M2M-REP: Reputation System for Machines in the Internet of Things

Muhammad Ajmal Azad[a], Samiran Bag[a], Feng Hao[a], and Khaled Salah[b]

[a]*School of Computing Science, Newcastle University, Newcastle Upon Tyne, United Kingdom*
[b]*ECE Department, Khalifa University, United Arab Emirates*

Abstract

In the age of IoT (Internet of Things), Machine-to-Machine (M2M) communication has gained significant popularity over the last few years. M2M communication systems may have a large number of autonomous connected devices that provide services without human involvement. Interacting with compromised, infected and malicious machines can bring damaging consequences in the form of network outage, machine failure, data integrity, and financial loss. Hence, users first need to evaluate the trustworthiness of machines prior to interacting with them. This can be realized by using a reputation system, which evaluates the trustworthiness of machines by utilizing the feedback collected from the users of the machines. The design of a reliable reputation system for the distributed M2M communication network should preserve user privacy and have low computation and communication overheads. To address these challenges, we propose an M2M-REP System (Machine to Machine REPutation), a privacy-preserving reputation system for evaluating the trustworthiness of autonomous machines in the M2M network. The system computes global reputation scores of machines while maintaining privacy of the individual participant score by using secure multi-party computation techniques. The M2M-REP system ensures correctness, security and privacy properties under the malicious adversarial model, and allows public verifiability without relying on a centralized trusted system. We implement a prototype of our system and evaluate the system performance in terms of the computation and bandwidth overhead.

Keywords: Machine to Machine Communications, Edge Computing, Internet of Things, Reputation System, Privacy-Preservation, Secure Computation, Trust

1. Introduction

The Internet of Things (IoT) is a system of interconnected and autonomous computing devices (objects, things, sensors, devices, machines, vehicles etc.) that has the ability to perform specific functions without requiring human intervention. The projected forecast for the IoT ecosystem shows that the number of connected IoT devices across the globe will grow up to more than 26 billion by the year 2020 [1],[2]. The projected forecast shows that there will be a large number of interconnected Vehicles and Machines [3] in the IoT ecosystem, establishing an Internet of Vehicles (IoV) and an Internet of Machines (IoM) networks. Specifically, there will be more than one billion Machine-to-Machine (M2M) devices and more than 250 million connected vehicles by the year 2020 [3, 4, 5]. The emergence of new telecommunication technologies (e.g. 4G, 5G networks) has also enabled mobile edge providers to provide real-time computing resources and services to the vehicles, IoT devices, and consumers near their premises. Vehicles and Machines in the M2M network interact directly with each other to gather information about the road conditions e.g. traffic congestion, roadside accidents etc. These nodes can also interact with the edge computing nodes or edge-base stations to outsource their time-sensitive computation tasks or have value-added services from the edge nodes e.g. for entertainment.

In the edge computing setup, edge nodes and value-added servers are typically deployed near the premises of their consumers to provide delay tolerant services. In this particular setting, nodes and machines are distributed and autonomous, thus can be exposed to attacks such as injection of malware to the unsecured machines, physical tampering of the machines, and attacks on the core network [6]. The compromised malicious machines not only disseminate unwanted content (i.e. trojans, worms, viruses, fake files, spam etc.) [7] to their users but also pose a threat to secretly collecting private information of users for malicious purposes. To protect consumers from having an interaction with the malicious actors in the network, there is a need to build a secure and reliable reputation system for the autonomous and distributed M2M and IoT systems [6]. The reputation system would enable machines and consumers to evaluate the trustworthiness of any machine in the network [8, 9, 10, 11] prior to initiating a request to the machine, based on the past behavior of machine towards its users.

Reputation systems have been widely used in a number of domains to evaluate the trustworthiness of nodes e.g. in the vehicular ad-hoc networks to evaluate the trustworthiness of vehicles [9, 10, 11], P2P (peer to peer) networks [12, 13, 14] to evaluate the trustworthiness of peers providing content, in an online marketplace for evaluating the

reputation of consumers and sellers [15, 16, 17, 18], and computing reputation of users in a service provider network (email, telephony, social networks) [19, 20, 21, 22] for identifying malicious users in a collaborative way. A reputation system can operate in two modes: the centralized mode -- having a centralized trusted authority for collecting and processing ratings submitted by the participants, and the distributed mode -- aggregating ratings in a completely distributed way. The centralized systems [17, 15] are mainly used in the online marketplaces, but a centralized trusted system poses a threat to the privacy of the participants i.e. identities and rating scores are exposed to the central entity. The distributed reputation systems [23, 14, 24] have been widely used in a P2P network but these systems have extensive network resources and also have a threat to the privacy of participants. In order to protect the privacy of participants (vehicles, devices or users), the reputation system can provide anonymity through the identity anonymization [25, 26, 27]. However, anonymization is vulnerable to de-anonymization techniques [28, 29]. The privacy of feedback provider can be protected using distributed trusted third parties and cryptographic tools [30, 13, 31, 32, 33, 34]. These systems either depend on a set of trusted peers [13, 35, 30] or the centralized system [34, 12] for the privacy protection. However, finding a set of trusted peers may prove difficult in a decentralized network.Furthermore, most of the existing systems are designed for semi-honest participants (participants who are honest in providing feedback) [13, 36, 35, 34], which could be easily circumvented in practice.

The reputation system for the distributed IoV and M2M systems should have following properties: 1) The design should protect the private information of participants providing the feedback scores; 2) it should not have any trusted centralized system for the management of cryptographic parameters and collection of feedback; 3) it should not have excessive computation and communication overhead in order to make the system suitable for resource-constrained devices, and 4) the computation should be verifiable by all participants.

To address these challenges, this paper describes the design of an M2M-REP (Machine to Machine REPutation) system that computes global reputation of machines in the network using secure multiparty computation techniques. The aggregated reputation score of a machine is computed in a decentralized and secure way without disclosing any private information of participants. The participating machines or participants (human) first assign a trust score to the machine based on the experience of their interactions with the machine, and then, they report cryptograms of trust scores to the public bulletin board. The reputation aggregator or reputation requester then computes global reputation of a machine by simply using the cryptograms from the bulletin board using a secure multi-party computation method without learning the individual trust-scores. The system does not require any trusted third party and trusted setup for the management of cryptographic parameters. Specifically, we present the protocol operations for the malicious adversarial model, where participants may attempt to provide false scores (out-of-range trust values) for the purpose of maliciously increasing or decreasing the aggregate reputation of some machines. The design also allows verifying operations by the protocol participants without relying on any trusted setup. Further, the system does not require participants to remain online during the aggregation process in contrast to existing reputation systems [14, 37, 38, 39] where feedback providers are required to remain online during the aggregation process.

This journal article extends our previous conference paper [40] in several aspects. First, we provide full security proofs for the malicious adversarial model, considering the condition where the adversary may collude with a set of participants (Section 5). Second, we present a full prototype implementation and evaluate the performance of the prototype with regard to the bandwidth and computation overhead (Section 6). Third, we analyze the computational complexity of the M2M-REP system in comparison to other centralized and decentralized reputation systems (Section 6). Finally, this article provides discussions on the salient features and limitations of the system (Section 7). In summary, this paper makes the following contributions.

- We propose a novel decentralized privacy-preserving reputation system for computing the trustworthiness of machines in the M2M network. This approach uses secure multi-party cryptographic techniques and efficient zero-knowledge proof of knowledge to enable participants to report their trust scores in a privacy-preserving way.
- We provide detail analysis on the security, privacy and correctness properties of the proposed system for the malicious adversarial model.
- We provide a prototype implementation of the cryptographic operations to evaluate the efficacy of the system in terms of the bandwidth consumption and computational overhead. We also compare the complexity of the proposed system with the other relevant systems.

The remaining part of the paper is organized as follows. Section 2 reviews related works on the computation of reputation in an M2M and P2P (peer to peer) networks. Section 3 describes preliminaries and formalizes the problem. Section 4 describes the design of the proposed M2M Reputation system. Section 5 analyses the security and privacy properties of the proposed system. Section 6 presents the prototype implementation and evaluates the system's performance for the bandwidth and computation overhead. Section 7 provides discussion on the important features and limitations of the M2M-REP system. Finally, Section 8 concludes the paper.

2. State of the Art

We present related work in two aspects: first, works performed in the domain of M2M network, and second, the P2P (peer to peer) network. Liu et al. [38] proposed a trust and reputation system for blocking the malicious machines from distributing content in the M2M network. It considers the trust values from participants, pairwise rating similarity measure and controlled propagation of trust ratings for computing the reputation of the machine. The privacy of participant has not been considered in this approach. Nitti et al. [41] proposed two reputation management models for detecting the malicious nodes in an IoT network. In the first model, each object computes the direct trustworthiness of other objects based on its direct experience, and in the second model, the trustworthy information of an object is propagated and stored using the DHT (Distributed Hash Table) structure. This enables all objects to have the same information about other objects in the system. In this approach, the direct feedback could be revealed to other objects, thus disclosing connectivity network of machines or objects. Yan et al. [34] proposed two approaches for protecting privacy and feedback scores of the participating nodes while computing trust and reputation of nodes. The first approach is based on the PKC (Public Key Cryptography) and uses an additive homomorphic system to protect the integrity of feedback provided by the participating nodes. The second approach is based on the additive pallier-cryptosystem. However, the privacy efficiency of these schemes relies on the trustworthiness of participating nodes i.e. nodes are honest in providing the correct feedback. The first scheme achieves better computational efficiency, while the second approach provides greater security at the expense of a higher computational cost. In [42], data from the smart grid application is aggregated by having the concentrators in the neighborhood of a smart grid network. Chen et al. [43] presents a fuzzy theory based trust and reputation model for the IoT network by utilizing cooperation among the IoT devices. However, the system has not considered the privacy of the participants.

Stojmenovic et al. [44] presented a decentralized auction-based system for the cyber-physical systems, but the system does not provide any security and privacy aspects of machines participating in the auction process. Efthymiou et al. [45] use anonymization techniques to protect privacy of reading data by anonymizing the smart meter data before submitting it to a third party arbitrator; however, anonymized data is subject to the de-anonymization attack by correlating information from multiple sources [28]. A non-trusted aggregator can evaluate the feedback values provided by the participants without imposing any limit on the number of participants [46]; however, it requires a large number of encryption keys to manage the individual feedbacks and decryption of the final scores.

Several decentralized and distributed systems have been proposed for the reputation aggregation in a P2P network. In [47] a decentralized system is proposed for the aggregating reputation of nodes in a P2P network; however, a malicious node can easily track activities of others by assigning a specific reputation score to the target node. In [48] a secure homomorphic cryptographic system is proposed that ensures privacy of nodes while computing global reputation of the nodes. This system has desired properties of security and privacy for the honest participants, however, it can be misused by the malicious nodes. In [14] an Eigen trust algorithm is proposed for aggregating the feedback scores in a decentralized P2P network. However, in the Eigen trust algorithm, the participating nodes know communication network of others, and further nodes need to remain online during the aggregation process. In [37, 13] a decentralized privacy preserving reputation protocol is proposed for the reputation aggregation under the malicious adversarial model. The protocol computes the aggregate reputation score by using the set of trusted users to whom participants submit their trust scores. However, having a set of pre-trusted users is not always feasible in a P2P network. It is desirable to have a system that is not dependent on a set of pre-trusted peers. In [26], another decentralized reputation system is proposed but it requires a trusted module chip at each participating agent or peers for the privacy protection. Ernesto et al. [23] proposed a P2Prep protocol which operates in two phases. First, the requester peer finds a set of peers that hold the required content, and second, it pools others to collect the votes about the behavior of the selected peers. The requester then uses the aggregate opinion to make the decision. Dimitriou et al. [49] proposed a voting-base reputation system for the decentralized network but it only ensures the privacy of participants under the semi-honest adversarial model.

