An Edge Based Attack Detection Model (EBAD) for Increasing the Trustworthiness in IoT Enabled Smart City Environment

R. I. MINU¹, (Member, IEEE), G. NAGARAJAN², (Senior Member, IEEE), ASMAA MUNSHI³,
K. VENKATA CHALAM⁴, (Senior Member, IEEE), WAFA ALMUKADI⁵,
AND MOHAMED ABOUHAWWASH⁶,7

¹Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur 603203, India
²Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, India
³Cybersecurity Department, University of Jeddah, Jeddah 23218, Saudi Arabia
⁴Department of Applied Cybernetics, University of Hradec Králové, 500 03 Hradec Králové, Czech Republic
⁵Department of Software Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia
⁶Mathematics Department, Faculty of Science, Mansoura University, Mansoura 35516, Egypt
⁷Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI 48824, USA

Corresponding author: Mohamed Abouhawwash (abouhaww@msu.edu)

ABSTRACT Several massive real-time services could be offered to the residents of smart cities by the incorporation of collaborative applications. All such applications require latency-aware network services for accomplishing various needs of the smart city environment. It requires technological enhancements to the existing mechanisms to serve better in smart environments. Such enhancements to the prevailing approaches also opened a wide range of chances to the intruders. Among such infringes, the identity-based attack is the most powerful attack, which may directly affect the credibility of legitimate network components. Such attackers aim to steal the identity of other legitimate entities. Thus, the prevailing trust-based approaches cannot withstand such attacks. The proposed Edge-based approach, EBAD has been designed for smart city environments, as a robust prevention mechanism for identity theft and misuse. EBAD is efficient enough to identify the Sybil attacker nodes and the early identification of such attacker nodes will nullify the probability of performing the Sybil attack over a Cooperative blackmailing attack (SA-CBA). EBAD uses an Edge-based accusation analysis approach to assess the malicious behavior of the network entities. The major part of the required computations has been placed at the edge node for reducing the computational overload of the end devices. Finally, the efficiency of EBAD has been examined under a malicious environment.

INDEX TERMS Edge computing, IoT, MEC, smart cities, Sybil attack.

I. INTRODUCTION

Smart Cities have been designed to uplift the life style of their residents. It could make a drastic change in the living environment with the help of Cloud computing. Several heterogeneous IoT devices are needed to meet the requirements for developing a smart city [1]. The large level deployment of highly efficient end devices is not always economically possible. Thus the end devices will have only a small scale computational capacity. Such devices may encounter serious security breaches due to resource unavailability to execute complex securing algorithms. Cloud computing cannot offer such security level services to the underlying network entities in an effective manner. Also, applications that demand real-time responses cannot be successfully deployed inside the smart city environment only by entrusting cloud servers.
The traditional Cloud-based architecture is not capable to serve such real-time applications due to high network latency and bandwidth issues [2]. Thus an edge-based computation approach is suitable for smart city environments for getting latency-free responses. The bandwidth-related issues can also be addressed by deploying the tiny Edge devices. Large-scale deployment of such devices will ensure service availability, resource availability, reduced latency, bandwidth availability, and cloud-independent data processing. An edge device is capable to offer all the services which had been done previously by the cloud server. A detailed report may be sent to the cloud server when the application or cloud server demands the same. The real-time data-dependent applications can run smoothly over Edge-based paradigm [3]. The smart city covers several potential areas like healthcare, education, smart transportation, etc., which handles highly sensitive real-time data. Thus security has become the prime requirement in IoT based Smart City environment. The deployment of tiny resource-limited IoT devices and Edge devices also increased the issues related to privacy and security. The attacks on network identities have become a major threat to privacy [4]. In identity-based attacks, the attacker masquerades as another legitimate entity. Thus identity-based individual monitoring of network entities cannot ensure the trustworthiness of the network. Such findings may mislead the network and finally turn into a reason for the complete network collapse. The identity-based attacks can be expected from both inside and outside the network. The identity-based attacks emerging from the outside network can be successfully prevented by incorporating a secure certificate scheme. But, inside attacking nodes will use the pilfered identities of already certified network entities. The certificate-based mechanism is not capable to identify such internal identity-based attacks [5]. Thus, the main threat to the network is insider attacks. In this case, some new mechanisms need to be incorporated to successfully prevent such attacks. Sybil attack is an example of an identity-based attack. The Sybil attacker node can perform any other attacks once it gets control over other legitimate devices. The impact will be worst when such attacker nodes join together to execute a Co-operative Blackmailing Attack [6]. This will increase the misdetection and the genuine devices may be marked as malicious. That will in turn destroy the network. The IoT-enabled networks handle highly sensitive data [7]. The chances of information leakage can be successfully prevented by using any encryption algorithms [8]. The proposed method possesses an accusation-based mechanism where each node is allowed to accuse any suspicious neighboring nodes. Thus, all the existing attacks over accusation/voting-based mechanisms can be expected in the proposed framework. The work aims at identifying and eliminating all such attacks efficiently. Such attacks can be classified into three categories. The first category includes the attacks from single malicious nodes. EBAD possesses a trust-based accused node analysis approach to defend against all such single node attacks. It includes false accusation contribution, false data circulation, misleading attacks, etc. The second category of attack is the parallel attacks from a group of nodes. The framework examines the effect of cooperative attacks over accusation-based approaches. Also, EBAD proposes an edge-based three-level assessment approach for identifying the cooperative behavior of the attacker nodes. The third level attack is the most critical attack over accusation-based attacks. It is a hybrid attack, where the single/co-operative attacks will be performed by maliciously compromised Sybil attacker nodes over an accusation-based mechanism. EBAD confirms the Sybil behavior of the attacker nodes by computing the malicious free weighted aggregate trust value of the suspicious nodes. EBAD framework has adequate techniques to withstand all the above-mentioned three categories of attacks. The paper deals with the following:

