iShare: Blockchain-Based Privacy-Aware Multi-Agent Information Sharing Games for Cybersecurity

Danda B. Rawat[‡], Laurent Njilla[†], Kevin Kwiat[†], Charles Kamhoua[*]
[‡]EECS Department, Howard University, Washington, DC, USA. E-mail: danda.rawat@howard.edu.
[†]US Air Force Research Lab, Cyber Assurance Branch. Email: {laurent.njilla,kevin.kwiat}@us.af.mil.
[*]US Army Research Lab, Network Security Branch. E-mail: charles.a.kamhoua.civ@mail.mil

***Abstract*—In this paper, we design, develop, and evaluate a novel information sharing (iShare) framework for cybersecurity with the goal of protecting confidential information and networked infrastructures from future cyber-attacks. The proposed iShare framework leverages the Blockchain concept used in Bitcoin systems where multiple organizations/agencies participate for information sharing (without violating their privacy) to secure and monitor their cyberspace. Note that the Bitcoin for financial transactions has already demonstrated that there is a trusted, auditable sharing with peer-to-peer communications accompanied by a public ledger. The main aim of the Blockchain-based iShare framework is to constantly collect high-resolution, cyber-attack information across organizational boundaries of which the organizations have no specific knowledge or control over any other organizations' data or damage caused by cyber-attacks. In the proposed iShare framework, the decentralized nature of the Blockchain and digitally signed transactions ensure that an adversary cannot pose as a legitimate organization/user or cannot control/hamper the system because of the digital-signatures and cannot learn anything from the public ledger that has just hashed pointers. Moreover, we analyze the security attacks by outsiders (not participating in the iShare) using a Stackelberg game.**

I. Introduction

Cyber-defense for prevention, detection, and response to cyber-attacks is an ongoing challenge that needs efforts to protect critical infrastructures and private information [1]–[4]. Complexity and scale of cyberspace and heterogeneity of networked systems make cybersecurity even more challenging. The cyber-threat information sharing across organizations could help prevent future cyber-attacks [5], [6]. The goal of low-cost, fair and privacy-aware information sharing for cybersecurity is far from being met with today's frameworks [5], [6]. The best policy should be "if you see something, say/report something" without revealing any private information so that others can take informed decisions/actions. Currently, different organizations/agencies hesitate to share their cyber-threat information with other organizations because of the following reasons: 1) absence of a common format and framework for information exchange for cybersecurity [5], [6]; 2) organizations are reluctant to share their information because of reputation concerns in case of cyber-attacks caused by negative publicity [7] and privacy concerns [8]; 3) rival organizations/agencies may misuse the shared information for their own rational/competitive advantages [6]; and 4) organizations may not see any immediate benefits of sharing their information for cybersecurity. The ITU-T Study Group 17 (SG17), consisting of cybersecurity experts, policy makers, governments and industry, has announced its cybersecurity information exchange framework [5] to enhance security in a global scale, leaving information sharing mechanisms open to researchers. There are few efforts in information sharing (e.g., [9], [10]) and in healthcare through the Fast Healthcare Interoperability Resources (FHIR) framework [11], [12], which is not applicable to our problem. Other works include in the area of Internet of Things (IoT) [13], privacy-risk control in healthcare, [14] and security in decentralized file/data storage [15], [16]. However, none of these works consider information sharing among organizations for combating cyber-attacks.

In this paper, we design, develop and evaluate a novel cybersecurity (i.e., cyber-threat and defense) information sharing (*iShare*, in short) framework for different organizations to protect their networked systems and infrastructures from future cyber-attacks. We propose to use the concept of Blockchain that is used in Bitcoin [17] system for privacy-aware information sharing and analyze the malicious actions using game theoretic approaches [18]–[20]. Note that the Bitcoin [17], [20] for financial transactions has already demonstrated that there is a trusted, auditable sharing with peer-to-peer communications accompanied by a public ledger. While sharing the information in the iShare framework, any identifiable information is anonymized, and only the summary (e.g., name and signature of the malware/virus) and cyber-defense solutions are shared with others through iShare. Note that, in all traditional data sharing applications, either we need to transfer bulky data to other organizations or we need a centralized unit to collect data. Centralization requires a single trust authority and poses a severe bottleneck problem. Transfer of bulky data could suffer significantly from limited bandwidth, and the organizations may loose their control over their own data and privacy. Because there is no universal authoritative standard, information sharing for interoperability to cross the institutional boundaries is a non-trivial task. Interoperability in the context of iShare framework is considered for structure/definition, semantics, and recommendations (such as cyber-defense solutions) necessary for protecting networked systems and infrastructures from future cyber-attacks. The iShare framework constantly collects high resolution cyber-attack information of which the organizations or users have no specific knowledge or control

Approved for public release: distribution unlimited. Case Number: 88ABW-2017-2682, Dated 09 June 2017.

Work of Danda B. Rawat was supported in part by AFRL 2017 Visiting Faculty Research Program and NSF Grants CNS 1650831 and CNS 1658972.

978-1-5386-3652-7/18/$31.00 ©2018 IEEE

over any other organizations' data or damage caused by cyber-attacks.