Raya at al.[50] proposed a system that protects private information of vehicles in a vehicular network by pseudonymizing the identity of the vehicles using anonymous public keys and a public key infrastructure (PKI). The trusted authority is responsible for controlling messages between vehicles and aggregation of responses .However, the trusted party poses a threat to the privacy of vehicles. Sun et al. [51] proposed a pseudonym-based scheme that provides traceability as required by the law enforcement agencies while providing desired security and privacy features to vehicles in the network. Parno et al. [52] discussed challenges in securing the vehicular networks and proposed a number of security mechanisms for securing the vehicular networks. Castelluccia et al. [53] used a method based on homomorphic encryption to aggregate the data collected from nodes in the wireless sensor networks. Keke et al. [54] proposed a security model that uses a multi-channel communications model to resolve the conflict between privacy protection and efficiency. Meng at al. [55] proposed a distributed communication mechanism for the exchange of communication messages between machines in the network in an industrial system architecture. The system only focuses on the exchange of messages between ma-

chines by relying on the trustworthiness of machines in the network. Chen et al. [56] developed an approach for the trust and reputation management of IoT objects based on a distributed collaborative filtering system to select feedback from the participants. The approach uses a number of metrics such as the similarity in the rating of connectivity network of objects, social contact, and community of interest relationships; however, privacy was not considered in the design.

To the best of our knowledge, this work is the first that computes the aggregated reputation of the machines in an M2M network system while preserving privacy of participating machines or users in a decentralized way. The proposed system ensures privacy of feedback providers for the honest-but-curious and the malicious adversarial models. Furthermore, the proposed system allows participants to verify the well-formedness of input as well as the integrity of the aggregated reputation. The small computation and bandwidth overhead make the scheme feasible for the networks and nodes that are resource-constrained.

3. Preliminaries

This section describes preliminaries that are necessary to describe the design of the proposed system in Section 4.

3.1. Graph Representation of M2M Network

The human-machine or machine to machine network can be represented as a directed weighted bipartite graph network $G(P, N, V, W)$ as shown in Figure 1, where P represents the identity of the participant accessing the machine services, N represents the identity of machine providing the services, edge V represents the edge between machine and the participant; it exists only if P interacted with the N at least once. The weight W represents the trust weight a participant has assigned to the machine for his past transactions. The participants in the M2M network can be either a machine, a device or a human using the machine. The weights on edges between nodes are computed after the completion of a transaction and it can be either 1 (trusted interaction), -1 (untrusted interaction) or 0 (uncertain or no interaction). The graph presented in Figure 1 can be represented as a sparse matrix where the row represents identities of participants and the column represents identities of the machines.

$$P_{ij} = \begin{cases} connected; & \text{if } P_i \text{ interacted } N_j \\ non-connected; & \text{Otherwise} \end{cases} \quad (1)$$

3.2. Problem Statement

Suppose there is a machine network of n machines $(N1, N2, \ldots, N_n)$ and there are p $(P1, P2, \ldots, P_p)$ users interacting with the machines. Each user in a network

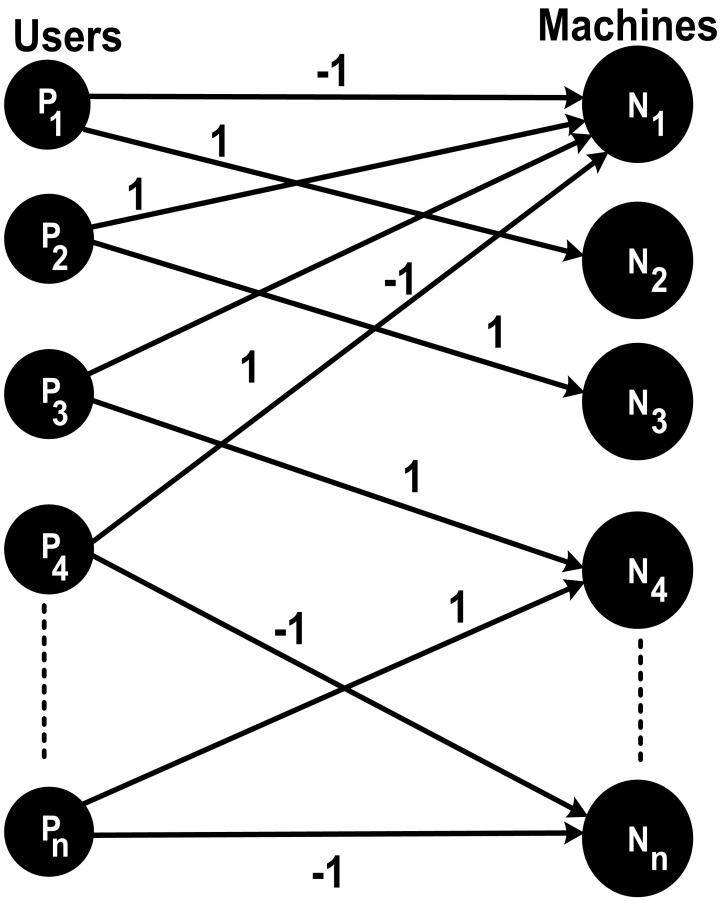


Figure 1: The representation of M2M and Human Participants and a Graph Network.

evaluates the trustworthiness of its directly interacted machines and assigns a direct trust score based on the outcome of transactions. Consider a trust matrix $M = (v_{ij})$, where $(i, j) \in N, P$, v_{ij} is the direct trust score assigned by the participant i to the machine j. The direct trust matrix can be represented as a matrix:

$$M = \begin{pmatrix} v_{11} & v_{21} & v_{31} & \cdots & v_{n1} \\ v_{12} & v_{22} & v_{32} & \cdots & v_{n2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & v_{3n} & \cdots & v_{pn} \end{pmatrix} \quad (2)$$

The trust value v_{ij} assigned by the participant P_i to the machine N_j can have one of the following three values:

$$v_{ij} = \begin{cases} -1; & \text{if Machine is not trustworthy} \\ 1; & \text{if machine is trustworthy} \\ 0; & \text{if the status is uncertain or not interacted} \end{cases} \quad (3)$$

There are some machines or users who want to interact or download content from the unknown machines in the network. Having interaction with the non-reputed machines has the risk of bringing damaging consequences in terms of data and financial loss if the content from the interacted

machine is packed with malware. Furthermore, the participants may hesitate to interact with the unknown machines because of fear of losing private information to the untrusted machines. The participant wishes to have information about the trustworthiness of machine he wishes to communicate with prior to submitting a request. This can be done by asking other peers for their feedback about the machine. There is a global trust vector representing the global reputation or global trustworthy score of machines $R = (t_1, t_2, \ldots, t_n)'$ such that each $t_i \in [1, h], \forall i \in [n]$, h being a small integer. The global trust vector represents the aggregate trustworthiness or reputation of machines as perceived by participants who have already interacted with the machines.

Let us assume there is an M2M network comprising n machines $N_1, N_2, \ldots, N_n$. Every participant holds a feedback trust vector $V_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, where $v_{ij} \in \{-1, 0, 1\}$ as represented in Equation 3. The global reputation of the machines can be represented as a vector of scores $R = (t_1, t_2, \ldots, t_n)$. $t_i \in [1, h], \forall i \in [n]$. If the machine is appearing for the first time, then the value of t_i for such a machine is initialized with 1 i.e. trusted. This would provide new machines a fair chance to introduce themselves to users in the network. In Equation 2 the columns of the matrix M_{nxn} are the local trust vectors (feedback scores) held by the p participants, that is $M = [V_1||V_2|| \ldots ||V_n]$. All the collaborating participants collaborate secretly for computing the temporary global reputation vector $R' = (R'_1, R'_2, \ldots, R'_n)$, where $R'_j = \lfloor \frac{nh + \sum_{i=1}^{n} M_{ij} * t_i}{nh + \sum_{i=1}^{n} R_i} * (h-1) \rceil, \forall j \in [n]$. The updated global reputation vector $T' = (t'_1, t'_2, \ldots, t'_n)$ for the iterative process (next aggregation cycle) can be computed as:

$$t'_i = 1 + R'_i \tag{4}$$

The problem is to compute the global trust vector of the machine by aggregating the feedback scores assigned to the machine by the participants in a secure and private way. The participant in our settings can be either a machine or a human user using the services. The challenges in the design of a reputation aggregation system for the distributed human-centric M2M network are fourfold: 1) the reputation aggregation process should ensure the privacy of participants providing the trust feedback, 2) the computation should be carried out without the use of any trusted setup or trusted third entity, 3) the feedback of participants should also be included in the final reputation aggregation process even if the participants of the protocol are off-line at the time of the aggregation process, 4) it should provide public verifiability.

3.3. Adversary Model

The privacy-preserving reputation system ensures that the trust scores of participants should not be used to infer the private information of feedback providers. The feedback values should be revealed as an aggregate result. Let TR be some private trust score which is held by the participants and is exchanged to the bulletin board as the input. The bulletin board, aggregator, adversary, and participants are considered as preserving the privacy of participants if they cannot infer any information apart from the aggregated reputation score of the target machine. The design of M2M-REP system ensures privacy and correctness for the honest but curious and malicious adversarial models. In the honest-but-curious model, the participants always provide the correct feedback about their interactions with the machines, however, they can try to learn the private information of other participants from the feedback values. In the malicious model, the participants can try to manipulate the feedback values in order to assign a high or low score to the specific machine, and further, they may try to learn the private information of other participants.

3.4. Notations

The notations used throughout the paper are summarized in Table 1. We denote the set of all machines as $N = \{N_1, N_2, \ldots N_n\}$. There is the set of participants $P = \{p_1, p_2, \ldots p_n\}$ using the services from N_i. We use $V'_i = (v_{i1}, v_{i2}, \ldots, v_{in})'$ to represent the local trust vector of P_i for the interacted machines. The Vector R represents the global reputation of machines in the setup and T' is the updated global reputation vector for the proceeding aggregation cycle. For the cryptographic operation, we use x_i to represent the private key of P_i, $X_i = g^{x_i}$ represents the public key of the P_i and $Y = g^{y_{i1}}$ represents the restructured key of P_i.

3.5. Homomorphic Cryptographic System

The homomorphic cryptographic system performs computation over the encrypted data without decrypting the encrypted data. The result of the computation performed over the encrypted data is similar to the computation performed over the non-encrypted data i.e. $Enc_{pk}(a) * Enc_{pk}(b) = Enc_{pk}(a+b)$. The homomorphic cryptographic system consists of three major algorithms: Key generation – responsible for generating the public and the private keys, Encryption – responsible for encrypting the data, and the Decryption – responsible for decrypting the results performed over the encrypted data. In this paper, we consider the additively homomorphic encryption system as we are only aggregating the feedback values from the participants.

The cryptographic primitives used in the design of M2M-REP is adapted from a decentralized aggregation system used in an electronic voting system [57] without relying on any trusted authority for the result aggregation. In [57] a group of n voters compute a final tally $T = \sum_{i=1}^{n} v_i$, where $v_i \in \{0, 1\}$ is the secret input of voter $V_i, \forall i \in [n]$. However, we modify the scheme presented in [57], so as to incorporate three values that are $v_i \in \{0, 1, -1\}$, assign weights to the inputs which are proportional to the value of the quantitative reputation of the feedback provider,

and also modify the zero knowledge proof for 1-out of 3 values.