- Contributes a robust malicious node identification mechanism.
- Contributes a method to identify the fake accusations emerging from maliciously compromised single nodes and Co-operative attacking nodes.
- Contributes an Edge based approach for analyzing the received accusations to detect the Sybil behaviour of a node.
- Contributes a trust-based method to verify the malicious nature of the suspecting node.
- Contributes a stable framework for the avoidance of attacks performed by Sybil nodes, especially the Co-operative Blackmailing Attack.

Section 2 of this paper analyses the research gaps present in the above-mentioned issues. Section 3 illustrates the architecture of EBAD. The proposed framework has been detailed in section 4. Section 5 examines the efficiency of EBAD by comparing the same with existing works. Section 6 concludes the work and discusses the future scope.
for detecting their attacking behavior. The Sybil attack over any other attacks needs to be evaluated carefully.

III. PROBLEM STATEMENT AND SYSTEM ARCHITECTURE

The IoT-based network mostly adopts an accusation or voting-based scheme to ensure the overall trust of the network. Every node will continuously assess its neighbors based on their involvement in the network activities. Also, they will immediately send accusations against malicious nodes. The trustworthiness of such accusations can be ensured by keeping a limit on the number of required accusations from different nodes for eliminating an accused node from the network. But, the same attack can be performed by utilizing the cooperative behavior of malicious nodes (Co-operative Blackmailing attack). In this case, the malicious nodes can contribute more accusations about a single legitimate node. The accused node will be eliminated from the network if the accusation count is satisfactory. But, this kind of attack can be prevented by trust-based individual node assessment. In Sybil Attack, a single entity will claim the identity of more than one legitimate entity. The identity-based individual node assessment will not be capable to identify the original culprit. Also, the existing systems cannot identify the cooperative behavior of the Sybil node which contributes to the false accusation about a legitimate node. The false accusation contribution can be either from a single Sybil node by using more number of identities or from different Sybil nodes. In both cases, the attacker nodes choose a legitimate node and send accusations against the targeted legitimate node by using different identities. The targeted legitimate node will be counted as malicious and the removal of such nodes will become a major threat to the network. Existing approaches fail to identify the cooperative behavior of the Sybil nodes. Figure 1 shows the architecture of EBAD. The group of IoT devices connected to the same Edge node will be considered as a cluster. A single IoT device is allowed to register only with one Edge node, even if they could find more than one Edge node in their range. The nearest edge node will be selected in such cases. All necessary computations will be handled at Edge nodes to reduce the power consumption at individual IoT end devices. The proposed framework is entrusted to identify the Sybil behavior of end-users IoT devices by utilizing the computing capacity of edge devices. The Sybil behavior of such nodes can be easily identified by employing a good trust management mechanism. But, the co-operative attacks from a maliciously compromised Sybil attack need more attention. The proposed framework offers a robust solution to the above-mentioned issue.