II. Brief Overview of Bitcoin and Blockchain

Bitcoin (developed by a programmer known as Satoshi Nakamoto – a name believed to be an alias) is based on cryptographic techniques that allows the recipient to receive money securely/genuinely without requiring a trusted third party, such as a bank or a company like PayPal [17], [21]. The Bitcoin network relies on a Blockchain – a distributed transaction public ledger – where a new block is generated by executing a consensus algorithm such as Proof-of-Work [17]. A Bitcoin client software helps users to connect to a decentralized network of other Bitcoin users through the Internet securely. It is reported in [17], [21] that the Bitcoin system is unbreakable since the mathematics involved in the Bitcoin ensures that the transactions can be easily verified, but it is practically impossible to generate malicious transactions to spend somebody else's Bitcoins.

III. The Blockchain-Based iShare Framework

The proposed iShare framework (shown in Fig. 1) uses Blockchain protocol over the public Internet as suggested/used in [16], [17]. In the iShare framework, three entities are as follows: *organizations* participating in sharing cyber-attack information to prevent future cyber-attacks; *services*, the providers of such cyber-attack related information and applications who process data; and *manager nodes*, trusted devices that maintain the Blockchain and distributed cryptographic keys. It is important to note that the organizations participating in information sharing system use changeable public keys and otherwise remain anonymous[1], but the Blockchain managers could store service profiles on the Blockchain and verify their identities.

In the proposed framework, the Blockchain accepts two types of transactions: 1) T_{accs} transaction for access control management; and 2) T_{info}, for information storage and retrieval. These transactions could be provided to organization through application program interfaces (APIs) that can be used during the software development process. A typical work-flow illustration is as follows. Each participating organization uses the proposed framework to share the information for preserving their privacy (possibly using web-based dashboard for an access as in Bitcoin [17]). When the given organization signs up, a new identity and associated permissions are generated and sent to the Blockchain using T_{acc} transaction. Cyber-attack information that is to be shared is encrypted using a shared encryption key and sent to the Blockchain using T_{info} transaction. While retrieving the information by a service or a user by querying the data using T_{info} transaction, only a pointer to the data on the public ledger is used. The Blockchain, with the help of the digital signature, verifies the organization and services. This approach for sharing information using iShare just tells whether the given organization detected any cyber-attack and would like to share, but it does not tell whether the cyber-attack was successful to damage the organization's networked systems/infrastructures or how much damage it caused if the cyber-attack was successful.

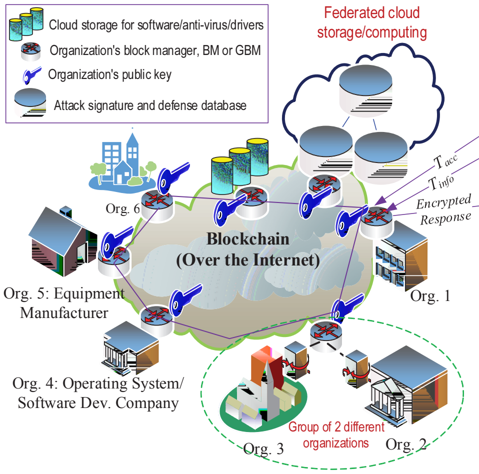
Cloud storage for software/anti-virus/drivers
Organization's block manager, BM or GBM
Organization's public key
Attack signature and defense database
Federated cloud storage/computing
User
T_{acc}
T_{info}
Encrypted Response
Services
Org. 1 user/device and services interacting with blockchain
Org. 6
Blockchain (Over the Internet)
Org. 5: Equipment Manufacturer
Org. 1
Org. 4: Operating System/ Software Dev. Company
Group of 2 different organizations
Org. 3
Org. 2

Fig. 1. A typical Blockchain-based information sharing (iShare) framework among multiple agents/organizations [16], [17].

IV. The Blockchain Based Proposed Approach

A. Blockchain and Transaction Process in iShare Framework

A typical Blockchain in iShare framework is shown in Fig. 2, which is composed of blocks with transactions. Blocks are practically impossible to manipulate without being caught since they are chained together using a hash, or a numeric digest of its content as shown in Fig. 2, that can be used to verify the integrity of the transactions. Furthermore, the hash of a block (say a block n) depends on its predecessor (say block $n-1$), as shown in Fig. 2, that makes the Blockchain immutable by malicious actions because a change in one block would require changes in the following blocks.

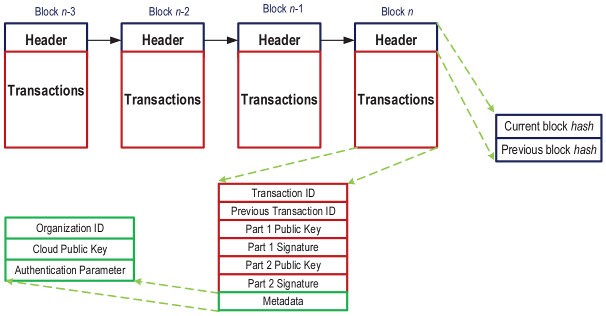

Fig. 2. A typical structure of the Blockchain [17] in iShare.

Organizations in the iShare framework, participate collaboratively to create a Blockchain by verifying and storing new transactions into it. Both the digital signature and an existence of the previous transaction in the same ledger are used to verify the legitimacy of the transactions in Blockchain . A new block is generated by executing a consensus algorithm such as Proof-of-Attack-Detection (PoAD) (see Section IV-B) similar to the Proof-of-Work [17]. The BM or GBM[2] then

[1] Hiding identity or private information of the participating organization, particularity in case of cyberattack, could save them from any socioeconomic/reputation damages caused by the cyber-attacks.