Let $P = \{1, 2, \ldots, n\}$ are the users or machines in the network holding the feedback scores (0,1,-1) for a certain machine. Let G be a DSA-like multiplicative group containing p elements. Let g be a generator of G. We assume that in G, the Decisional Diffie-Hellman (DDH) problem is hard to compute. In order to provide the feedback , the ith user first generates a random value $x_i \in \mathbb{Z}_q^\star$ for all $i \in N$. The value of x_i is set as the private key and value of public key X_i is computed as follows.

$$X_i = g^{x_i} \tag{5}$$

The machine or user then makes this public key available to others. Each of the participants in the system then computes the restructured key as follows.

$$Y_i = \prod_{j \in N, j<i} X_i \Big/ \prod_{j \in N, j>i} X_i. \tag{6}$$

Computing Y_i as above ensures that the following equation holds

$$\prod_{i \in N} Y_i^{x_i} = 1. \tag{7}$$

The possible trust score that a participant can assign to his interacted machines is 1 (trusted), or -1 (non-trusted), or 0 (not interacted with). The cryptogram of trust score is generated as following:

$$c_i = \begin{cases} c_{1i} = Y_i^{x_i} g; \text{ if the feedback is } 1 \\ c_{0i} = Y_i^{x_i}; \text{ if the feedback is } 0 \\ c_{-1i} = Y_i^{x_i}/g; \text{ if the feedback is } -1 \end{cases} \tag{8}$$

Furthermore, the user also computes and presents a zero-knowledge proof of well-formedness $NIZK[x_i : X_i, Y_i, c_i]$ for the encrypted feedback scores. A non-interactive zero-knowledge proof (NIZK), is a zero-knowledge proof of the statement where the sender (prover) can prove to the receiver (verifier) that a given statement is true, without revealing any other information. In M2M-REP, we prove the knowledge of a secret value is 0, 1 or -1. A NIZK proof can be generated using the Σ protocol [58] and the Fiat-Shamir heuristic [59].

4. M2M-REP: System Architecture and Protocol Operations

In this section, we present the architecture of an M2M-REP system and detail its protocol operations.

4.1. System Model

The M2M-REP system is a decentralized system. The system architecture of M2M-REP is shown in Figure 2. The system consists of three major components: *the machines* providing services to their users or participants, *the participants* that are using services of machines and provide feedback, and *the public bulletin board* that holds encrypted trust scores and the non-interactive zero-knowledge proof reported by the participants. The participants evaluate the trustworthiness of the machine by assigning the trust score to the interacted machine and report encrypted trust score together with a non-interactive zero-knowledge (NIZK) to the bulletin board.

Notation	Meaning
$N_1, N_2, \ldots, N_n$	machines
$P_1, P_2, \ldots, P_n$	participants
NIZK	non-interactive zero knowledge
G	cyclic group of p elements in which DDH problem is hard
$[n]$	the set $\{1, 2, \ldots, n\}$
$[a, b]$	the set $\{a, a+1, \ldots, b\}$
c_{ij}	encrypted feedback generated by P_i for P_j.
$\lfloor a \rceil$	nearest integer of a
$(x_{i1}, x_{i2}, \ldots, x_{in})$	private key of P_i
$(g^{x_{i1}}, g^{x_{i2}}, \ldots, g^{x_{in}})$	public key of P_i
$(g^{y_{i1}}, g^{y_{i2}}, \ldots, g^{y_{in}})$	restructured key of P_i
$V_i = (v_{i1}, v_{i2}, \ldots, v_{in})'$	local trust vector of P_i
M	the matrix $[V_1 \| V_2 \| \ldots \| V_n]$
u_j	$\sum_{k=1}^{n} t_k v_{kj}$
$R = (t_1, t_2, \ldots, t_n)'$	$(n \times 1)$ global reputation vector
T'	$(n \times 1)$ updated global reputation vector for next cycle

Table 1: Notations & abbreviations used in the design of M2M-REP.

4.2. Protocol Assumptions

We assume that each participant has a unique identity (IP address, identity) and can access services from the value-added machines and nodes. The participants wish to report their experience with the interacted machine to collaboratively suggest to others whether to interact with the machine or not and identify the non-trusted machines. There is a publicly accessible append only bulletin board to which the participants report their encrypted feedback and the NIZK proof of knowledge . The participants or feedback providers authenticate every message they upload to the bulletin board by digitally signing the message. We assume that participants have only append & read access to the Bulletin Board (BB) over the authentic channel. Further, we assume that participants are only providing feedback for the machines whom they have interacted with during the aggregation time window.

4.3. Protocol Operations

The reputation aggregation process in an M2M-REP system consists of three steps. 1) Each participant generates the secret and public keys; keeps the secret keys to

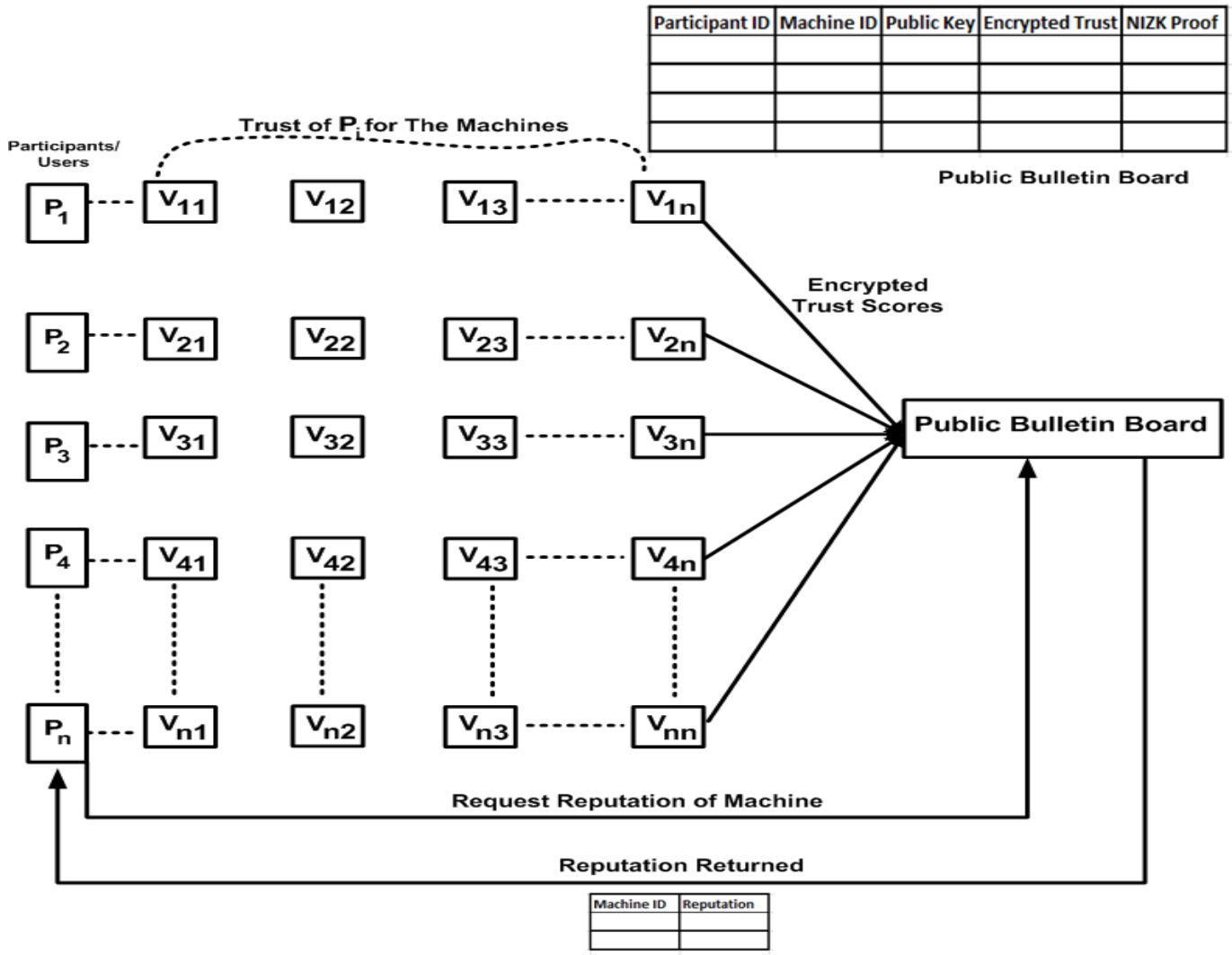


Figure 2: M2M-REP system architecture. Participants assign direct scores to machines with whom they interacted. The encrypted feedback is then sent to the bulletin board. The reputation is then aggregated without revealing the individual trust scores.

themselves, and publishes the public keys on the bulletin board. 2) The participants then compute the restructured key from the public keys, and generate the cryptogram of feedback and associated NIZK proof using the private key and the restructured key. They then publish cryptograms along with NIZK proofs to the bulletin board (BB). 3) Finally, participants compute the global reputation vector by multiplying the published cryptograms. The reputation aggregation procedure is represented in Algorithm 1 and detailed as below:

4.3.1. Reporting Public Keys

In a setup phase each participant $p_i, i \in [P]$ chooses a random secret key $x_i = (x_{i1}, x_{i2}, \ldots, x_{in}) \in_R \mathbb{Z}_p^n$. It keeps the secret key $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ and publishes the corresponding public key $X_i = (g^{x_{i1}}, g^{x_{i2}}, \ldots, g^{x_{in}})$ on the public bulletin board.

4.3.2. Reporting Trust Scores

This phase consists of two steps: first, generating the restructured key, and second creating the cryptogram of the direct trust score.

In first step, the participant P_i generates $g^{y_{ij}}$, a restructured public key as follows:

$$g^{y_{ij}} = \prod_{k=1}^{i-1} g^{x_{kj}} / \prod_{k=i+1}^{n} g^{x_{kj}}, \forall j \in [n] \tag{9}$$

where y_{ij} is

$$y_{ij} = \sum_{k=1}^{i-1} x_{kj} - \sum_{k=i+1}^{n} x_{kj} \tag{10}$$

$$g^{y_{ij}} = \prod_{k=1}^{i-1} g^{x_{kj}} / \prod_{k=i+1}^{n} g^{x_{kj}} \tag{11}$$

In a second step, each participant $P_i, i \in [n]$ computes a feedback $C_i = (c_{i1}, c_{i2}, \ldots, c_{in})$, where the value of each

Algorithm 1 Computing Reputation

input: Participants with Trust Scores of Interacted Machines
output: Reputation of Machines in the Network
procedure CRYPTOGRAPHIC KEYS(Given: cyclic Group G with generator g)
    $x_{ij} \leftarrow \in \mathbb{Z}_q^\star, i, j \in N$
    $X_{ij} \leftarrow g^{x_{ij}}, i, j \in N$
Publish X_{ij} on the bulletin Board for all $i, j \in N$
Publish NIZK Proof of Knowledge of x_{ij} on the bulletin Board for all $i, j \in N$
For Each participant P_i in the Network Compute Y_{ij} as:
    $Y_{ij} \leftarrow \prod_{k \in N, k<i} X_{kj} \Big/ \prod_{k \in N, k>i} X_{kj}$.
procedure CREATING CRYPTOGRAMS(Given $x_{ij}, Y_{ij}, g, T = (t_1, t_2, \ldots, t_n)$ and Score)
    $c_{ij} \leftarrow Y_i^{x_{ij}} g^{t_i}$; if the trust score is 1
    $c_{ij} \leftarrow Y_i^{x_{ij}}$; if the score is 0
    $c_{ij} \leftarrow Y_{ij}^{x_{ij}} / g^{t_i}$; if the trust score is -1
Generate NIZK Proof of Well-formedness of c_{ij} as discussed in section 4.3.4
Publish Feedback and NIZK on the Bulletin Board
procedure COMPUTING REPUTATION(Given: Cryptograms of Scores and NIZK)
    $l_j = \prod_{i=1}^{n} c_{ij} = g^{\sum_{k=1}^{n} t_k v_{kj}} = g^{u_j}, \forall j \in [1, n]$.
    $u_j = \log_g l_j, \forall j \in [1, n]$.
    $u'_j = u_j + n * h, \forall j \in [1, n]$.
    $R'_j = \lceil \frac{u'_j (h-1)}{nh + \sum_{i=1}^{n} t_i} \rceil, \forall j \in [1, n]$
    $T' = (1 + R'_1, 1 + R'_2, \ldots, 1 + R'_n)$

c_{ij} is computed as following:

$$c_{ij} = g^{x_{ij} y_{ij}} g^{t_i v_{ij}} \tag{12}$$

As the values of $g^{x_{ij}}$ are available publicly on the bulletin board, P_i can compute $g^{y_{ij}}$ for all $j \in [n]$ without calculating y_{ij}. Hence, participants P_i can compute c_{ij} as following:

$$c_{ij} = (g^{y_{ij}})^{x_{ij}} g^{t_i v_{ij}} \tag{13}$$

The participant also provides NIZK (non-interactive zero knowledge proof) to ensure that the feedback provided by P_i is one of the three values (0,1 and -1). The NIZK proof consists of a witness to the fact that $c_{ij} \in \{g^{x_{ij} y_{ij}} / g^{t_i}, g^{x_{ij} y_{ij}}, g^{x_{ij} y_{ij}} g^{t_i}\}$. The construction of this proof is discussed in Section 4.3.4. P_i posts on the bulletin board C_i and $PW_{ij}[\cdot]$ for all $j \in [n]$.