IV. PROPOSED METHODOLOGY

The proposed method, EBAD has three major sequential procedures for detecting and confirming the false accusation from a Sybil attacker.

- Trust based Accusation mechanism
- Edge based analysis of received accusations
- Confirming the Sybil behavior by edge node

EBAD uses a trust based accusation mechanism to report the malicious nodes to edge nodes. In order to identify false accusations from a maliciously compromised Sybil node, it executes signal strength evaluation.

A. TRUST BASED ACCUSATION MECHANISM

EBAD uses a recommendation based trust evaluation mechanism. A node will monitor the neighboring nodes (1-hop) occupied in the same cluster. It considers both self recommendation as well as the recommendations from common neighbors while evaluating a neighboring node. The recommendation value is formulated based on the node’s forwarding behavior. The forwarding behavior for both data packets and control packets will be considered for generating recommendations. The recommendation by node \( n_i \), about node \( n_j \) can be calculated by using the (1).

\[
R_{ij} = \frac{op_{ij} - dp_{ij}}{op_{ij}} \quad (1)
\]

where, \( op_{ij} \) is the count of offered packets to \( n_j \) by \( n_i \) and \( dp_{ij} \) is the packets drop experienced at \( n_j \). All nodes in the network will compute the recommendation for all their neighbors by using (1). While calculating the trust value of neighboring node, the assessing node \( n_i \) will consider the recommendations from common neighbors along with self-assessed recommendation (\( SR_{ij} \) (2). The final recommendation-based trust value (\( RT_{ij} \) (4) of a node will be computed based on the received recommendations (\( RR_{ij} \) (3) during last three-time
intervals \((t - \Delta t, t & t + \Delta t)\).

\[
SR_{ij} = \frac{SR_{ij(t-\Delta)} + SR_{ij(t)} + SR_{ij(t+\Delta)}}{3}
\]

\[
RR_{ij} = \frac{\sum_{i=1}^{k} R_{ij(t-\Delta)}}{3k} + \frac{\sum_{i=1}^{l} R_{ij(t)}}{3l} + \frac{\sum_{i=1}^{m} R_{ij(t+\Delta)}}{3m}
\]  

(3)

Since we are considering three set of recommendation values, the set of common neighboring nodes will be different for different time intervals due to mobility. Here \(k, l\) and \(m\) represent the number of common neighbors of \(n_i\) and \(n_j\) during the time intervals \((t - \Delta t, t & t + \Delta t)\) respectively.

\[
RT_{ij} = \frac{SR_{ij} + RR_{ij}}{2}
\]  

(4)

The value of \(RT_{ij}\) lies in a closed interval of 0 and 1. The threshold value for generating accusations has been fixed based on the simulations as 0.6. Node \(n_i\) will send accusation to edge node about its neighboring node \(n_j\), when Recommendation Trust value falls lower than the threshold. The compromised Sybil attacker may generate false accusations against legitimate nodes. Sybil behavior of a network entity needs to be identified as early as possible.

**B. EDGE BASED ANALYSIS OF RECEIVED ACCUSATIONS**

Compromised nodes which perform direct attacks can be easily identified by recommendation based trust value. All such findings will be communicated to the connected edge device as in the form of accusations and the identified nodes will be isolated from further communications. Sometimes the number of reported accusations about a node might be lower. That may happen due to the following three reasons.

- **Case 1:** Lower number of neighboring nodes
  
  Since the trust management mechanism considers only the 1-hop neighbors, only the neighboring nodes can contribute accusations against a compromised node. In some cases, accusation count will be lower than the required count. In such cases, the recommendation trust value of accuser nodes will be evaluated to take the decisions.