[2] In case of partnering organizations, they can nominate a group leader (based on their business MoU) as a block manager and named as a group block manager (GBM). The gateway of each organization (e.g., org. 2 and org. 3) will be connected to a GBM as shown in Fig. 1, and GBM maintains the public key.

creates a new block and forwards it to other BMs for block verification, which allows all BMs to at least contribute to a transaction to digitally sign the block to endorse its correctness. Then, the block is returned to the original BM, which then adds the block to its local Blockchain. Finally, a new Blockchain is distributed to all nodes in the system. The proposed Blockchain network comprises different organizations including equipment manufacturers, computers, operating system/software providers, security patch or anti-virus providers, IDS/IPS service providers, and cloud storage providers or devices such as laptops, cell phones, tablets, cyber-physical system devices, and IoT devices.

In the iShare framework, software/anti-virus providers and computers or IoT-devices of a given organization can share the data in a distributed manner (as in Fig 1). In case of many similar devices (e.g., computers) in a given organization, a block manager BM is chosen, and it manages the public Blockchain to store iShare transactions. Furthermore, each organization with private networked systems (e.g., computer network, smart building network, etc.) maintain a private, centrally managed Blockchain, aka private ledger, containing all transactions related to the given organization. Then, the private ledger is linked to the block manager, BM, by using a hash that contains the hash of the public Blockchain . Note that each organization is centrally managed by a trusted device known as a local manager, which is integrated in the Internet gateway and maintains a local private ledger that connects the organization to iShare network. All communications to and from the organization are routed through the local manager that is integrated in the Internet gateway. This assumption is closely analogous to Port Address Translation (PAT) or Network Address Translation (NAT) in traditional IPv4 networks.

B. Cyber-Attack Detection and Sharing the Information

Each organization is assumed to be responsible for deploying the recent updates, security patches, and updated operating systems based on Evaluation Assurance Level (EAL) standard for all devices [22], firewalls and IDS/IPS (e.g., [3], [23], [24]), and for sharing the detected cyber-attack information or attack-signature (with possible countermeasures) through iShare framework[3]. This sharing is done through Blockchain after verifying the attack with the help of equipment manufacturer, operating systems and/or anti-virus developers that are participating in iShare. For instance, attack detected by an organization that had Microsoft Windows 8 with firewall and Norton anti-virus on Dell computers should be verified through Blockchain by Microsoft, Dell and Norton companies to reach to the consensuses. This process is known as PoAD. This process is initiated first by the organization who detects an attack, and it is considered as a source of information. To avoid duplicate reporting (in case of two or more organizations detecting the same attack at the same time and reporting it through Blockchain), cloud storage chooses the one who has countermeasure, if any, and discards the rest. Once the cyber-defense solution is available to the cloud storage, it is published like other software or updates so that all organizations can download and deploy to protect their networks/infrastructures as discussed in Section IV-C.

In this setup, malicious organizations are those who do not participate in a timely and positive way in Share. For instance, 1) anti-virus companies who do not develop security patches to *known* vulnerabilities or create viruses in order to sell their anti-virus product and 2) operating system developers who leave *known* loopholes or back-doors open for a long time without providing security patches, are also regarded as malicious organizations.

C. Deploying Cyber-Defense Solutions and Updates

Deploying robust cyber-defense solutions to prevent cyber-attacks is one of the most critical security challenges in any networked systems. In iShare, when a given software provider creates a new version or a patch, it initiates the process for sharing/transferring using Blockchain by considering it as a source to store the updates software/patches in the cloud that is accessible to all participating organizations. Then, the software provider creates a multi-signature transaction where its own part 1 key and signature (generated using signed hash) are stored. The software binary file is assumed to be stored in the cloud for users to download. Thus, the hash can be verified by the other participating devices to ensure the data integrity. The key of the equipment manufacturer is written in the part 2 field of the transaction. To forward the received update to all devices or networks within the organization, both keys and signatures for part 1 and 2 of Blockchain should be matched. Otherwise, it is forwarded to other organizations' gateways. Upon receiving the transaction from the gateway of a given organization, each networked device verifies it by matching the key in the transaction with its equipment manufacturer's key. For a legitimate software update, network or networked devices download the software updates directly from the cloud using authentication parameters available in metadata of the received multisignature transaction, as shown in Fig. 2. The signed hash of both the software provider and equipment manufacturer can be used to verify that it was not altered. Similarly, when a cyber-attack is detected by one of the participating organizations, which is then verified using Blockchain with the help of an equipment manufacturer, operating system and/or anti-virus developers participating in iShare, the attack threat information as well as cyber-defense solutions (if developed or available) are shared, which will then be stored in the cloud-based information base of iShare.

V. Analysis of Cyber-Attack/Defense Games

A. Cross-Group Attack Game in Blockchain-based iShare Framework: One-Way Attack

In an iShare framework, similar organizations, such as airlines (Delta, American, KLM, Thai, Virgin Airlines, etc.), hospitals (public and private), hardware/software companies (Microsoft, HP and Dell), banks (Bank of America, Citi Bank, DB), etc., can form a Group and work together for the group's benefit that provides profit to them individually.