4.3.3. Reputation Computation

Once the encrypted direct trust scores of machines have been reported to BB (bulletin board), anyone (Network Manager, the aggregator, the system administrator or any participant) can compute the global reputation score of any particular machine in the network as $R = (R_1, R_2, \ldots, R_n)$, where the value R_i is computed as below:

$$l_j = \prod_{k=1}^{n} c_{ij} \tag{14}$$

$$= \prod_{k=1}^{n} g^{x_{kj} y_{kj}} g^{t_k * v_{kj}} \tag{15}$$

$$= g^{\sum_{k=1}^{n} x_{kj} y_{kj}} g^{\sum_{k=1}^{n} t_k v_{kj}} \tag{16}$$

$\sum_{k=1}^{n} x_{kj} y_{kj} = \sum_{k=1}^{n} x_{kj} (\sum_{m=1}^{k-1} x_{mj} - \sum_{m=k+1}^{n} x_{mj}) = \sum_{k=1}^{n} \sum_{m<k} x_{mj} x_{kj} - \sum_{k=1}^{n} \sum_{m>k} x_{mj} x_{kj}$.

Now, $\sum_{k=1}^{n} \sum_{m<k} x_{mj} x_{kj} = \sum_{m,k=1,m<k}^{n} x_{mj} x_{kj} = \sum_{m,k=1,m>k}^{n} x_{mj} x_{kj} = \sum_{k=1}^{n} \sum_{m>k} x_{mj} x_{kj}$.

Thus,

$$\sum_{k=1}^{n} x_{kj} y_{kj} = 0 \tag{17}$$

Hence,

$$l_j = g^{\sum_{k=1}^{n} t_k v_{kj}} = g^{u_j} \tag{18}$$

Since, $u_j \in [-nh, nh]$, a limited brute force search on l_j would yield u_j. Let, $u'_j = u_j + n * h, \forall j \in [1, n]$. Then, the aggregator can compute $R'_j = \lfloor \frac{u'_j (h-1)}{nh + \sum_{i=1}^{n} t_i} \rceil$ and update the global trust vector T' for the next aggregation cycle using Equation 4.

4.3.4. Verification

The verification process is performed for two operations, the knowledge of the secret key and the well-formedness of trust score.

Proof of knowledge of the secret key: The participant $P_i; i \in [1, n]$ generates secret keys x_{ij} for all $j \in [1, N]$. The participant P_i publishes corresponding public keys $X_{ij} = g^{x_{ij}}, \forall j \in [1, n]$ along with the NIZK proof of knowledge of $x_{ij}, j \in [1, n]$. These NIZK proofs can be constructed as follows. The prover generates a random $r \in_R \mathbb{Z}_p$ and computes a commitment $com = g^r$. Let, the challenge of the NIZK proof be ch. The prover calculates a response $res = r - ch * x_{ij}$. The prover then publishes the commitment com and the response res. The verification is performed as follows:

$$g^{res} \stackrel{?}{=} com / (g^{x_{ij}})^{ch} \tag{19}$$

If Equation 19 is satisfied, then the proof is correct. This NIZK proof has one commitment and one response. Hence, the size of the proof is 2. The proof is computed in 1 modular exponentiation and the verification requires two exponentiations, respectively.

Proof of knowledge of the well-formedness: The verification of well-formedness of the feedback score at the BB is the fundamental step in the design of the M2M-REP system. This verification would prevent participants

from providing out-of-range false values about machines in order to disrupt the system and maliciously increase the reputation of some machines. This would also prevent malicious participants to assign high trust scores by making the artificial social circle. M2M-REP provides verification by checking the values of zero-knowledge proof that provides information whether the reported local trust is -1 or 0 or 1 in a non-interactive way and without learning the value of the feedback.

Each encrypted feedback is of the form $c_{ij} = g^{x_{ij}y_{ij}}g^{t_i v_{ij}}$, where $g^{x_{ij}}, g^{y_{ij}}$ is provided on the bulletin board, v_{ij} is -1 or 0 or 1, and t_i comes from the global trust vector T. Here, we discuss how each participant can construct a NIZK proof $PW_{ij}[c_{ij} : g^{x_{ij}}, g^{y_{ij}}, t_j]$. This proof consists of a witness to the fact that exactly one of the three statements below is true:
1) $c_{ij} = g^{x_{ij}y_{ij}}g^{t_j}$
2) $c_{ij} = g^{x_{ij}y_{ij}}$
3) $c_{ij} = g^{x_{ij}y_{ij}}/g^{t_j}$
where $g, g^{x_{ij}}, g^{y_{ij}}$ and t_j are public. This is a 1-out-of-3 statement. Let us assume that the first statement is true, that is $c_{ij} = g^{x_{ij}y_{ij}}g^{t_j}$. Hence, the prover will have to provide a real proof for the first statement and two simulated proofs for two other statements. For the sake of clarity, we denote $c_{ij}, x_{ij}, y_{ij}, t_j$ as c, x, y and t respectively. Hence, the prover has to prove that $c = g^{xy}g^{-1}$, or g^{xy} or $g^{xy}g$. The prover chooses a random $r_1 \in_R \mathbb{Z}_p$ and computes a commitment $com_1 = g^{r_1}, com_1' = (g^y)^{r_1}$. The prover then chooses random challenges $ch_2, ch_3 \in_R \mathbb{Z}_p$ and two responses $res_2, res_3 \in_R \mathbb{Z}_p$ and computes 4 commitments:
$com_2 = g^{res_2}(g^x)^{ch_2}, com_2' = (g^y)^{res_2}c^{ch_2}$
$com_3 = g^{res_3}(g^x)^{ch_3}, com_3' = (g^y)^{res_3}(c * g^t)^{ch_3}$
Let the grand challenge of the NIZK statement be ch. The prover calculates $ch_1 = ch - ch_2 - ch_3$. Then the prover computes a response $res_1 = r_1 - x * ch_1$.

The verification equations are as below:

1. $g^{res_s} \stackrel{?}{=} \frac{com_s}{(g^x)^{ch_s}}, \forall s \in \{1, 2, 3\}$
2. $(g^y)^{res_1} \stackrel{?}{=} \frac{com_1'}{(c/g^t)^{ch_1}}$
3. $(g^y)^{res_2} \stackrel{?}{=} \frac{com_2'}{c^{ch_2}}$
4. $(g^y)^{res_3} \stackrel{?}{=} \frac{com_3'}{(c*g^t)^{ch_3}}$

If these six verification equations are satisfied, then the proof is accepted. The total number of commitments of the proof is 6, the total number of responses is 3 and the total number of challenges is 3. Hence, the size of the NIZK proof is 12.

Similarly, NIZK proof can be generated for the two other cases, that is for $c = g^{xy}$ and for $c = g^{xy}/g^t$.

4.4. Public Bulletin Board

Public Bulletin Board (BB) is used to provide a way for the exchange of trust scores and cryptographic parameters among the participants of the M2M-REP system. The bulletin board itself does not have the ability to generate the cryptograms. It can only write the information provided by the participants. The bulletin board can also validate the well-formedness of the received feedbacks before putting them on the bulletin board, and make sure that no entity (participants or other parties) could delete or change the published data.
The bulletin board holds the following key information: the cryptograms of the feedback scores, zero-knowledge proofs to prove that cryptograms are well-formed, and the identity of the machine for which feedback is provided. Anyone can access the information from the bulletin board to compute the aggregated reputation of the machine in the network. All the computation performed on the information obtained from the bulletin board will be publicly verifiable by executing the aggregation process.
There are a few ways of implementing the functionalities of a bulletin board. One possible way is to use the distributed database by using the blockchain technology [60, 61] to hold the cryptograms submitted by the participants. An implementation of the bulletin board for small-scale boardroom voting based on Ethereum's blockchain is presented by McCorrry et al. [62]. An alternative method is to use a mirrored website as a bulletin board [63, 64, 65]. Only authenticated users can post messages on the bulletin board and all posted data are publicly readable. The user is not allowed to overwrite or alter the published data. To overwrite or alter previous data, the user must do this for all mirrored websites, which will make the tampering publicly evident.

5. Security Analysis of M2M-REP

In this section, we analyze correctness, security and privacy properties of the M2M-REP system.

5.1. Correctness of Our Scheme

In this section, we prove that our scheme is correct. The scheme correctly computes the updated reputation vector $T' = (t_1', t_2', \ldots, t_n')$ as discussed in section 4.3, $u_j = \sum_{k=1}^{n} t_k v_{kj}$, where $t_k \in [1, h]$. Now, $u_j + n * h, \forall j \in [1, n]$ and $R_j' = \lfloor \frac{u_j'(h-1)}{nh + \sum_{i=1}^{n} t_i} \rceil$. Let, k be such that $u_k = h * \sum_{i=1}^{n} t_i$, and hence, $u_k' = nh + h * \sum_{i=1}^{n} t_i$. Then $R_k' = h - 1$ and $t_k' = h$. Thus, our protocol assigns maximum weight to the machine who is trusted by everyone. Also, note that if there exists a machine M_r such that $u_r = -nh$, then u_r' will be 0. So, R_r' will be 0 too, ensuring that $t_r' = 1$. So, the machine who is not trusted by anyone else would get the lowest possible weight 1. All other machines will get weights in between 1 and h depending upon the value of weighted sum of scores obtained by them. Hence, the scheme is correct.

5.2. Security Analysis

We analyze the security and privacy aspects of the proposed M2M-REP system for the malicious participants

model. The malicious participants also have the ability to collude with other participants to find the trust scores assigned by the target participant. Let us assume that the adversary $\mathcal{A}$ colluded with k ($N_1, N_2, \ldots, N_k$) number of participants. The honest participants are $\{N_i : i \in [k, n]\}$. The adversary $\mathcal{A}$ acquires the local trust scores and the secret keys of the colluding participants. In Lemma 5, we prove that the adversary is only able to learn the partial aggregated sum of the targeted honest participants i.e. $\sum_{i=k+1}^{n} t_i v_{ij}$ for the honest participants $j \in [n]$. Lemma 5 proves that the aggregation protocol of the M2M-REP system would not allow the adversary to correlate information from the colluding participants and the aggregated sum to infer the trust scores assigned by the targeted participant. Further, the adversary would not be able to infer the communication network of the targeted participant as well. In a nutshell, the M2M aggregation protocol in an SMC (Secure Multi-party Computation) setting achieves the maximum protection of trust scores and relationship network without the use of a trusted setup and a set of preselected trusted users.