- **Case 2:** Less involvement of accused node in the network communications
  
  The recommendation trust mechanism proposed in this work depends on the forwarding behavior of the assessed node. The assessing nodes will get information regarding the same based on the involvement of assessed node in the network communications. Thus, the accusation count may be lower in some cases due to the lower involvement of malicious nodes in network communications. So, the trust value of accuser nodes will also be counted with equal importance while reaching to a conclusion.

- **Case 3:** False accusations emerging from maliciously compromised nodes
  
  In this third scenario, the accusations will be false accusations coming from maliciously compromised nodes. In such cases, the recommendation trust based analysis will reveal the actual behavior of accuser nodes.

All the issues involved with the above-mentioned scenarios can be rectified with the help of recommendation-based trust management. Even the cooperative behavior of malicious nodes can also be identified by the recommendation based trust evaluation. The system fails when such attacks have been emerging from Sybil nodes. Sybil nodes have the capacity to mislead all the routing as well as data related communications. Upon calculating the Recommendation based trust of the actual identity holder, the system will interpret the accusations as genuine accusations and the decisions will be taken accordingly. This work aims at identifying the Sybil attacker nodes while it performs cooperative blackmailing attacks. Thus, the Sybil attacker will be eliminated before it achieves cooperation among the other Sybil nodes. EBAD examines the Sybil behavior by the following steps.

- Signal strength evaluation of received accusations
- Estimation of expected Signal Strength
- Preparation of Temporary Identification List (TIL)

Initially the edge node will calculate the signal strength of reported accusations. Expected signal strength of all the cluster members will also be examined. The possible matches for the signal strength of received accusations from the expected signal strength values will be identified in the second stage. Such identified nodes will be added to TIL. The recommendation trust value of identified nodes will be computed for taking the final decision. All these operations will be done by the Edge node. Thus we could reduce the computational overhead of individual IoT devices. The Signal strength based malicious behavior identification is illustrated in Figure 2.

**FIGURE 2.** The signal strength based malicious behavior identification.
1) SIGNAL STRENGTH EVALUATION OF RECEIVED ACCUSATIONS

The accusations from a Sybil attacker will claim a different identity, but the accuser node cannot maintain the signal strength equivalent to the expected signal strength of claimed identity. Let us assume that a \( p \) number of accusations have been received against a node in the cluster. The accusations/accuser nodes can be represented as \( a_1, a_2, \ldots, a_p \). The received signal strength \( P_r(d) \) of \( i^{th} \) accusation can be evaluated by the following equation (5),

\[
P_r(d) = \frac{P_i}{d_{ei}^k}
\]

where \( i \) represents the \( i^{th} \) accuser node \((e_i, a_i)\). \( P_i \) is the transmission power of the \( i^{th} \) accuser node. \( d_{ei} \) represents the Euclidean distance from Edge server to Accuser node. \( m_r \) is the Relation factor and \( k \) is a Constant. \( d_{ei} \) can be computed as follows, equation (6)

\[
d_{ei} = d_{ei}(x, y) = \sqrt{(x_e - x_i)^2 + (y_e - y_i)^2}
\]

where, \((x_e, y_e)\) represents the Cartesian Co-ordinates of edge node and \((x_i, y_i)\) represents the Cartesian Co-ordinates of the accuser. The relation factor, \( m_r \), depends on the propagation model. In our simulation, we are using Two-ray ground reflection model. Hence, the value of relation factor \( m_r = 4 \). The constant \( k \) is also dependent on the selection of the propagation model. The constant value \( k \) is determined by considering the antenna height of the transmitter, antenna height of the receiver, gain at receiver antenna and gain at transmitter antenna.

2) ESTIMATION OF EXPECTED SIGNAL STRENGTH

Only one accusation will be received from a single node against another node. Thus a \( p \) number of accusations represent \( p \) number of accuser nodes. The accuser nodes of a single node in the cluster can be considered as a subset of total nodes in the cluster \( \{ n_1, n_2, \ldots, n_i, \ldots, n_m \} \). Then, the edge node will send a Hello packet to all the nodes and the reply to messages will be examined by using the (5) for getting the normal expected signal strength of cluster nodes. The expected signal strength of the cluster nodes will be added to a two-dimensional array \( E_{Si} \). The array can be represented as, \( E_{Si} = \{ s_1, s_2, \ldots, s_i, \ldots, s_m \} \). Here \( s_i \) represents the expected signal strength of node \( n_i \).