For the sake of simplicity, we consider two groups: Group 1 and Group 2, with N_1 and N_2 (total $N = N_1 + N_2 + ...$) number of member organizations, respectively, sharing their

[3] When an organization does not follow the standard guidelines, it will be treated as a malicious agent/organization since it is indirectly helping attackers or is not helping to secure the system from possible attacks.

cyber-attack information through the iShare framework. The benefit utility they achieve in a group is shared among group members when they work in a group. Although motivated by the Blockchain-based Bitcoin systems, there is no immediate reward/payment for organizations individually, but they get rewarded equally after completion of a task [17], [20].

Some group members (say from Group 2) could form a sub-group (could be sub-group of just one organization) and act as an organization to cross-participate in another group (say Group 1) or not participate in legitimate block formation in their own Group 2 by not releasing the detected cyber-attack information or by not developing a security patch for a known security breach. The aim of the one-way attack is to reduce the utility/interest of Group 1 by using sub-group of $X_{2\to1}$ ($\leq N_2$) members from Group 2, where $X_{2\to1}$ members of Group 2 could try to hinder the Blockchain building process. For Blockchain-based iShare, the direct utilities of group k can be expressed as

$$U_k \quad = \quad \log(\sigma_k + \gamma_k), \quad k = 1, 2, \tag{1}$$

where $\log(\sigma_k + \gamma_k)$ is a generic convex function of γ_k for each group k and typical value of $\sigma_k = 1$. $X_{2\to1}$ members of Group 2 participate in Group 1, who are considered malicious members since they do not participate in their own group but participate in another group. In this case, the total number of organizations who legitimately participate in the Blockchain process is $N - X_{2\to1}$. Then, γ_1, i.e., the quality factor in (1) of the Blockchain generation process for the Group 1 can be expressed as

$$\gamma_1 \quad = \quad \frac{N_1}{N_1 + (N_2 - X_{2\to1})} = \frac{N_1}{N - X_{2\to1}}. \tag{2}$$

For Group 2, $X_{2\to1}$ members do not participate in the process, leaving $N_2 - X_{2\to1}$ organizations in the group. Thus, γ_2, i.e., the quality factor in (1) of the Blockchain-generation process for the Group 2 can be expressed as

$$\gamma_2 \quad = \quad \frac{N_2 - X_{2\to1}}{N_1 + (N_2 - X_{2\to1})} = \frac{N_2 - X_{2\to1}}{N - X_{2\to1}}. \tag{3}$$

As mentioned earlier, there is no mechanism to reward the legitimate members only, all members of a given group and cross-participating members get rewards equally. Thus, the Group 1 members share their utility with its legitimate members and the members from Group 2 that intruded it. Next, the utility density for Group 1 can be expressed as

$$u_1 = \frac{U_1}{N_1 + X_{2\to1}} = \frac{\log\left(1 + \frac{N_1}{N - X_{2\to1}}\right)}{N_1 + X_{2\to1}} \tag{4}$$

Similarly, the utility density for Group 2 after considering the contributions of $X_{2\to1}$ (ı.e., $X_{2\to1} \times u_1$ as in [17], [20]) can be expressed as

$$u_2 = \frac{U_2 + X_{2\to1} \times u_1}{N_2} = \frac{\log(\frac{N_2 - X_{2\to1}}{N - X_{2\to1}}) + X_{2\to1}\frac{\log\left(1 + \frac{N_1}{N - X_{2\to1}}\right)}{N_1 + X_{2\to1}}}{N_2} \tag{5}$$

For finite number of organizations participating in iShare, the game always has a Nash equilibrium with $X_{2\to1}$ value, where

$$\frac{\partial u_1}{\partial X_{2\to1}} = 0, \qquad \text{and} \qquad \frac{\partial u_2}{\partial X_{2\to1}} = 0. \tag{6}$$

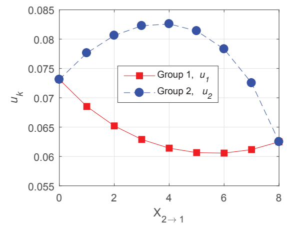

Fig. 3. Variation of expected utility vs the number of cross-group participants, where $N = 16$ organizations/users are equally divided into two groups.

To evaluate the performance of the game, we simulated a scenario with a different number of cross-group participants, $X_{2\to1}$, where $N = 16$ organizations/users are equally divided into two groups. Fig. 3 shows the variation of group utilities of two groups for different number of organizations, $X_{2\to1}$, participating in cross-group activities. When $X_{2\to1}$ increases, the utility of Group 1 decreases until 50% of the organizations cross-participate. However, the utility increases for group 2 because they get rewards from both cross-group participation and their own group as shown in Fig. 3. When all group members of group 2 cross-participate in group 1, that is, $X_{2\to1} = N_2$, they get the contribution of the subgroup, which is less than they get from legitimate participation. Thus, we could conclude that the best response is not to participate in cross-group activities, but a dominant strategy of the game would be cross-group participation with all members of the group.

