1
Total	1.40	2.60	1.00	
Normalize	0.28	0.52	0.20	

As shown in the equation, Belief function (Support) is:

$$Bel_1 \oplus Bel_2 (\{G\}) = m_1 \oplus m_2 (\{G\}) = 0.678$$

$$Bel_1 \oplus Bel_2 (\{M\}) = m_1 \oplus m_2 (\{M\}) = 0.264$$

$$\begin{aligned} Bel_1 \oplus Bel_2 (\{G, M\}) &= m_1 \oplus m_2 (\{G\}) + m_1 \oplus m_2 (\{M\}) + m_1 \oplus m_2 (\{G, M\}) \\ &= 0.678 + 0.264 + 0.057 = 1.0 \text{ (applying equation 8)} \end{aligned}$$

Let's assume there are new pieces of evidence from Edge<sub>HU-4</sub>: which is from another state: Edge<sub>HU-4</sub>: HB-4 = {IP=162.243.149.0/24, SP=25, DP=445, BY=12 KB, PR=TCP}.

Since this is a station under State<sub>HU-2</sub>, by checking with the Fed<sub>HU</sub> there would be an existing case with similar IP address range, which implies that the Fed<sub>HU</sub> takes complete control of the case going forward. State<sub>HU-1</sub> will seize further investigation including other state stations that may later have evidence. All they do is continue forwarding evidence to Fed<sub>HU</sub>. Table 7 shows the computation result of BPA assigned to  $m_4(\{HB4-A\})$ .

As shown in the table BPA is assigned to:

$$m_4(\{HB4-A\}) = \{G:\text{Genuine}=0.28, M:\text{Malicious}=0.52, G,M:\text{Uncertainty}=0.20\}.$$

Applying Dempster rule of combination:  $m_3 \oplus m_4$  as shown in Table 8

$$m_1 \oplus m_2 (\{G\}) = 1.7452 \times (0.190 + 0.016 + 0.136) = 0.597$$

$$m_1 \oplus m_2 (\{M\}) = 1.7452 \times (0.137 + 0.030 + 0.053) = 0.384$$

$$m_1 \oplus m_2 (\{G, M\}) = 1.7452 \times 0.011 = 0.019$$

Denote as a new mass:  $m_5 := m_3 \oplus m_4 = m_5(\{G\}:0.597, \{M\}:0.384, \{G,M\}:0.019)$ .

If you observe  $m(M)$  is slightly increasing and  $m(G)$  is decreasing.

The belief function Bel(A) in phase 4 shows the minimum probability in the evidence for A directly; we need to assign the plausibility  $p(A)$ , which is now phase

**Table 8**  $m_3 \oplus m_4(\{G \text{ genuine}, M \text{ malicious}, G, M \text{ uncertainty}\})$ 

Combination: $m_3 \setminus m_4$	$\{G\}:0.28$	$\{M\}:0.52$	$\{G,M\}:0.20$
$\{G\}: 0.678$	0.190	$\emptyset: 0.353$	0.136
$\{M\}: 0.264$	$\emptyset: 0.074$	0.137	0.053
$\{G, M\}: 0.057$	0.016	0.030	0.011

$$\alpha = 1/1 - (0.074 + 0.353) = 1.7452$$

**Table 9** Independent random events from hub stations

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

5 and it is derived from the sum of all the masses of the sets  $B$  where there is an intersection with the set  $A$  [wiki]. Plausible  $Pl(A)$  amount to the maximum possible probability value (plausible maximum belief), share of the evidence for  $A$ . Let's go back to our example of a given set  $A = \{h_1, h_2, h_3\}$ .

$$Pl(\{h_1, h_2\}) = m(h_1) + m(h_2) + m(h_1, h_2) + m(h_1, h_3) + m(h_2, h_3) + m(h_1 h_2, h_3) \quad (9)$$

Closely related to these two (Belief and Plausibility) are Disbelief and Belief Interval.