3) PREPARATION OF TEMPORARY IDENTIFICATION LIST (TIL)

The SA-CBA can be performed either by a single Sybil node or by the cooperation of more than one Sybil nodes. Both modes of attack can be detected by the signal comparison approach. The array of received signal strength values of accuser nodes can be denoted as \( R_{Sj} = \{ r_1, r_2, \ldots, r_j, \ldots, r_p \} \). Here \( r_j \) represents the received signal strength of \( j^{th} \) accuser node. We can find the expected signal strength of \( j^{th} \) accuser nodes from \( E_{Si} \). Let \( s_j \) be the expected signal strength of \( j^{th} \) accuser node. Both values will be compared to find the difference \( \Delta d \), by using the (7).

\[
\Delta d = |r_j - s_j|
\]

A threshold value has been calculated over \( \Delta d \) to determine the suspicious behavior of accuser node. The threshold value, Difference Threshold \( d_{tr} \) will be calculated dynamically by using the (8).

\[
d_{tr} = (s_{i,\text{max}} - s_{i,\text{max}}) \times l
\]

where, \( s_{i,\text{max}} \) represents maximum signal strength received during the last five reception of reply packet from \( i^{th} \) node. \( s_{i,\text{min}} \) represents minimum signal strength received during the last five reception of reply packet from \( i^{th} \) node and \( l \) is a Constant. The constant value \( l \) will be calculated dynamically by considering the transmission power and the distance between the edge node and the accuser node. The received signal strength of all accuser nodes will be validated and the accuser nodes having \( \Delta d \) value greater than \( d_{tr} \) will be listed separately to check Sybil behavior. The received signal strength of such doubtful accuser nodes will be matched with the expected signal strength of all cluster members. Three cluster nodes having expected signal strength in similar range of received signal strength of one accuser node will be identified. All those nodes will be added to a separate list known as Temporary Identification List \( \text{(TIL)} = \{ h_1, h_2, \ldots, h_i \} \). In other words, for each \( a_i \), a set of three nodes will be selected from \( \{ n_1, n_2, \ldots, n_i, \ldots, n_m \} \). If \( n_i, n_j \) and \( n_k \) are the selected nodes for \( a_i \), then \( s_i, s_j \) and \( s_k \) will be in the range of \( r_i \). Since we have assumed \( p \) as the total number of accuser nodes for a single accused node, the size of \( \text{TIL} \) will be smaller than or equal to \( 3 \times p \). If the Sybil attack is emerging from a single compromised malicious node, then the number of nodes in \( \text{TIL} \) will be less and the count of nodes will be high, if the attack happens from multiple Sybil attacker. The overall algorithm for analyzing the received accusations by the edge node is detailed in algorithm 1 (Table 1).

The doubtful accusations need to be evaluated further before reaching to a conclusion. The edge node will examine the nodes listed in TIL to verify the trustworthiness of accusations.

4) CONFIRMING THE SYBIL BEHAVIOR

The edge node will monitor the nodes listed in TIL. The Edge node collects the recommendation trust values from the neighboring nodes of suspicious accuser nodes listed in TIL and computes the aggregated trust value. The received recommendation trust can be stored in a \( (1 \times q) \) matrix, where \( q \) is the total number of 1-hop neighbors of \( n_j \) (9).

\[
RT(e_k, n_j) = [RT_{1j} RT_{2j} \ldots - - RT_{qj}]
\]

The collected recommendations may contain contributions from maliciously compromised nodes. In order to minimize the effect of such contributions, edge node performs a deviation-based analysis on the received Recommendation
TABLE 1. Algorithm 1: Edge based analysis of received accusations.