Assumption 1. *[**DDH assumption**] Given $g, g^a, g^b \in G$ and a challenge $\Omega \in_R \{g^{ab}, R\}$, it is hard to decide whether $\Omega = g^{ab}$ or $\Omega = R$.*

Assumption 2. *Given $g, g^a, g^b \in G$,$t \in \mathbb{Z}_p$, and a challenge $\Omega \in \{g^{ab}g^t, g^{ab}g^{-t}, g^{ab}\}$, it is hard to decide whether $\Omega = g^{ab}g^t$ or $\Omega = g^{ab}g^{-t}$ or $\Omega = g^{ab}$.*

Lemma 1. ***Assumption 1 implies assumption** 2.*

Proof. According to assumption 1, $(g, g^a, g^b, t, g^{ab}) \overset{c}{\approx} (g, g^a, g^b, t, R) \overset{c}{\approx} (g, g^a, g^b, t, R * g^t) \overset{c}{\approx} (g, g^a, g^b, t, g^{ab}g^t)$. Similarly, $(g, g^a, g^b, t, g^{ab}) \overset{c}{\approx} (g, g^a, g^b, t, R) \overset{c}{\approx} (g, g^a, g^b, t, R * g^{-t}) \overset{c}{\approx} (g, g^a, g^b, t, g^{ab}g^{-t})$. Hence, the result. □

Lemma 2. ***If there exists two participants** P_i **and** P_j**, such that** $t_i = t_j = t$**. If for some** $r \in [n]$ $v_{\alpha r} + v_{\beta r} = 0$**, for some** $r \in [n]$**,** $v_{\alpha r}$ **and** $v_{\beta r}$ **cannot be compromised**.*

Proof. Let

$$M = \begin{bmatrix} v_{11} & v_{12} & \cdots & \ldots & v_{1n} \\ v_{21} & v_{22} & \cdots & \ldots & v_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \cdots & \cdots & v_{\alpha r} & \cdots & \cdots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \cdots & \cdots & v_{\beta r} & \cdots & \cdots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ v_{n1} & v_{n2} & \cdots & \ldots & v_{nn} \end{bmatrix}^T$$

Now, consider these 3 cases:
(i) $v_{\alpha r} = 1, v_{\beta r} = -1$
(ii) $v_{\alpha r} = -1, v_{\beta r} = 1$
(iii) $v_{\alpha r} = 0, v_{\beta r} = 0$
Our aim is to show that the final bulletin board does not provide any information that could make these three cases distinguishable from each other. We prove it by showing that if there exists an adversary $\mathcal{A}$, who can distinguish between these three cases, it could be used as a distinguisher against Assumption 2. Let, $g, g^a, g^b, \Omega \in \{g^{ab}g^t, g^{ab}g^{-t}, g^{ab}\}$ be given inputs. The distinguisher D needs to find whether $\Omega = g^{ab}g^t$, or $\Omega = g^{ab}g^{-t}$, or $\Omega = g^{ab}$. The distinguisher uses $\mathcal{A}$ to distinguish them. We assume that the adversary $\mathcal{A}$ has compromised all other $n-2$ participants in the protocol except P_α and P_β. So, it can program them with trust values of its own choice. The distinguisher D against Assumption 2 works an follows:
she lets $\mathcal{A}$ control an arbitrary number of participants except P_α and P_β. Let, $S_\mathcal{A}$ be the set of all participants for which all the secret information including trust values and secret keys are selected by $\mathcal{A}$. For the rest of $n-2-|S_\mathcal{A}|$ peers, the trust values and the secret keys are assigned by D. Now, let the public key of peer P_i be given by $Pub_i = (g^{x_{i1}}, g^{x_{i2}}, \ldots, g^{x_{in}})$. The distinguisher D implicitly assigns $g^a = g^{x_{\alpha r}}$ and $g^b = g^{x_{\beta r}}$. D chooses random values for all values of $x_{ik}, \forall i \in \{\alpha, \beta\}$ and $k \in [n] \setminus \{r\}$. For all participants in $S_\mathcal{A}$, $\mathcal{A}$ selects their public keys and trust values. Now, for all $i \in [n] - \{\alpha, \beta\}$, such that $P_i \notin S_\mathcal{A}$, D publishes the vector $C_i = (c_{i1}, c_{i2}, \ldots, c_{in})$ as $c_{ij} = g^{x_{ij}y_{ij}}g^{tv_{ij}}, j \in [n]$. Since, the values of x_{ij}, y_{ij} are known to D, it can calculate c_{ij}s for all i, j such that $P_i \notin S_\mathcal{A} \bigcup \{P_\alpha, P_\beta\}$ and $j \in [n]$. Similarly, for all i such that $P_i \in S_\mathcal{A}$, $\mathcal{A}$ can compute C_i as it selects all secrets for these participants. Now for $i \in \{\alpha, \beta\}$, for $j \in [n] \setminus \{r\}$, D can calculate c_{ij} as it knows all the necessary secrets. Now, D assigns $c_{\alpha r} = g^{aK_1}/\Omega$ and $c_{\beta r} = g^{bK_2}\Omega$, where $K_1 = \sum_{k=1}^{\alpha-1} x_{kr} - \sum_{k=\alpha+1}^{\beta-1} x_{kr} - \sum_{k=\beta+1}^{n} x_{kr}$ and $K_2 = \sum_{k=1}^{\alpha-1} x_{kr} + \sum_{k=\alpha+1}^{\beta-1} x_{kr} - \sum_{k=\beta+1}^{n} x_{kr}$. Since, D has chosen all these values itself, it can compute K_1 and K_2. Now, observe that since $c_{\alpha r} = g^{x_{\alpha r}y_{\alpha r}}g^{tv_{\alpha r}}$, and D has set $c_{\alpha r} = g^{aK_1}/\Omega$, if $\Omega = g^{ab}g^t$, we will implicitly have $v_{\alpha r} = -1$. Similarly, since $c_{\beta r} = g^{x_{\beta r}y_{\beta r}}g^{tv_{\beta r}}$, and D has set $c_{\beta r} = g^{bK_2}\Omega$, if $\Omega = g^{ab}g^t$, we will implicitly have $v_{\beta r} = 1$. Similarly, if $\Omega = g^{ab}g^{-t}$, we have $v_{\alpha r} = -v_{\beta r} = 1$. Also if $\Omega = g^{ab}$, we have $v_{\alpha r} = v_{\beta r} = 0$. Now, if $\mathcal{A}$ can properly distinguish the bulletin boards for the three cases, then D can also distinguish between the three plausible values of Ω. Hence, the lemma holds. □

Lemma 2 proves that when there exist two honest participants having the same weight such that the sum of their inputs is zero, then the adversary, who has corrupted all other participants, will not be able to distinguish between the following three cases:

1. $v_{\alpha r} = 1, v_{\beta r} = -1$
2. $v_{\alpha r} = -1, v_{\beta r} = 1$
3. $v_{\alpha r} = 0, v_{\beta r} = 0$

The reason behind this is the fact that our scheme only allows everyone (including the adversary) to learn the weighted sum of the inputs. The weights are publicly known. Also

known to the adversary, is the set of inputs of all the $n-2$ colluding participants. Thus, the adversary can find the weighted sum of the two honest participants. This leaves the adversary with a linear relation of the form $v_1+v_2=\lambda$, where v_1 and v_2 are the inputs of the two honest participants and λ can be obtained via dividing the weighted sum of the two honest participants by the weights of the two honest participants. In Lemma 2, we show that the adversary will not be able to distinguish between all the possible values of v_1 and v_2 that make the sum equal to 0. Also, in Lemma 3, we show that a similar adversary will not be able to distinguish between the two cases $(v_1, v_2) = (1, 0)$ and $(v_1, v_2) = (0, 1)$, when the sum of v_1 and v_2 is 1, since these are the only possible values that could make $v_1 + v_2 = 1$. Similarly, Lemma 3 also proves that when $v_1 + v_2 = -1$, the same adversary will not be able to find whether $(v_1, v_2) = (-1, 0)$ or $(v_1, v_2) = (0, -1)$.

Lemma 3. ***If there are two honest participants*** P_α ***and*** P_β ***such that*** $t_\alpha = t_\beta = t$ ***and*** $v_{\alpha r} + v_{\beta r} \in \{-1, 1\}$ ***for some*** $r \in [n]$***,*** $v_{\alpha r}$ ***and*** $v_{\beta r}$***, and there exists exactly one*** $k \in \{\alpha, \beta\}$***, such that*** $v_{kr} = 0$***, no adversary can deduce whether*** $k = \alpha$ ***or*** $k = \beta$***.***

Proof. Let,

$$M = \begin{bmatrix} v_{11} & v_{12} & \cdots & \dots & v_{1n} \\ v_{21} & v_{22} & \cdots & \dots & v_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ \cdots & \cdots & v_{\alpha r} & \cdots & \cdots \\ \dots & \dots & \dots & \dots & \dots \\ \cdots & \cdots & v_{\beta r} & \cdots & \cdots \\ \dots & \dots & \dots & \dots & \dots \\ v_{n1} & v_{n2} & \cdots & \dots & v_{nn} \end{bmatrix}^T$$

Now consider these two cases;

1. $v_{\alpha r} + v_{\beta r} = 1$
2. $v_{\alpha r} + v_{\beta r} = -1$

We can divide case 1 into two subcases as follows;
(i) $v_{\alpha r} = 1, v_{\beta r} = 0$,
(ii) $v_{\alpha r} = 0, v_{\beta r} = 1$.
Similarly, we can divide case 2 into these two subcases;
(i) $v_{\alpha r} = -1, v_{\beta r} = 0$,
(ii) $v_{\alpha r} = 0, v_{\beta r} = -1$