Dempster–Shafer theory declares that the disbelief or doubt in  $A$ :  $Dis(A)$ , implies we are looking for  $B$  which do not intersect with  $A$ , simple  $Bel(\neg A)$ .

It's derived by the sum of all masses of the sets  $B$  that have no intersection with the set  $A$ . It's related to plausibility as the equation below shows:

$$Pl(A) = 1 - Dis(A) \quad (10)$$

The Belief Interval of  $A$  [ $Bel(A)$ ,  $Pl(A)$ ] helps determine the certainty of beliefs associated with a given subset  $A$ . The difference between  $Bel(A)$  and  $Pl(A)$  indicates the degree of certainty. A small difference indicates certainty, while large indicates uncertain in the belief. The Belief Interval should best be seen as probable certainty associated with reasoning and belief. As evidence in our model, we have reduced the computation complexity by managing the power set efficiently and in the rule of combination by representing the belief interval with the uncertainty element and if threat is imminent, the  $m(M)$  will continue to slightly grow while  $m(G)$  decreases. The

Table 10 Process breakdown (proposed DST approach breakdown)

Operation center	Edge hub	Action	XYZ: represent IP address range—1.1.1.0/24					Comments
StateHU-1	EdgeHU-1	HB-1	IP	SP	DP	BY	PR	First event. Packet does not exist at StateHU and FedHU
		Assign BPA (HB1-A)	XYZ	2525	445	12 KB	TCP	BPA assigned at the StateHU with no previous evidence ( $X=x Y=0$ )
			Genuine {G}		Malicious {M}		Uncertainty {G, M}	
		$m_1$ (HB1-A)	0.60		0.20		0.20	
EdgeHU-2		Evidence update: IP: {1.1.1.0/24} SP:{2525} DP:{445} BY:{12} PR:{TCP}	StateHU sent update to FedHU					
		HB-2	IP	SP	DP	BY	PR	New event. No related IP range at the FedHU
		Assign BPA	XYZ	135	138	12 KB	UDP	BPA assigned at the StateHU with only IP evidence ( $Y=1$ ). Others ( $X=x Y=0$ )
			Genuine {G}		Malicious {M}		Uncertainty {G,M}	
		$m_2$ (HB2-A)	0.44		0.36		0.20	
		Evidence update: IP: {1.1.1.0/24} SP:{2525, 135} DP:{445, 138} BY:{12} PR:{TCP, UDP}	More evidence: SP, DP and PR					
		Rule of combination $m_3 = m_1 \oplus m_2$	0.639		0.258		0.103	StateHU updates the FedHU

Table 10 continued

Operation center	Edge hub	Action	XYZ: represent IP address range—1.1.1.0/24					Comments
FedHU	EdgeHU-4	HB-4	IP	SP	DP	BY	PR	New event from different StateHU. Now a FedHU case
		Assign BPA	XYZ	25	445	12 KB	TCP	BPA assigned at the FedHU going forward StateHU only forward events
		$M_4(\text{HB4-A})$	Genuine {G}		Malicious {M}			Uncertainty {G,M}
		Evidence update: $m_5 = m_3 \oplus m_4$	0.28		0.52		0.20	More evidence: SP {25}
FedHU		Rule of combination	$m_5 = m_3 \oplus m_4$					Observe the slight changes
	EdgeHU-6	HB-6	IP	SP	DP	BY	PR	New event from a different StateHU. Still a FedHU case
		Assign BPA	XYZ	2525	445	12 KB	TCP	BPA assigned with existing evidence that match packet. ( $X=x Y=1$ )
		$m_6(\text{HB6-A})$	Genuine {G}		Malicious {M}			Uncertainty {G,M}
		Evidence update: $m_7 = m_5 \oplus m_6$	$m_7 = m_5 \oplus m_6$					No new piece of evidence to add
	Rule of combination		0.428		0.565		0.007	First intersection of {G} and {M}