| Input: \( n_1, n_2, \ldots, n_m, e_1, a_2, \ldots, a_p \) |
| Output: \( h_1, h_2, \ldots, h_r \) |
| Initialization: \( j, m, E, [m], p, RS[p], d_T, E = \max, S = \max, T = \max, u, v, w \) |
| 01: Begin |
| 02: Accept the accusations at \( e \) |
| 03: For \( (i = 1 \text{ to } p) \) do |
| 04: Calculate \( P_e(d) \) by using the (1); |
| 05: \( r_i = P_e(d) \); \( RS[i] = r_i \) |
| 06: End For |
| 07: For \( (i = 1 \text{ to } m) \) do |
| 08: \( e \) sends Hello packets to \( n_i \) |
| 09: Receive reply from \( n_i \) at \( e \) |
| 10: Calculate \( P_e(d) \) by using the (1); |
| 11: \( s_i = P_e(d) \); \( ES[i] = s_i \) |
| 12: End For |
| 13: For \( (i = 1 \text{ to } p) \) do |
| 14: Find \( k \), where \( \alpha_k = n_k \) |
| 15: \( \Delta d = 1 \text{ RS}[i] - ES[k] \) |
| 16: If \( \Delta d > d_T \) then |
| 17: For \( (j = 1 \text{ to } m) \) do |
| 18: \( Temp[j] = ES[i] \); \( RS[i] \) |
| 19: End for |
| 20: For \( (j = 1 \text{ to } m) \) do |
| 21: If \( \text{Temp}[j] < F \) then |
| 22: \( T = S \); \( S = F \); \( F = \text{Temp}[j] \); \( u = j \) |
| 23: Else if \( \text{Temp}[j] < S \) then |
| 24: \( T = S \); \( S = \text{Temp}[j] \); \( v = j \) |
| 25: Else if \( \text{Temp}[j] < T \) then |
| 26: \( T = \text{Temp}[j] \); \( w = j \) |
| 27: End if |
| 28: End for |
| 29: Add \( \Delta n, n_u, n_v \) and \( n_w \) to \( \text{TIL} \) |
| 30: \( F = \max, S = \max, T = \max \) |
| 31: End if |
| 32: End For |
| 33: End |

Trust values. The Trust Average of received recommendation values can be computed by using (10)

\[
\text{Trust Average} = \frac{\sum_{i=1}^{q} RT_{ij}}{q} \quad (10)
\]

The deviation from Trust Average can be calculated by using the (11)

\[
dev_{ij} = |\text{Trust Average} - RT_{ij}| \quad (11)
\]

The obtained values can be represented in a matrix as shown below, (12)

\[
dev_{(1 \times q)} = [dev_{ij} \ dev_{v2} \ldots dev_{vq}] \quad (12)
\]

Let \( HD \) represents the highest value in the above matrix. Another difference matrix can be formed by using the (13)

\[
diff_{ij} = (HD - 0.0001) - dev_{ij} \quad (13)
\]

The difference matrix can be represented as (14)

\[
diff_{(1 \times q)} = [diff_{ij} \ diff_{v2} \ldots diff_{vq}] \quad (14)
\]

The average of all the elements in \( diff_{1 \times q} \) will be computed using (15)

\[
\text{Average Difference} = \frac{\sum_{i=1}^{q} diff_{ij}}{q} \quad (15)
\]

The weight value for calculating the malicious free aggregated trust value at edge node can be calculated by (16)

\[
w_i = \frac{\text{diff}_{ij}}{\text{Average Difference}} \quad (16)
\]

Weight values \( w_1 \) to \( w_q \) can be calculated. The malicious free aggregated trust of node \( n_j \) can be evaluated by the following (17).

\[
AT_{ij} = \sum_{i=1}^{q} w_i \times RT_{ij} \quad (17)
\]

The weighted aggregate trust value calculation nullifies the effect of malicious contribution. The Aggregated Trust Value less than 0.6 confirm the Sybil behavior of a node. The identified Sybil attacker nodes will be immediately excluded from further communications. Nodes having an aggregated trust value greater than or equal to 0.6 will be released from TIL. The accusations made by such nodes will be taken into consideration and the decisions will be taken in usual manner.

C. COMPARISON AND ANALYSIS OF EXPERIMENTAL RESULTS

The performance of EBAD has been examined under the environment simulated using NS 2.35 network simulator. The proposed method has been introduced to identify the nodes which show the Sybil behavior as well as perform the SA-CBA. The efficiency of EBAD has been evaluated based on the comparative analysis done with the existing works, SAODV [14], SLICER-TMU [15], SOKMTC [16] and SAL-SAO DV [17]. The main contribution of the proposed method includes trust based accusation mechanism, the detection of Sybil behavior of an IoT device and the prevention of SA-CBA [18]. In order to assess the efficiency of proposed work towards detecting Sybil attacker nodes, the experimental evaluation has been carried out under the malicious environment [19]. The simulation parameters have been listed in table 2.