We shall prove that the two subcases of case 1 are indistinguishable; the proofs for the other cases are omitted as they easily follow case 1. We prove this by showing that if there exists an adversary $\mathcal{A}$ who can distinguish between the two sub-cases of case 1, it can be used as an adversary against the DDH assumption. Let, $g, g^a, g^b, \Omega \in \{g^{ab}, g^{ab}g^t\}$ be given inputs. The distinguisher D needs to find whether $\Omega = g^{ab}$ or $\Omega = g^{ab}g^t$. The distinguisher uses $\mathcal{A}$ for this purpose. We assume that D has compromised all the $n-2$ peers other than P_α and P_β. So, it can either program them with trust values of its own choice or may allow $\mathcal{A}$ to do the same. The distinguisher D works as follows: it lets $\mathcal{A}$ control an arbitrary number of peers except P_α and P_β. Let $S_\mathcal{A}$ be the set of all peers controlled by $\mathcal{A}$. For all peers in $S_\mathcal{A}$, $\mathcal{A}$ selects the values of all secret keys and the trust vectors suitably. For the rest of $n-2-|S_\mathcal{A}|$ peers, the distinguisher D selects all trust values and secrets randomly. Let, the public key of peer P_i be given by $Pub_i = (g^{x_{i1}}, g^{x_{i2}}, \dots, g^{x_{in}})$. D inserts g^a as $g^{x_{\alpha r}}$ and g^b as $g^{x_{\beta r}}$. For $i \in \{\alpha, \beta\}$ and $k \in [n] \setminus r$, D chooses random values as x_{ik}. Now, for all i such that $P_i \in S_\mathcal{A}$, $\mathcal{A}$ publishes the vector $C_i = (c_{i1}, c_{i2}, \dots, c_{in})$, where $c_{ij} = g^{x_{ij}y_{ij}}g^{v_{ij}t_i}, \forall j \in [n]$. Since, $\mathcal{A}$ selects all secrets for these peers, it can compute the vector C_i for these peers. Similarly, for all $i \in [n] - \{\alpha, \beta\}$ such that $P_i \notin S_\mathcal{A}$, D computes the vector C_i. Since, D selects the secrets for all these peers, it can compute the vectors C_i for all these peers. Now for $i \in \{\alpha, \beta\}$, and for $j \in [n] \setminus \{r\}$, D can calculate c_{ij} as it knows all the necessary secrets. Now, D assigns $c_{\alpha r} = g^{aK_1}g^t/\Omega$ and $c_{\beta r} = g^{bK_2}\Omega$, where $K_1 = \sum_{k=1}^{\alpha-1} x_{kr} - \sum_{k=\alpha+1}^{\beta-1} x_{kr} - \sum_{k=\beta+1}^{n} x_{kr}$ and $K_2 = \sum_{k=1}^{\alpha-1} x_{kr} + \sum_{k=\alpha+1}^{\beta-1} x_{kr} - \sum_{k=\beta+1}^{n} x_{kr}$. Since, $\forall k \in [n], g^{x_{kr}}$ are known to D, it can compute K_1 and K_2, and hence can compute $c_{\alpha r}, c_{\beta r}$. Observe that since, $c_{\alpha r} = g^{x_{\alpha r}y_{\alpha r}}g^{v_{\alpha r}t_\alpha} = g^{x_{\alpha r}y_{\alpha r}}g^{v_{\alpha r}t}$, and D has set $c_{\alpha r} = g^{aK_1}g^t/\Omega$, if $\Omega = g^{ab}g^t$, then we will have $v_{\alpha r} = 0$ and if $\Omega = g^{ab}$, then we will have $v_{\alpha r} = 1$. Similarly, since $c_{\beta r} = g^{x_{\beta r}y_{\beta r}}g^{v_{\beta r}t_\beta} = g^{x_{\beta r}y_{\beta r}}g^{v_{\beta r}t}$, and D has set $c_{\beta r} = g^{bK_2}\Omega$, if $\Omega = g^{ab}g^t$, we will have $v_{\beta r} = 0$ and if $\Omega = g^{ab}$, we will have $v_{\beta r} = 1$. All these cryptograms are uploaded to the bulletin board. Now, if $\mathcal{A}$ can properly distinguish the bulletin boards for the two sub-cases, namely for $\Omega = g^{ab}$ and $\Omega = g^{ab}g^t$, then D can also distinguish between the three plausible values of Ω.

Using the above method, we can prove the lemma for the second case as well. The proof is almost same as above. However, in this case, the distinguisher will have to set $c_{\alpha r} = g^{aK_1}/\Omega$ and $c_{\beta r} = g^{bK_2}\Omega/g^t$. Everything else should remain same. So, if $\Omega = g^{ab}$, we will have $v_{\alpha r} = 0$ and $v_{\beta r} = -1$. Alternatively, if $\Omega = g^{ab}g^t$, we will have $v_{\alpha r} = -1$ and $v_{\beta r} = 0$. The proofs for the second and other cases are omitted as they easily follow the proof for the first case. □

The security of the M2M-REP reputation protocol under the DDH assumption is proved in Lemma that proves the security of multi-party computation under Assumption 3 . Hence, the protocol is secure under the DDH assumption.

Assumption 3. *Let* $g^{a_i}, g^{b_i}, i = 1, 2, \dots, t$ *be given. Also let,* $\Omega_1 = (l_1, l_2, \dots, l_{t+1}), \Omega_2 = (l'_1, l'_2, \dots, l'_{t+1})$*, where* $l_i = g^{a_ib_i}g^{m_i}$ *and* $l'_i = g^{a_ib_i}g^{n_i}, i = 1, 2, \dots, t$ *and* $l_{t+1} = \frac{1}{\prod_{j=1}^{t} g^{a_ib_i}}g^{m_{t+1}}, l'_{t+1} = \frac{1}{\prod_{j=1}^{t} g^{a_ib_i}}g^{n_{t+1}}$*. Again assume,* $g^{\sum_{i=1}^{t+1} m_i} \overset{c}{\approx} g^{\sum_{i=1}^{t+1} n_i}$*. Now, given* $\Omega \in \{\Omega_1, \Omega_2\}$*, it is hard to decide whether* $\Omega = \Omega_1$ *or* $\Omega = \Omega_2$*.*

Lemma 4. *DDH assumption implies assumption 3.*

Proof. According to the DDH assumption given g, g^{a_i}, g^{b_i}, $g^{a_i b_i} \overset{c}{\approx} R$. Hence, $g^{a_i b_i} g^{m_i} \overset{c}{\approx} R \overset{c}{\approx} g^{a_i b_i} g^{n_i}, \forall i \in [t]$. Hence, $\Omega_1 = (l_1, l_2, \ldots, l_{t+1}) = (g^{a_1 b_1} g^{m_1}, g^{a_2 b_2} g^{m_2}, \ldots,$ $g^{a_t b_t} g^{m_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i}} g^{m_{t+1}}) \overset{c}{\approx} (g^{a_1 b_1} g^{m_1}, g^{a_2 b_2} g^{m_2}, \ldots,$ $g^{a_t b_t} g^{m_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i} g^{m_i}} g^{\sum_{i=1}^{t+1} m_i}) \overset{c}{\approx} (R_1, R_2, \ldots, R_t,$ $\frac{1}{\prod_{j=1}^{t} R_i} g^{\sum_{i=1}^{t+1} m_i}) \overset{c}{\approx} (R_1, R_2, \ldots, R_t, \frac{1}{\prod_{j=1}^{t} R_i} g^{\sum_{i=1}^{t+1} n_i})$ $\overset{c}{\approx} (g^{a_1 b_1} g^{n_1}, g^{a_2 b_2} g^{n_2}, \ldots, g^{a_t b_t} g^{n_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i} g^{n_i}} g^{\sum_{i=1}^{t+1} n_i})$ $\overset{c}{\approx} (g^{a_1 b_1} g^{n_1}, g^{a_2 b_2} g^{n_2}, \ldots, g^{a_t b_t} g^{n_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i}} g^{n_{t+1}})$ $= (l'_1, l'_2, \ldots, l'_{t+1}) = \Omega_2$. □

In Lemma 5, we extend the results of Lemma 2 and 3. In Lemma 2 and 3, we considered the privacy of two honest users having the same weight in a setting where all other participants are corrupted by the adversary. In Lemma 5, we consider the scenario where there are a number of honest participants each one having a distinct weight. Here, we also show that the adversary is strictly limited to learn the weighted sum of the inputs of the uncompromised participants. Let, $V_1, V_2, \ldots, V_t$ be the t uncompromised participants, with weights equal to $w_1, w_2, \ldots, w_t$, and inputs equal to $v_1, v_2, \ldots, v_t$, then the adversary can only compute $\sum_{i=1}^{t} w_i v_i$. This is a linear equation where w_i's are public and v_i's can be only -1, 0 or 1. Note that, the adversary can compute the same by subtracting the weighted sum of the inputs of the compromised participants from the weighted sum of all inputs. That is, the adversary will not learn anything extra other than the output of the protocol. In other words, our protocol does not divulge any information that the adversary cannot deduce from the final output of the protocol. Thus, our scheme is secure.

Lemma 5. *Let us assume that the adversary $\mathcal{A}$ colludes with peers in the set $S_{\mathcal{A}} = \{P_i : i \in [k]\}$ for some arbitrary k. Let,*

$$M = \begin{bmatrix} v_{11} & v_{21} & \cdots & v_{k1} & v_{k+11} & v_{k+21} & \cdots & v_{n1} \\ v_{12} & v_{22} & \cdots & v_{k1} & v_{k+12} & v_{k+22} & \cdots & v_{n2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1k} & v_{2k} & \cdots & v_{kk} & v_{k+1k} & v_{k+2k} & \cdots & v_{nk} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1n} & v_{2n} & \cdots & v_{kn} & v_{k+1n} & v_{k+2n} & \cdots & v_{nn} \end{bmatrix}$$

$$M' = \begin{bmatrix} v_{11} & v_{21} & \cdots & v_{k1} & v'_{k+11} & v'_{k+21} & \cdots & v'_{n1} \\ v_{12} & v_{22} & \cdots & v_{k1} & v'_{k+12} & v'_{k+22} & \cdots & v'_{n2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1k} & v_{2k} & \cdots & v_{kk} & v'_{k+1k} & v'_{k+2k} & \cdots & v'_{nk} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1n} & v_{2n} & \cdots & v_{kn} & v'_{k+1n} & v'_{k+2n} & \cdots & v'_{nn} \end{bmatrix}$$

Also assume that $\sum_{i=k+1}^{n} t_i v_{ij} = \sum_{i=k+1}^{n} t_i v'_{ij}, \forall j \in [n]$. The adversary $\mathcal{A}$ will not be able to distinguish between the two bulletin boats corresponding to the two sets of local trust values M and M'.

Proof. Let us denote the compromised participants as $P_1, P_2, \ldots, P_\kappa$. The adversary chooses the critical parameters for all the compromised participants. This includes the scores and the secret keys. So, the adversary $\mathcal{A}$ can compute the feedbacks for all the compromised participants. Let us also assume that the secret key of P_i is $(x_{i1}, x_{i2}, \ldots, x_{in})$ and the corresponding public key is $(g^{x_{i1}}, g^{x_{i2}}, \ldots, g^{x_{in}})$. Hence the feedback of $P_i, i \in [k+1, n]$ will be $C_i = (c_{i1}, c_{i2}, \ldots, c_{in})$ when M is used as the matrix of local trust values. We again assume that the feedback of P_i is $C'_i = (c'_{i1}, c'_{i2}, \ldots, c'_{in})$ when M' is the matrix of local trust values. Here, $c_{ij} = g^{x_{ij} y_{ij}} g^{t_i v_{ij}}$ and $c'_{ij} = g^{x_{ij} y_{ij}} g^{t_i v'_{ij}}; \forall i, j \in [n]$. We know that $g^{x_{nj} y_{nj}} = \frac{1}{\prod_{k=1}^{n-1} g^{x_{kj} y_{kj}}}, \forall j \in [n]$. Hence, $c_{nj} = \frac{g^{t_n v_{nj}}}{K_j \prod_{k=\kappa+1}^{n-1} g^{x_{kj} y_{kj}}}$. According to the assumption $\sum_{i=k+1}^{n} t_i v_{ij} = \sum_{i=k+1}^{n} t_i v'_{ij}, \forall j \in [n]$. Now, from Assumption 3, we can say $(c_{k+1j}, c_{k+2j}, \ldots,$ $c_{nj} K_j) \overset{c}{\approx} (g^{x_{k+1j} y_{k+1j}} g^{t_{k+1} v_{k+1j}}, g^{x_{k+2j} y_{k+2j}} g^{t_{k+2} v_{k+2j}}, \ldots,$ $g^{x_{n-1j} y_{n-1j}} g^{t_{n-1} v_{n-1j}}, \frac{g^{t_n v_{nj}}}{\prod_{z=k+1}^{n} g^{x_{zj} y_{zj}}})$ $\overset{c}{\approx} (g^{x_{k+1j} y_{k+1j}} g^{t_{k+1} v'_{k+1j}}, g^{x_{k+2j} y_{k+2j}} g^{t_{k+2} v'_{k+2j}}, \ldots, g^{x_{n-1j} y_{n-1j}}$ $g^{t_{n-1} v'_{n-1j}}, \frac{t_n v'_{nj}}{\prod_{z=k+1}^{n} g^{x_{zj} y_{zj}}}) = (c'_{k+1j}, c'_{k+2j}, \ldots, c'_{n-1j}, c'_{nj} *$ $K_j)$. Hence the lemma holds. □

5.3. Integrity Analysis

We analyze the privacy of collaborating participants in two aspects: first the adversary does not know the trust scores of the collaborating participants, and second, the scores on the bulletin board are unlinkable. Each participant can have the global reputation of machines from the public bulletin board, which could not be used in correlation with information from other participants to infer the local trust scores of the target participants and their relationship network (which participants are connected with which machines). The published feedback on the bulletin board is the valid score of either $-1, 0$, or 1 in the following format $g^{xy} g^{v}$ for $v = -1, 0$, or 1. The associated 1-out-of-3 NIZK reveals nothing more than the statement of feedback correctness: the v is either $-1, 0$, or 1. The encrypted trust score ensures that participating users would not learn anything about the feedback except the final aggregated reputation score. The final global reputation is public on the public bulletin board, and it is impossible to ensure the privacy of feedback if exceptionally all participants collaborate with each other against the target participant, but this is an extreme scenario. The feedback values are fully protected if the adversary colludes with only a few interacted machines of the target participant as shown by Lemma 5.