Table 10 continued

Operation center	Edge hub	Action	XYZ: represent IP address range—1.1.1.0/24					Comments
Fed <sub>HU</sub>	Edge <sub>HU-5</sub>	HB-5	IP	SP	DP	BY	PR	New event from State <sub>HU-2</sub> . Still a Fed <sub>HU</sub> case
		Assign BPA	XYZ	135	138	12 KB	UDP	BPA assigned with existing evidence that match packet. ( $X=x Y=1$ )
		$m_6$ (HB5-A)	Genuine { $G$ }		Malicious { $M$ }		Uncertainty { $G,M$ }	
		Evidence update: IP:{1.1.1.0/24} SP:{2525, 135, 25} DP:{445, 138} BY:{12} PR:{TCP, UDP}	0.20		0.60		0.20	No new piece of evidence to add
	Rule of combination	$m_9 = m_7 \oplus m_8$	0.274		0.724		0.002	{ $G$ } decline and { $M$ } increases
Fed <sub>HU</sub>	Edge <sub>HU-3</sub>	HB-3	IP	SP	DP	BY	PR	New event from State <sub>HU-2</sub> . Still a Fed <sub>HU</sub> case
		Assign BPA	XYZ	134	136	12 KB	UDP	BPA assigned with no existing evidence for only SP and DP. ( $X=x Y=0$ )
		$m_{10}$ (HB3-A)	Genuine { $G$ }		Malicious { $M$ }		Uncertainty { $G,M$ }	
		Evidence update: IP:{1.1.1.0/24} SP:{2525, 135, 25, 134} DP:{445, 138, 136} BY:{12} PR:{TCP, UDP}	0.36		0.44		0.20	More evidence: SP {134} DP{136}
	Rule of combination	$m_{11} = m_9 \oplus m_{10}$	0.249		0.750		0.001	Degree of certainty is high

Table 10 continued

Operation center	Edge hub	Action	XYZ: represent IP address range—1.1.1.0/24					Comments
Fed <sub>HU</sub>	Edge <sub>HU-1</sub>	HB-1	IP	SP	DP	BY	PR	New event from State <sub>HU-1</sub> . Still a Fed <sub>HU</sub> case
		Assign BPA	XYZ	25	445	12 KB	TCP	BPA assigned with existing evidence that match packet. ( $X=x Y=1$ )
		$m_{12}(\text{HB1-A})$	Genuine {G}		Malicious {M}		Uncertainty {G,M}	
		Evidence update: IP: {1.1.1.0/24} SP: {2525, 135, 25, 134} DP: {445, 138, 136} BY: {12} PR: {TCP, UDP}	0.20	0.60	0.20		No new piece of evidence to add	
Federation is alerted		Rule of combination $m_{13} = m_{11} \oplus m_{12}$	$m_{12}$	0.143			0.0002	Packets are malicious
		Bel(A)			0.857			Bel and Pl are taken care of throughout
		Pl(A)			0.8572			
		B. Interval			0.0002			

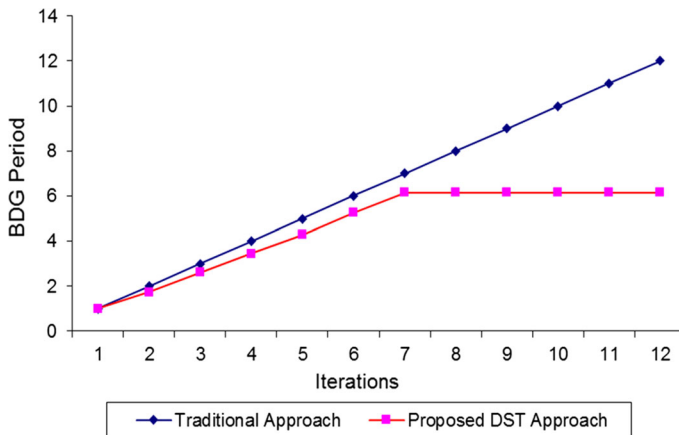


**Table 11** Summary of the iterations for Basic Probability Assignments  $m(A)$ 

Hypotheses	Basic probability assignments $m(A)$						
	State <sub>HU-1</sub>		State <sub>HU-2</sub>	State <sub>HU-3</sub>	State <sub>HU-2</sub>	State <sub>HU-1</sub>	
	Edge <sub>HU-1</sub> $m_1$	Edge <sub>HU-2</sub> $m_2$	Edge <sub>HU-4</sub> $m_4$	Edge <sub>HU-6</sub> $m_6$	Edge <sub>HU-5</sub> $m_8$	Edge <sub>HU-3</sub> $m_{10}$	Edge <sub>HU-1</sub> $m_{12}$
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