The efficiency has been evaluated by changing the load (scenario 1) and number of nodes (scenario 2). The nodes have been deployed in an area of 1000m x 1000m with an
average speed of 25m/s. The performance of EBAD has been evaluated based on seven significant network parameters.

1) BASED ON LOAD
Under this scenario the load has been varied from 1000 kb to 6000 kb. The number of nodes has been fixed to 100. The behavior of each protocol towards Sybil attacker nodes under different network loads has been studied in this section. All simulations have been carried out with active Sybil attacker nodes. Figure 3 represents the fraction of node compromise experienced during the simulations. It is a measure of compromised communication links. Upon identifying Sybil nodes, EBAD excludes them from all the ongoing as well as further communication links. Thus, the number of communication links with the compromised nodes will be low in the proposed protocol. EBAD could maintain a lower node compromise value while comparing with other existing works. The average end-to-end delay-based comparison has been plotted in Figure 4. Congestion, packet drop, normal node reduction, etc. can be a reason for network delay. Among these reasons, normal node reduction will be the prime cause for network delay due to the presence of Sybil nodes which could perform CBA. Congestion will be experienced at the intermediate nodes due to the insufficient number of normal nodes. The waiting time experienced at intermediate nodes will be high due to congestion. EBAD could reduce the overall delay by eliminating the chances of performing the cooperative blackmailing attack. The packet drop measure is plotted in Figure 5. It is a count of lost packets. The packet drop may happen because of network congestion, the presence of attacker nodes, etc. All existing works have also been developed for securing the network entities. But none of them possess an accusation-based Sybil behavior identification scheme. EBAD can withstand SA-CBA. The proper identification of Sybil behavior will reduce the overall packet drop in EBAD. All other existing protocols are not capable to identify the attacks emerging from a Sybil attacker by using the forged identity of other legitimate nodes. The misdetection ratio of the five protocols has been shown in Figure 6. The misdetection ratio is less in EBAD. All other existing works fail to identify the presence of attackers. Thus the misdetection ratio increases with the higher load.
obtained PDR with respect to the increased load has been drawn in Figure 7. All the simulations have been carried out with the presence of attacker nodes. All existing protocols experience the unwanted removal of legitimate nodes inside the clusters because of Sybil attacker nodes. Thus, the packet delivery ratio decreases when the load increases. EBAD could withstand the above-mentioned situation by the behavioral analysis of both attacker nodes as well as normal nodes. EBAD attains high PDR, even with a higher load.

2) BASED ON THE NUMBER OF NODES
In this section, the performance of all five protocols has been evaluated in different environments. The network load is fixed as 500kb. The simulations under this section have also been carried out in a malicious environment. Some nodes have been introduced as Sybil attacker nodes which are having the capacity to perform a Co-operative Blackmailing Attack. Figure 8 represents the average throughput of five works. The values have been obtained by frequently changing the environment. EBAD could attain higher throughput by the early elimination of Sybil Attacker from the network. The Network resilience under scenario 2 has been plotted in Figure 9. The lower network resilience value indicates good performance. EBAD outperforms all other existing works by using the edge based suspicious accusation identification technique. The successful identification of Sybil nodes increases the credibility of the network. The inclusion of more number of nodes contributes a slight increase in network resilience. Among other compared works, SAL - SAODV has been introduced to eliminate the identity based vulnerabilities present in fog networks. Thus SAL - SAODV could attain good network resilience while comparing with other existing works. The PDR of the compared protocols has also been assessed under scenario 2. The obtained PDR for a different number of nodes has been drawn in Figure 10. The early identification of such attacker nodes will decrease the chances of performing SA-CBA. In the case of SOKMTC, the proposed work itself has a secure key management-based approach to prevent identity theft. But SOKMTC does not hold an accusation-based approach for identifying the misdetections. EBAD holds accusations based on Sybil attack detection. Thus, the attacker nodes cannot contribute false accusation data to the Edge node. EBAD attains high PDR, even during the inclusion of more nodes, by reducing the chances of having normal node reduction.
V. CONCLUSION