6. Complexity Analysis and Evaluation

In this section, first, we analyze the complexity of protocol operations of M2M-REP, and then provide the prototype implementation to analyze the computation and bandwidth overhead.

6.1. Complexity Analysis

Table 2 presents the computational and communication complexity of the protocol for the user and the ag-

Entity	Computational overhead			Communication overhead		
	Keys	feedback	NIZK Proof	Keys	feedback	NIZK Proof
Participant	$O(n)$	$O(n)$	$O(n)$	$O(n)$	$O(n)$	$O(n)$
Aggregator	-	$O(n)$ brute force search	$O(n^2)$	$O(n^2)$	$O(n^2)$	$O(n^2)$

Table 2: Computational and Communication Complexity of Cryptographic Operations of M2M.

Proposal	Architecture	Adversarial Model	Privacy	Complexity
Kamvar et al. [14]	Decentralized	Honest	privacy not protected	O(logn)
Zhai et al. [30]	Distributed	Honest	depends on selected peers	O(logn)+O(logn)
Bethencourt et al. [12]	Centralized	Malicious	depends on trusted party	O(1)
Stefanos et al. [66]	Decentralized	Semi-honest	protects privacy	- -
Clark et al. [67]	Decentralized	Semi-honest	protects privacy	- -
Hasan et al. [37]	Decentralized	Malicious	depends on preselected peers	O(n)+(logN)
Androulaki et al. [36]	Decentralized	Semi-honest	compromised if users collude	O(n)
Gudes et al. [35]	Decentralized	Semi-honest	depends on witness peers	O(n^2)+O(N)
Nitti et al. [41]	Distributed	Honest	privacy not protected	- -
Chen et al. [43]	Distributed	Honest	privacy not protected	- -
Yan et al.[34]	Centralized	Semi-honest	privacy protected	O(N)
Hasan et al. [13]	Decentralized	Semi-honest	depends on preselected peers	O(n)
Nithyanand et al.[48]	Distributed	Semi-honest	privacy protected	O(N^2)
Pavlov et al. [47]	Distributed	Semi-honest	privacy depend on witness peers	O(N^3)
Lin et al. [38]	Distributed	Honest	privacy not protected	O(n^2)
M2M-REP	**Decentralized**	**Malicious/Semi-honest**	**protects privacy**	**O(n)+O(n)**

Table 3: Comparison of M2M Reputation System with other Centralized and Decentralized Reputation Systems.n is the number of users and N is preselected or witness peers.

gregator. At the user side, the protocol requires n exponentiations to generate the keys (public, private and restructured), and the cryptograms of trust score, and $11n$ exponentiations to generate the proof of knowledge of the secret key and the well-formedness proofs. Here, n is the total number of machines in the network. Similarly, the aggregator requires $O(n^2)$ for the verification of the well-formedness and $O(n)$ for the computation of final global reputation score. In aggregate, the total computational cost for generating the cryptogram (feedback and NIZK) is $O(n)+O(n)$. In terms of bandwidth, the protocol incurs the following costs for reporting the cryptograms to the bulletin board at the user side: $O(n)$ bandwidth is required for exchanging the keys, $O(n)$ for the exchange of participants identities, $O(n)$ for the encrypted trust scores, and $O(n)$ for exchanging the non-interactive zero-knowledge proof.

In Table 3, we compare the M2M-REP system with centralized and decentralized privacy preserving reputation schemes with respect to computational complexity, system architecture, adversarial model and the privacy implication of the system. From Table 3, we can observe that our approach achieves acceptable computational overhead when compared to other reputation systems for the malicious models e.g. the approach of Hasan et al. has a computation complexity of $O(n + logN)$, but requires a pre-trusted set of users for the privacy protection and the approach of Bethencourt et al. [12] that requires a trusted centralized system for receiving and aggregation of feedback from clients.

6.2. Prototype Implementation

We now evaluate the performance of the M2M-REP system. We implemented cryptographic operations of M2M-REP in Java using the bouncy castle cryptographic library. We used the standard NIST Curve P-256 [68] and SHA-512 for 128-bit security. The experiments were performed on an Intel i-7 CPU (3.4GHz) system, having 8GB memory with a Windows 10 operating system. The implementation consists of two parts. 1) The client-side module that computes and reports cryptograms of trust scores to the bulletin board, and 2) the aggregator module that computes aggregated reputation of machines by utilizes cryptograms from the bulletin board. The functionalities of the client and the aggregator are implemented as separate Java modules, and the bulletin board is implemented as a web server.

At the client side, the computation time is measured for three major operations: 1) generating the encryption keys (private, public, and restructured public keys), 2) creating a cryptogram of trust score, and 3) generating a non-interactive zero-knowledge proof of well-formedness. At the aggregator side, the evaluation is performed for computing the global reputation.

6.3. Computation Runtime

We begin by analyzing the amount of CPU time required to compute the cryptograms at the client side for a varied number of machines. The computation time at the client side depends on three major operations: generating cryptographic parameters (public, private and restructured keys), creating a cryptogram of trust score and

the NIZK proof. We evaluate the performance over the single core of Intel 3.4GHz CPUs with 8GB of memory. The number of machines is varied from 100 to 100K. We iterate experiments 10 times and report the average computation time. Figure 3.A presents the computational run time required for generating the cryptograms with the different number of machines. We observe that the time required to generate the cryptograms for 1000 machines is around less than 50 seconds, however, it increases linearly with the number of machines in the aggregation time window. The computation time is acceptable as normally a large number of participants only interact with a small subset of machines. The key generation and encryption are very efficient operations since they only involve simple computations. On the other hand, generating a NIZK proof is the most expensive operation as it requires 10 modular exponentiations for generating and making the proof non-interactive, respectively. If we exclude the NIZK proof (i.e. if we consider only honest but curious model) then the computation time required even for a large number of machines reduces to around 200 seconds i.e. for 100K machines. M2M-REP operations can be parallelized and implemented over multiple cores. The parallelization of computation over multiple cores would significantly reduce the computation time within acceptable bounds even for a very large number of machines.

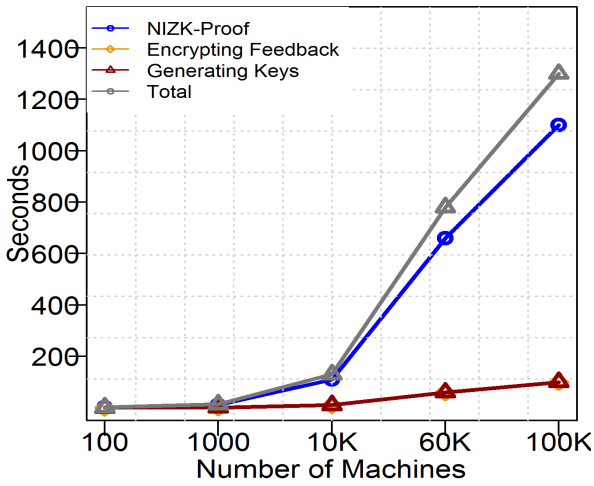
At the aggregator side, the time required for computing the aggregated reputation score for 100K responses is around 100 seconds which can also be reduced further by parallelization of computation over multiple cores.

6.4. Communication Bandwidth

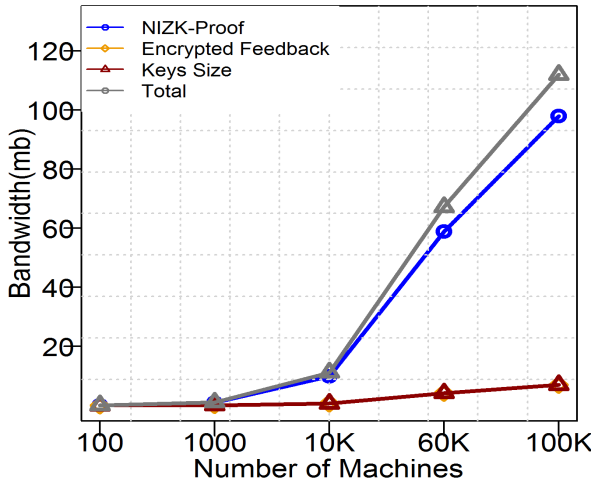
Regarding the bandwidth overhead, each participant needs to send the public keys, the cryptograms of trust scores and the associated NIZK proofs of cryptogram's well-formedness to the public bulletin board. This results in a bandwidth overhead of around less than 20MB if the client provides feedback for 1000 machines in the network as shown in Figure 3.B. Generations of the keys and the encrypted feedbacks are lightweight operations. The computation of NIZK proofs in the feedback phase is the most expensive operation. The use of NIZK proofs of well-formedness brings the benefit of not allowing the malicious participant to significantly influence the aggregation process. The bandwidth overhead also increases linearly with the number of machines. Specifically, for the 100K machines, this results in a bandwidth of around 120MB. It can be observed that the'honest but curious' model would not incur high communication overhead.

7. Salient Features and Limitations

In this section, we outline main features of the proposed system and its limitations.



(a) Computation Runtime



(b) Communication Bandwidth

Figure 3: Computation and Communication Cost for the Feedback provider.

7.1. Features of The Protocol

The main features of the protocol are as follows:

1. The encrypted direct trust scores of participants (feedbacks for their interacted machines) are available on the public bulletin board, which can be used by anyone to deduce the aggregated reputation of the machine. The requesting participant does not require to ask her friends about the reputation of unknown peers, instead, she has to query the bulletin board for the updated reputation of any machine in the network. Further, the reputation of any machine can be computed any time whether the feedback provider is online or offline. The participant can also verify the well-formedness of input scores and reputation scores without learning anything about participants. The system ensures privacy-preservation at every stage of computation.
2. The system does not ensure that the participating users are providing honest recommendations (i.e. a

machine provided honest content but may be rated by some others as being malicious intentionally). It assumes that participants act honestly while selecting their feedback scores. However, all the participants are strictly limited to providing within-range inputs (i.e. values of 0, -1 and 1) and are required to demonstrate this by means of zero-knowledge proofs of well-formedness of feedbacks. The well-formedness proofs of trust score do not allow participants to report out-of-range trust scores. This would prevent participants from maliciously increasing or decreasing reputation of some specific machines. Furthermore, the collaborating participant cannot alter or delete already submitted trust scores available on the bulletin board.