B. Cross-Group Attack Game in Blockchain-Based iShare Framework: Two-Way Attack

In this attack, a sub-group of Group 1 of size $X_{1\to2} < N_1$ acts maliciously or participates in Group 2, and a sub-group of Group 2 of size $X_{2\to1} < N_2$ acts maliciously or participates in Group 1. The direct utility of group k can be expressed as

$$U'_k \quad = \quad \log(1 + \gamma'_k), \qquad k = 1, 2, \tag{7}$$

where γ'_k can be calculated as follows.

$$\gamma'_k \quad = \quad \frac{N_k - \sum_{\forall j} X_{k\to j}}{N - \sum_{\forall j} X_{k\to j} - \sum_{\forall j} X_{j\to k}} \tag{8}$$

Here, $X_{k\to j}$, and $X_{j\to k}$ represent the total number of cross-participating organizations from group k to j and j to k respectively. When we consider two groups $k = 1, 2$, we have

$$\gamma'_1 \quad = \quad \frac{N_1 - X_{1\to2}}{(N_1 - X_{1\to2}) + (N_2 - X_{2\to1})} = \frac{N_1 - X_{1\to2}}{N - X_{1\to2} - X_{2\to1}} \tag{9}$$

$$\gamma'_2 \quad = \quad \frac{N_2 - X_{2\to1}}{(N_1 - X_{1\to2}) + (N_2 - X_{2\to1})} = \frac{N_2 - X_{2\to1}}{N - X_{1\to2} - X_{2\to1}} \tag{10}$$

Total utility is divided among participating organizations, that is, members of a given group and members of sub-groups that are cross-participating from other groups. Then, the utility density for the group k can be expressed as

$$u'_k \quad = \quad \frac{U'_k + \sum_{\forall j} X_{k\to j} \times u'_j}{N_k + \sum_{\forall j} X_{j\to k}} \tag{11}$$

TABLE I
EXPECTED UTILITY OF EACH GROUP.

	Group 2 - No attack	Group 2 - Attack
Group 1 - No attack	$u_1^{'}, u_2^{'}$	$u_1^{''} < u_1^{'}, u_2^{''} > u_2^{'}$
Group 1 - Attack	$u_1^{''} > u_1^{'}, u_2^{''} < u_2^{'}$	$u_1^{''} < u_1^{'}, u_2^{''} < u_2^{'}$

When we consider 2 groups $k = 1, 2$, we will have utility densities as

$$u_1' = \frac{U_1' + X_{1\to 2} \times u_2'}{N_1 + X_{2\to 1}} \qquad (12)$$

$$u_2' = \frac{U_2' + X_{2\to 1} \times u_1'}{N_2 + X_{1\to 2}} \qquad (13)$$

Solving (12) and (13) for u_1 and u_2, we get,

$$u_1' = \frac{N_2 U_1' + X_{1\to 2}(U_1' + U_2')}{N_1 N_2 + N_1 X_{1\to 2} + N_2 X_{2\to 1}} \qquad (14)$$

$$u_2' = \frac{N_1 U_2' + X_{2\to 1}(U_1' + U_2')}{N_1 N_2 + N_1 X_{1\to 2} + N_2 X_{2\to 1}} \qquad (15)$$

As players are allowed to play a mixed strategy and the number of players N_1 and N_2 are finite, the game always has a Nash equilibrium with $X_{1\to 2}$ and $X_{2\to 1}$ values, where

$$\frac{\partial u_1'}{\partial X_{1\to 2}} = 0 \quad \text{and} \quad \frac{\partial u_2'}{\partial X_{2\to 1}} = 0 \qquad (16)$$

This game with rational players looks like a zero-sum game, where loss (or gain) in one group's utility is proportional to the gain (or loss) of the other group's utility. For a two-way, cross-group participation game, the strategy space of the players can be defined as $\mathcal{S} = \{\textit{Do not attack, Attack}\}$. The outcome of the game and (dominant) strategies for both groups/players are summarized in Table I and are also summarized with an example of values in Fig. 4, where utilities with 'attack' and 'no attack' are denoted as $u_k^{''}$ and $u_k^{'}$ for $k = 1, 2$, respectively. Utilities of both groups would be higher if they choose not to attack, however, the dominant strategies for both groups are to attack.

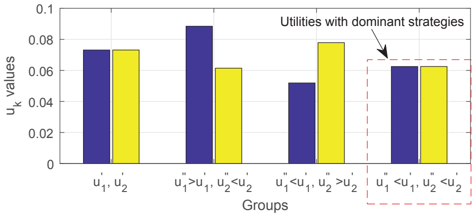

Fig. 4. Example of expected group utilities.

C. Stackelberg Game for Cyber-Attack and Defense Analysis

In previous sub-sections, we assumed that the organizations participate in iShare framework, but some of them act maliciously to contribute negatively by not sharing the known attack information with other participating organizations. However, in many cases, attackers do not participate in the information sharing process at all but just launch the cyber-attacks – these attackers are regarded as outsiders. Without loss of generality, based on the past attacks and success rate of the recovery from the attacks, the security level of an organization k can be considered as $0 \leq \ell_k \leq 1$, $\forall k$ (where security level is directly proportional to a system hardening investment of the organization and the average security level of the organization (among N organizations) can be expressed as $\overline{\ell}_k = \frac{1}{N}\sum_{k=1}^{N} \ell_k$. Next, the probability of cyber-attacks for a given organization k can be expressed as $p_k = (1 - \ell_k)(1 - \overline{\ell}_k), \forall k$.