**Table 12** Summary of the iterations for Rule of Combination

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	Threat!
Malicious	0.264	0.384	0.565	0.724	0.750	0.857	
Uncertainty	0.057	0.020	0.007	0.002	0.001	0.0002	

**Fig. 8** Variation of detection for BDG using proposed approach and traditional approach versus the DST iterations

computation cost for the number of iterations can also be managed from the threatroscope table of conditional probabilities based on assigned probability values. To look at threatroscope flow of operations comprehensively from start to when information is disseminated to block generator for necessary action, let us now assume an independent random events (Table 9) at the different hub stations and see how pieces of evidence from multiple sources can help our reasoning and belief from an initial state of uncertainty about packet being threat to a degree of certainty of imminent attack.

The process breakdown is shown in Table 10. Summary of the iterations for Basic Probability Assignments  $m(A)$  is shown in Table 11, and summary of the iterations for Rule of Combination is shown in Table 12:

At some point in the iterations, as the  $m(M)$  grows closer to probability of 1.0 (in this case  $m(M)$  at 0.857 in Table 10 and in Table 11), there are enough evidences gathered to prove there are potential threats/attacks; the information is passed on through a designated special channel to block generator for consensus rule. The decision is broadcasted to the entire federation intelligence community. The necessary defense mechanisms are updated and hardened using effective information from the mirrored data (IP, PR, BY, SP, DP). The security experts and professionals in different organizations where packets have gone are notified to act accordingly in accordance with organization security policy. Lastly, all necessary operation's storage purged of records containing this IP address. Please note that similar steps are followed by monitoring egress network traffic with index on final packet destination IP address, to detect external botnets or Internet relay chat bots that may be communicating with sensitive servers without administrator's knowledge. We plotted the BDG achieved using proposed approach and the existing zero-day approach as shown in Fig. 8. The proposed approach reduces the BDG as shown in Fig. 8.

## 4 Conclusion

In this paper, we have demonstrated how to reduce BDG for cyber-attacks using the proposed blockchain-enabled federated cloud computing framework which uses Dempster–Shafer theory for monitoring the data traffic. Note that minimizing the BDG for cyber-attacks is a big concern for organizations and governments since many cyber-attacks have been gone undetected for days to years before they are detected for cyber defense. We have evaluated the proposed approach using numerical results, and results have shown that the proposed framework can reduce the BDG for cyber-attacks.

**Acknowledgements** This work was supported in part by the U.S. National Science Foundation (NSF) under Grants CNS-1658972 and CNS-1650831, and by the U.S. Department of Homeland Security (DHS) under Grant award number, 2017-ST-062-000003. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies. All co-authors have contributed in this paper.

## References

1. Wang Y-M (2009) Security challenges in an increasingly connected world
2. Government Accountability Office (GAO), Center for Science, Technology, and Engineering Report to Congressional Requesters: Internet of Things Status and implications of an increasingly connected world
3. FTC Staff Reporting, “Internet of Things: Privacy and Security in a Connected World”
4. EndGame (2016) Mind the Detection Gap: Three things SOC teams must consider for earliest detection of unknown threats
5. Hutchins EM, Cloppert MJ, Amin RM (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lead Iss Inf Warf Secur Res* 1:80