3. The collaborating participants do not require to remain online during the aggregation process. The participant can submit the direct score and leave the network without deleting their data on the bulletin board or reassigning any of their unfinished tasks to other participants.

7.2. Limitations

The M2M-REP system restricts participants from presenting invalid feedback through the usage of proofs of well-formedness. However, it does not provide any mechanism for demonstrating whether the feedback providers have indeed had transactions with the machine or not. This limitation can be addressed through the use of unique token issued to the feedback provider, but generating such a token without a trusted system in a decentralized network is a challenging task. In this setup, the feedback is only posted on the bulletin board if the participants prove holding of a token. We are looking into the possible ways to generate the unique token and its associated zero-knowledge proof to ensure that the feedback provider is a valid participant. The current design of M2M-REP system does not offer any personalization, i.e. it does not allow appraisal of feedback scores from a finite subset of all participants. As part of our future work, we are looking into methods of improving this baseline method so that the requester or the aggregator can select a subset of feedback providers without letting them know while ensuring the preservation of the privacy and security properties. This can be analogous to the schemes for collaborative filtering and collaborative recommendation with privacy-preservation.

8. Conclusion

M2M-REP is a privacy-preserving decentralized reputation system for evaluating the trustworthiness of machines in the autonomous M2M communication system. Specifically, the trustworthiness of machines is computed by aggregating the direct trust scores obtained from the users, who already have had interactions with the machines. We achieve properties relating to privacy-preservation through the use of secure multi-party computation techniques. The system exhibits the following properties: 1) the computation operations of M2M are decentralized and no trusted authority is required for preserving the participant privacy, 2) the participants cannot provide out-of-range encrypted trust scores which diminishes the freedom of malicious participants, 3) it incurs reasonable communication and computation overheads with the added benefit of privacy protection under the malicious adversarial model, and 4) it provides public verifiability of computation. We prototype the functionalities of this system in order to evaluate the computation and communication overhead. Our reputation scheme has minimal computation and communication overheads with the additional properties of decentralization, verification, and privacy preservation under the malicious adversarial model.

Acknowledgment

Muhammad Azad, Samiran Bag, and Feng Hao are supported by the ERC Starting Grant, No. 306994. We thank the anonymous reviewers for their invaluable comments and suggestions towards improving this paper.

References

[1] D. Evans, "The internet of things how the next evolution of the internet is changing everything," *White Paper Cisco Internet Business Solutions Group (IBSG)*, 2011.

[2] "Gartner says the internet of things installed base will grow to 26 billion units by 2020." 2017. [Online]. Available: http://www.gartner.com/newsroom/id/2636073.

[3] "Cellular m2m forecasts: unlocking growth cellular m2m connections forecast to reach 1 billion by 2020, GSMA Report," 2015.

[4] J. Worner, "Focused delivery of key market enablers in 2017/18," 2017. [Online]. Available: https://www.gsma.com/iot/newscat/mautomative-newscat/

[5] (2017) Gartner says by 2020, a quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities. [Online]. Available: http://www.gartner.com/newsroom/id/2970017.

[6] I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in m2m communication," *IEEE Vehicular Technology Magazine*, vol. 4, no. 3, pp. 69–75, Sept 2009.

[7] "Fridge sends spam emails as attack hits smart gadgets, BBC News," 2014. [Online]. Available: http://www.bbc.co.uk/news/technology-25780908

[8] X. Lin, "Cat: Building couples to early detect node compromise attack in wireless sensor networks," in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, Nov 2009, pp. 1–6.

[9] F. Gómez Mármol and G. Martínez Pérez, "Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, May 2012.

[10] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25 408–25 420, 2017.

[11] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[12] J. Bethencourt, E. Shi, and D. Song, "Signatures of reputation: Towards trust without identity," in *Proceedings of the 14th International Conference on Financial Cryptography and Data Security*, ser. FC'10, 2010, pp. 400–407.

[13] O. Hasan, L. Brunie, and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems," *Computer and Security*, vol. 31, no. 7, pp. 816–826, Oct. 2012.

[14] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International Conference on World Wide Web*, ser. WWW '03, 2003, pp. 640–651.

[15] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[16] L. De Alfaro, A. Kulshreshtha, I. Pye, and B. T. Adler, "Reputation systems for open collaboration," *ACM Communications*, vol. 54, no. 8, pp. 81–87, Aug. 2011.

[17] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," *Journal of Parallel and Distributed Computing*, vol. 75, no. Supplement C, pp. 184 – 197, 2015.

[18] S. Bag, M. A. Azad, and F. Hao, "A privacy-aware decentralized and personalized reputation system," *Computers & Security*, 2018.

[19] M. Azad and R. Morla, "Rapid detection of spammers through collaborative information sharing across multiple service providers," *Future Generation Computer Systems*.

[20] M. Sirivianos, K. Kim, and X. Yang, "Socialfilter: introducing social trust to collaborative spam mitigation," in *Proceedings of Workshop on Collaborative Methods for Security and Privacy (collSec)*, 2010.

[21] M. A. Azad, S. Bag, S. Tabassum, and F. Hao, "privy: Privacy preserving collaboration across multiple service providers to combat telecoms spam," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1–1, 2017.

[22] M. A. Azad and S. Bag, "Decentralized privacy-aware collaborative filtering of smart spammers in a telecommunication network," in *Proceedings of the Symposium on Applied Computing*, ser. SAC '17, 2017, pp. 1711–1717.

[23] E. Damiani, S. D. C. D. Vimercati, S. Paraboschi, and P. Samarati, "Managing and sharing servants' reputations in p2p systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, no. 4, pp. 840–854, 2003.

[24] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for fast reputation aggregation in peer-to-peer networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 9, pp. 1282–1295, Sep. 2008.

[25] S. Steinbrecher, "Enhancing multilateral security in and by reputation systems," in *The Future of Identity in the Information Society*, 2009.

[26] S. Clauß, S. Schiffner, and F. Kerschbaum, "K-anonymous reputation," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, 2013, pp. 359–368.

[27] S. Marti and H. Garcia-Molina, "Identity crisis: anonymity vs reputation in p2p systems," in *Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003)*, Sept 2003, pp. 134–141.

[28] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2009, pp. 173–187.

[29] ——, "Robust de-anonymization of large sparse datasets," in *Proceedings of 29th IEEE Symposium on Security and Privacy (sp 2008)*, 2008, pp. 111–125.

[30] E. Zhai, D. I. Wolinsky, R. Chen, E. Syta, C. Teng, and B. Ford, "Anonrep: Towards tracking-resistant anonymous reputation," in *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, 2016, pp. 583–596.

[31] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *ICT Systems Security and Privacy Protection*, 2016, pp. 398–411.

[32] Z. Li and C. T. Chigan, "On joint privacy and reputation assurance for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2334–2344, 2014.

[33] P. Dewan and P. Dasgupta, "P2p reputation management using distributed identities and decentralized recommendation chains," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 7, pp. 1000–1013, 2010.

[34] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos, "Two schemes of privacy-preserving trust evaluation," *Future Generation Computer Systems*, vol. 62, pp. 175 – 189, 2016.

[35] E. Gudes, N. Gal-Oz, and A. Grubshtein, "Methods for computing trust and reputation while preserving privacy," in *Proceedings of 23rd Annual IFIP WG 11.3 Working Conference Data and Applications Security*, 2009, pp. 291–298.

[36] E. Androulaki, S. G. Choi, S. M. Bellovin, and T. Malkin, "Reputation systems for anonymous networks," in *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies*, 2008, pp. 202–218.

[37] O. Hasan, L. Brunie, E. Bertino, and N. Shang, "A decentralized privacy preserving reputation protocol for the malicious adversarial model," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 949–962, June 2013.

[38] L. Liu, M. Loper, Y. Ozkaya, A. Yasar, and E. Yigitoglu, "Machine to machine trust in the iot era," in *Proceedings of the 18th International Conference on Trust in Agent Societies - Volume 1578*, 2016, pp. 18–29.

[39] R. Zhou and K. Hwang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions Parallel Distributed Systems*, vol. 18, no. 4, pp. 460–473, Apr. 2007.

[40] M. A. Azad, S. Bag, and F. Hao, "M2m-rep: Reputation of machines in the internet of things," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 28:1–28:7.

[41] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[42] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 53–59, April 2011.

[43] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "Trm-iot: A trust management model based on fuzzy reputation for internet of things," *Computer Science and Information Systems*, vol. 8, pp. 1207–1228, 2011.

[44] I. Stojmenovic, "Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 122–128, April 2014.

[45] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of 2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 238–243.

[46] M. Joye and B. Libert, "A scalable scheme for privacy-preserving aggregation of time-series data," in *Proceedings of 17th International Conference on Financial Cryptography and Data Security*, 2013, pp. 111–125.

[47] E. Pavlov, J. S. Rosenschein, and Z. Topol, "Supporting privacy in decentralized additive reputation systems," in *Proceedings of Second International Conference on Trust Management*, C. Jensen, S. Poslad, and T. Dimitrakos, Eds., 2004, pp. 108–119.

[48] N. Rishab and R. Karthik, "Fuzzy privacy preserving peer-to-peer reputation management," *IACR Cryptology ePrint Archive*, 2009.

[49] T.Dimitriou and A.Michalas, "Multi-party trust computation in decentralized environments in the presence of malicious adversaries," *Ad Hoc Networks*, vol. 15, pp. 53 – 66, 2014.

[50] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc net-

works," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[51] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[52] B. Parno and A. Perrig, "Challenges in securing vehicular networks,," *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), 2005.*

[53] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proceedings of the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, 2005, pp. 109–117.

[54] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in edge-of-things," *Future Generation Computer Systems*, vol. 85, pp. 190 – 200, 2018.

[55] Z. Meng, Z. Wu, C. Muvianto, and J. Gray, "A data-oriented m2m messaging mechanism for industrial iot applications," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 236–246, Feb 2017.

[56] I. R. Chen, J. Guo, and F. Bao, "Trust management for soa-based iot and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, May 2016.

[57] F. Hao, P. Y. A. Ryan, and P. Zielinski, "Anonymous voting by two-round public discussion," *IET Information Security*, vol. 4, no. 2, pp. 62–67, June 2010.

[58] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[59] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proceedings of Advances in Cryptology CRYPTO' 86*, 1987, pp. 186–194.

[60] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf."

[61] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, 2018.

[62] P. McCorry, S. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proceedings of 21st Financial Cryptography and Data Security*, 2017.

[63] C. Culnane, J. Heather, S.Schneider, and Z.Xia, "Software design for vec vvote system," *Surrey Computing Sciences Report CS-13-01*, 2013.

[64] A. Essex, "Cryptographic end-to-end verifiability for real-world elections by," *PhD thesis University of Waterloo*, 2012.

[65] F. Hao, M. N. Kreeger, B. Randell, D. Clarke, S. F. Shahandashti, and P. H.-J. Lee, "Every vote counts: Ensuring integrity in large-scale electronic voting," *USENIX Journal of Election Technology and Systems (JETS)*, pp. 1–25, 2014.

[66] O. Stefanos, T. Litos, and D. Zindros, "Trust is risk: A decentralized financial trust platform," *Proceedings of 21st Financial Cryptography and Data Security 2017*, 2017.

[67] M. R. Clark, K. Stewart, and K. M. Hopkinson, "Dynamic, privacy-preserving decentralized reputation systems," *IEEE Transactions on Mobile Computing*, vol. 16, no. 9, pp. 2506–2517, 2017.

[68] "Digital signature standard (dss), u.s. department of commerce/national institute of standards and technology." 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.