These cyber-attacks and defense actions can be modeled as a game to study conflicting strategies. A typical multi-agent game for cybersecurity can be formulated as follows. Attackers take malicious actions to attack the organizations based on defenders'/organizations' strategies. Then, the defending organizations to defend attacks take actions based on attackers strategies and share the detected cyber-attack information through the iShare. This game can be formulated as a Stackelberg game with leader and follower sub-games [18], [19]. Note that organizations are expected to follow the government and industry standard practices for hardening their networked systems based on the recent attacks and known vulnerabilities. Thus, in the proposed Stackelberg game, legitimate organizations are treated as followers since they act on cyber-attacks or known vulnerabilities and the attackers are treated as the leaders who attack the organizations' networked information systems.

Defenders/Follower Sub-Game: In this sub-game, followers try to minimize the effect of any cyber-attack by hardening the networked information system and sharing the known cyber-attack information. Based on security level and investment of a given organization, an attacker chooses a strategy a_k, $\forall k$ with the expected level of security impact $i_{m,k}$ to a victim organization k. Then, the organization may suffer from the attack or may not, which depends on both impact level $i_{m,k}$ and organization's socioeconomic tolerance level. Thus, for a given organization k, the goal is to minimize the attack impact that can be achieved by solving the following optimization problem:

$$\begin{aligned} \underset{\Psi_k, p_k, \forall k}{\text{minimize}} \quad & O_{U_k} = p_k S_k \beta_k \log(1 + \Psi_k) \\ \text{subject to} \quad & \sum_{\forall m} i_{m,k} \Psi_k \leq \overline{B}_k; \\ & i_{m,k} \geq 0; \quad \forall m, \forall k; \\ & \Psi_k \geq \overline{\Psi}_k; \quad \forall k; \\ & S_k \in \{1, 0\}, \quad s_k > 0, \quad \text{and} \quad c_k > 0; \quad \forall k, \end{aligned} \qquad (17)$$

where $\overline{B}_k$ is the maximum tolerable socioeconomic (reputation and budget) level for the organization k because of the cyber-attacks, $i_{m,k}$ is the targeted impact level of cyber-attack m to a given organization k using an attack strategy a_k, $\Psi_k \geq \overline{\Psi}_k$ is each organization's investment level constraint for cyber-defense that accommodates the cost of hardening the system and sharing the cyber-attack information through iShare etc., S_k is the binary strategy set (i.e., share = 1 or not share = 0, but we consider that legitimate organization share the information, thus, $S_k = 1$), $s_k > 0$ and $c_k > 0$, respectively, represent the cost of sharing the information and cost of participating in the information sharing through iShare. When s_k and c_k are incorporated in the investment Ψ_k, these constraints can be relaxed. The β_k is the utility scaling factor, and, without loss of generality, we consider $\beta_k = 1$ for simplicity. Then, the problem (17) can be expressed as

$$\begin{aligned} \underset{\Psi_k, p_k, \forall k}{\text{minimize}} \quad & O_{U_k} = p_k \log(1+\Psi_k) \\ \text{subject to} \quad & \sum_{\forall m} i_{m,k}\Psi_k \leq \overline{B}_k; \\ & i_{m,k} \geq 0; \quad \forall m, \forall k; \\ & \Psi_k \geq \overline{\Psi}_k; \quad \forall k; \end{aligned} \tag{18}$$

The problem (18) is convex in Ψ_k, and thus the problem has unique optimal solution. We can solve the problem (18) using Lagrangian method. Let us consider λ_1, λ_2 and λ_3 as Lagrange's multipliers for different constraints in (18). Then, we can express the Lagrangian equivalent of (18) as

$$\begin{aligned} L_{O_{U_k}} = \; & p_k \log(1+\Psi_k) - \lambda_1 \left(\sum_{\forall m} i_{m,k}\Psi_k - \overline{B}_k \right) \\ & + \lambda_2 \left(i_{m,k} - 0 \right) + \lambda_3 \left(\Psi_k - \overline{\Psi}_k \right) \end{aligned} \tag{19}$$

and the complementary Slackness conditions for (19) are

$$\lambda_1 \left(\sum_{\forall m} i_{m,k}\Psi_k - \overline{B}_k \right) = 0, \tag{20}$$

$$\lambda_2 (i_{m,k} - 0) = 0, \tag{21}$$

$$\lambda_3 \left(\Psi_k - \overline{\Psi}_k \right) = 0, \tag{22}$$

$$\lambda_1 > 0, \lambda_2 \geq 0, \lambda_3 \geq 0, \tag{23}$$

where $\lambda_2 = 0$ since $i_{m,k}$ of an attack should be greater than zero, otherwise there is no point of attacking the organization, and $\lambda_3 \geq 0$ since there should be minimum investment for cyber-defense, $\Psi_k \geq \overline{\Psi}_k$, for protecting the organization. The first-order optimality of (19) can be obtained by differentiating $L_{O_{U_k}}$ w.r.t. Ψ_k and equating it to zero; that is,

$$\frac{\partial L_{O_{U_k}}}{\partial \Psi_k} = 0, \quad \forall k \qquad \Rightarrow \qquad \frac{p_k}{1+\Psi_k} - \lambda_1 \sum_{\forall m} i_{m,k} + \lambda_3 = 0. \tag{24}$$

When investment level is greater than the minimum investment level, we have $\lambda_3 = 0$. Then, (24) can be expressed as

$$\Psi_k = \frac{p_k}{\lambda_1 \sum_{\forall m} i_{m,k}} - 1 \tag{25}$$

By substituting (25) into (20), after few steps, we get

$$\lambda_1 = \frac{p_k}{\sum_{\forall m} i_{m,k} + \overline{B}_k} \tag{26}$$

After substituting (26) into (25), we get

$$\Psi_k = \frac{\sum_{\forall m} i_{m,k} + \overline{B}_k}{K i_{m,k}} - 1, \quad \forall k, \tag{27}$$

which is the best response of the follower sub-game for the given attack strategies.