6. SANS Institute (2014) Killing advanced threats in their tracks: an intelligent approach to attack prevention
7. Silvey L (2016) Cybersecurity and data breach: impact on business in Illinois
8. Kaspersky Lab. (2017) Damage control: the cost of security breaches IT security risks special report series
9. Germano JH, Goldman ZK (2014) After the breach: cybersecurity liability risk
10. Experis (2014) Security breaches: is anyone safe?
11. Valdetero J, Zetoony D, Cave B (2014) Data security breaches incident preparedness and response
12. Ponemon Institute (2011) Reputation impact of a data breach
13. NTT Com Security (2016) Security Breaches—what’s the real cost to your business? Risk:Value Report
14. Sungard Availability Services, “The consequences of a Cyber Security Breach” Retrieved from <https://www.sungardas.com/en/cyber-security-advice/articles/the-consequences-of-a-cyber-security-breach.html>
15. Gold S (2011) Advanced evasion techniques
16. Phan B Seven key features to help you stop advanced evasion techniques at the firewall Senior Security Architect, McAfee
17. Matrosov A, Rodionov E (2013) Advanced evasion techniques by Win32/Gapz
18. OECD (2010) The changing consumer and market landscape
19. KPMG (2017) The changing landscape of disruptive technologies
20. Stratton AM, Wong KW (1997) Issues essential to world web market
21. Kehrl J (2016) Blockchain explained
22. Narayanan A, Miller A (2016) Cryptocurrencies, blockchains, and smart contracts; hardware for deep learning
23. Lemieux VL (2018) Trusting records: is blockchain technology the answer?
24. Dinh TT, Wang J, Chen G, Liu R, Ooi BC, Tan K (2017) BLOCKBENCH: a framework for analyzing private blockchain
25. Li W, Fedorov S, Sforzin A, Karame GO Towards scalable and private industrial blockchains
26. Emmadi N, Narumanchi H (2017) Reinforcing immutability of permissioned blockchains with keyless signatures. Infrastructure
27. Stiller B, Bocek T Blockchains and smart contracts—a valuable alternative for distributed data bases
28. Digitalogy (2017) All you need to know about blockchain!
29. Tapscott D, Tapscott A (2017) How blockchain will change organization
30. Ding CH, Nutanong S, Buyya R Peer-to-peer networks for content sharing
31. De Gruyter (2017) Blockchain revolution
32. Norta A (2015) Creation of smart-contracting collaborations for decentralized autonomous organization
33. Monax (2017) Explainer–blockchain. Retrieve from <https://monax.io/explainers/Blockchains>
34. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L (2017) ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability
35. Pilkington M (2015) Blockchain technology: principles and applications
36. Hull R (2017) Blockchain: distributed event-based processing in a data-centric world
37. Gervais A, Karame GO, Wust K (2016) On the security and performance of proof of work blockchains
38. Larimer D (2013) Transactions as proof-of-stake
39. Milutinovic M, Wu H, He H, Kanwal M (2016) Proof of luck: an efficient blockchain consensus protocol
40. Cachin C (2016) Architecture of the hyperledger blockchain fabric
41. Mazieres D (2016) The stellar consensus protocol: a federated model for internet-level consensus
42. Baliga A (2017) Understanding blockchain consensus models
43. ComputerWeekly. Nearly a third of malware attacks are zero-day exploits. Retrieved from <http://www.computerweekly.com/news/450415866/Nearly-a-third-of-malware-attacks-are-zero-day-exploits>
44. Digital-Guardian (2017) 91% Of cyber attacks start with a phishing email: here’s how to protect against phishing. Retrieved from <https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing>
45. Sentz K, Ferson S (2002) Combination of Evidence in Dempster–Shafer theory, April 2002
46. Horneman A, Dell N (2014) Smart collection and storage method for network traffic data
47. He J (2015) Dempster–Shafer theory of evidence

48. Rawat DB, Njilla L, Kwiat K, Kamhoua CA (2018) iShare: Blockchain Based Privacy-aware Multi-Agent Information Sharing Games for Cybersecurity. In: Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC): Communications and Information Security Symposium. Maui, Hawaii, USA, March 5–8, 2018
49. Rawat DB, Alshaikhi A (2018) “Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints.” In: Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC): Communications and Information Security Symposium, Maui, Hawaii, USA, March 5–8, 2018