Attacker/Leader Sub-Game: Next, attackers attack the organizations without cooperating with each other with an aim of halting the service provided by the victim organization, gaining unauthorized access to private information or gaining economical benefits. The non-cooperative attacker game (AG) can be represented as $AG = \langle \mathcal{K}, \{\mathcal{A}_k\}_{k \in \mathcal{K}}, \mathcal{U}_k(.) \rangle$, where three components of the game are as follows: $\mathcal{K} = \{1, 2, \ldots, K\}$ is the set of active players/attackers where each attacker could attack a single or multiple organizations; $\mathcal{A}_k$ is the set of attacking strategies $\{a_1, a_k, ..., a_K\}$; and $\mathcal{U}_k(.) : \{\mathcal{A}_1 \times .. \times \mathcal{A}_K\}$ is the utility/payoff given in (28) that maps strategy spaces to a positive real number. Then, the utility optimization problem for an attacker with a strategy a_k can be expressed as

$$\underset{a_k, \forall k}{\text{maximize}} \quad A_{U_m}(a_k, \mathbf{a_{-k}}) = \sum_{k=1}^{N} p_k (1 - i_{m,k}(a_k))(1 - \Psi_k) \tag{28}$$

$$\begin{aligned} \text{subject to} \quad & \{a_k\} \neq \emptyset, \quad \forall k, \\ & \overline{i}_{m,k} \geq i_{m,k} \geq 0, \quad \forall m, \forall k. \\ & p_k > 0, \quad \forall k. \end{aligned} \tag{29}$$

Here, $\{a_k\} \neq \emptyset$ implies that there should be at least one attack strategy to maximize attacker's utility. The attack impact maximization problem (28) can be solved by Lagrangian method by expressing (28) with its constraints in (29) and taking the first derivative and equating it to zero to get the impact level value. Then, for an iterative approach, the *expected* impact level of a attack can be updated as in (30). As discussed earlier, in this paper, we consider that launching a cyber-attack a_k against a given organization is accompanied by the following: 1) denial-of-service attack, i.e., halting regular business operations $r_b = [0, 1]$ (attack in the computer system of airline company could result in flight cancellations/delays, etc.); 2) cause slow response to customers'/users' requests $r_d = [0, 1]$; and 3) reduction in reputation of a given organization $r_r = [0, 1]$. Thus, the *expected* impact level of a cyber-attack m to a given organization k (i.e., attack a_k) can be expressed as

$$i_{m,k}(a_k) = \max\{\eta_{m,k} r_b(m,k) + \theta_{m,k} r_d(m,k) + \mu_{m,k} r_r(m,k) - \ell_k, \overline{i}_{m,k}\} \tag{30}$$

where $0 \leq \eta_{m,k} \leq 1$, $0 \leq \theta_{m,k} \leq 1$ and $0 \leq \mu_{m,k} \leq 1$ are the weighting factors for halting regular business operations, causing slowness in responding to customers'/users' requests and reduction in reputation levels, respectively, due to the cyber-attack m by taking an attack action a_k to victim organization k. Note that when the *expected* impact level in (30) is 0 or negative, there is no point of targeting an organization by a cyber-attack. $\overline{i}_{m,k} = 1$ is the maximum. level. We corroborate the existence and uniqueness of the equilibrium point through simulation results in the following section.

Performance Evaluation: In order to corroborate our analysis, we set up 1) a simulation scenario with four organizations with different security and investment levels, and 2) an attacker with four different expected attack impact levels. To see the variation in results, we consider an iterative approach where an attacker, with different random attack levels, starts attacking four organizations with $\overline{B}_k = 0.1, \forall k$ and random initial security levels. Then, organizations start calculating their utilities based on their security levels, cyber-defense and investment levels, and attacker's expected impact. The maximum *effective* attack-impact levels could be one or 100%, but we consider for simulation that $\overline{i}_{m,k} = \{0.27, 0.26, 0.24, 0.25\}$.

We have plotted the utilities of four different organizations vs iterations, security/investment levels vs iterations, attacker's

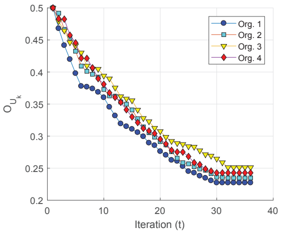

Fig. 5. Expected utility of different organizations with different security/investment levels vs. iterations.

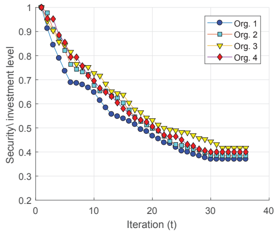

Fig. 6. Expected security/investment levels caused by the impact of cyber-attack vs. iterations

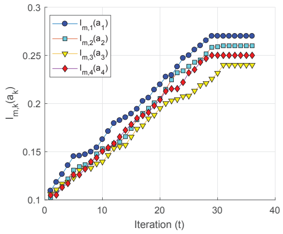

Fig. 7. Variation of attack impact $i_{m,k}$ vs. iterations.

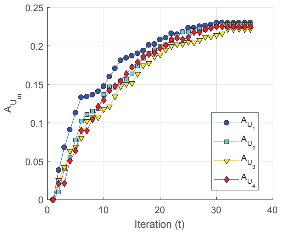

Fig. 8. Variation of expected utility of attacker vs. the iterations.

expected impact levels vs iterations, and attacker's utilities for different expected attack-impact levels vs iterations, as shown in Fig. 5, Fig. 6, Fig. 7, and Fig. 8, respectively. Fig. 5 shows that the organizations' expected utilities decrease for increasing iterations because of the increasing attack-impact levels from the attacker for a given security and investment level as shown in Fig. 7. Similarly, increase in attack-impact levels from the attacker results in a decrease in security level of the organizations for the given investment levels, as shown in Fig. 6. Attackers take different actions a_k with different attack-impact levels for different victim organizations, as shown in Fig. 7. Fig. 7 shows that organization 3 has the lowest expected attack impact from the attacker that results in the highest security level for a given investment of the organization, as shown in Fig. 5. Furthermore, Fig. 8 shows that the attacker gets the highest (or lowest) utility with the highest (or lowest) attack-impact level for organization 1 (or organization 3) that had the lowest (or highest) security and investment level as shown in Fig. 5. Simulation results show that the game has the uniqueness equilibrium point where the game has converged.

VI. Conclusion

In this paper, we have studied an information sharing (iShare) framework for multiple organizations to protect them from future cyber-attacks. The proposed framework leverages the Blockchain concept used in Bitcoin system (aka a trusted, auditable public ledger) to enhance data integrity and protecting privacy. The Blockchain-based iShare ensures that the participating organizations (i.e., agents/users) own and control their data without requiring a trusted third party for security and privacy. We have analyzed games where some of the participating organizations act maliciously to mislead the cyber-defense or get benefit from the system by cross-participation. We have also presented a Stackelberg game-based cyber-attack and defense analysis when outsiders attack the organizations. We have formally analyzed the games and validated them through numerical results obtained from extensive simulations.

References

[1] R. C. Armstrong, J. R. Mayo, and F. Siebenlist, "Complexity science challenges in cybersecurity," *Sandia National Laboratories SAND Report*, 2009.

[2] D. Rawat and C. Bajracharya, *Vehicular Cyber Physical Systems: Adaptive Connectivity and Security*. Springer, 2016.

[3] D. B. Rawat and C. Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, Oct 2015.

[4] D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, 2017.

[5] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird *et al.*, "CYBEX: The cybersecurity information exchange framework (x.1500)," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 5, pp. 59–64, 2010.

[6] Securing the Homeland Through Information Sharing and Collaboration, Report on Department of Homeland Security Information Sharing Strategy, April 18, 2008. URL (accessed on May 21, 2017): https://goo.gl/IoUx1n.

[7] Why Cyber-Security Is Central to Your Reputation, URL (accessed on May 21, 2017): http://www.cioinsight.com/it-management/expert-voices/why-cyber-security-is-central-to-your-reputation.html.

[8] C. Clifton, M. Kantarciolu, A. Doan, G. Schadow, J. Vaidya, A. Elmagarmid, and D. Suciu, "Privacy-preserving data integration and sharing," in *Proc. of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery*. ACM, 2004, pp. 19–26.

[9] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 7341–7346.

[10] R. Garrido-Pelaz, L. Gozalez-Manzano, and S. Pastrana, "Shall we collaborate? A model to analyse the benefits of information sharing," *arXiv preprint arXiv:1607.08774*, 2016.

[11] B. Tim, "Principles of Health Interoperability HL7 and SNOMED," *Health Informatics*, 2010.

[12] Y. Lindell and B. Pinkas, "Secure multiparty computation for privacy-preserving data mining," *Journal of Privacy and Confidentiality*, vol. 1, no. 1, p. 5, 2009.

[13] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. ACM, 2017, pp. 173–178.

[14] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, p. 218, 2016.

[15] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk a blockchain-based decentralized file storage application," Technical Report. http://metadisk.org/metadisk. pdf, Tech. Rep., 2014.

[16] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*, 2015, pp. 180–184.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, 2008," *URL (accessed on May 21, 2017): http://www.bitcoin.org/bitcoin.pdf*, 2008.

[18] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness," *J. Artif. Intell. Res.(JAIR)*, vol. 41, pp. 297–327, 2011.

[19] T. Başar and R. Srikant, "A Stackelberg network game with a large number of followers," *Journal of Optimization Theory and Applications*, vol. 115, no. 3, pp. 479–490, 2002.

[20] I. Eyal, "The miner's dilemma," in *2015 IEEE Symposium on Security and Privacy (S&P)*, 2015, pp. 89–103.

[21] Tom Simonite, "What Bitcoin Is, and Why It Matters," MIT Technology Review, May 25, 2011. URL (Accesed on June 1, 2017): https://goo.gl/Btqrfc.

[22] D. E. R. Denning, *Information Warfare and Security*. Addison-Wesley Reading, 1999, vol. 4.

[23] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[24] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.