The impact of the identity-based attack in the smart city environment is quite high. Such attacks may focus either on the sensitive data or on the network stability. In both cases, the network will encounter serious performance degradation. As already mentioned in this paper, data security can be ensured by adopting some cryptographic algorithms. The proposed method contributes a robust solution toward securing the network from identity-based attacks. A Sybil attacker can execute other attacks anonymously in the Smart city environment by stealing the identity of a legitimate node. The impact of such attacks, especially SA-CBA on accusation-based IoT networks is quite high. EBAD offers an Edge-based Sybil node detection mechanism. It primarily analyzes received accusations for identifying Sybil behavior. Afterward, the Edge node will confirm the Sybil behavior of the suspicious accused nodes. The early elimination of the Sybil node decreases the chances of performing the Sybil attack over the Blackmailing attack. The result of the experimental evaluation justifies that the proposed scheme can perform better even under a malicious environment. As per the obtained results, 60% of the overall packet drop could be reduced by the early elimination of attacker nodes. Also, EBAD experiences lower node compromises while comparing with other existing works. All the existing methods eliminate the lower trustworthy nodes from the communication path. EBAD could raise the trust level of individual nodes, thus the availability of intermediate nodes for establishing the communication path is also high. That in turn reduces the delay in the network. EBAD could achieve 90% more throughput and delivery ratio than other existing methods. The proposed method can be incorporated with any other works for eliminating the various forms of Identity-based attacks. The impact of the proposed model on the Internet of Medical Things (IoMT) needs to be examined further. The health care applications handle sensitive data. Thus data confidentiality is the prime concern in IoMT. Attacks on voting-based scenarios may employ a higher impact on network decisions. An attacker can steal the patient’s information by misleading the data flow. Thus the Sybil attack can be considered as a major threat in IoMT. EBAD provides an adequate solution to the above-mentioned issue. Thus the incorporation of EBAD in the IoMT network may produce better results.

REFERENCES

[1] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, “Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing,” IEEE Access, vol. 4, pp. 529–541, 2016.
[2] A. Kirimtat, O. Krejcic, A. Kertesz, and M. F. Tasgetiren, “Future trends and current state of smart city concepts: A survey,” IEEE Access, vol. 8, pp. 86448–86467, 2020.
[3] X. Hou, Z. Ren, J. Wang, W. Cheng, Y. Ren, K. Chen, and H. Zhang, “Reliable computation offloading for edge-computing-enabled software-defined IoT,” IEEE Internet Things J., vol. 7, no. 8, pp. 7097–7111, Aug. 2020.
[4] B. Zhao, P. Zhao, and P. Fan, “EPUF: A lightweight double identity verification in IoT,” Tsinghua Sci. Technol., vol. 25, no. 5, pp. 625–635, Oct. 2020.
[5] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K.-R. Choo, “Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks,” IEEE Internet Things J., vol. 7, no. 7, pp. 6610–6622, Jul. 2020.
[6] Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang, and X. Zhou, “Power control identification: A novel Sybil attack detection scheme in VANETs using RSSI,” IEEE J. Sel. Areas Commun., vol. 37, no. 11, pp. 2588–2602, Nov. 2019.
[7] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “CorrAUC: A malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques,” IEEE Internet Things J., vol. 8, no. 5, pp. 3242–3254, Mar. 2021.
[8] I. Wang, S. Hao, R. Wen, B. Zhang, L. Zhang, H. Hu, and R. Lu, “IoT-pretor: Undesired behaviors detection for IoT devices,” IEEE Internet Things J., vol. 8, no. 2, pp. 927–940, Jan. 2021.
[9] L. Fang, H. Zhang, M. Li, C. Ge, L. Liu, and Z. Liu, “A secure and fine-grained scheme for data security in industrial IoT platforms for smart city,” IEEE Internet Things J., vol. 7, no. 9, pp. 7982–7990, Sep. 2020.
[10] A. A. Elsaeidy, N. Jagannath, A. G. Sanchis, A. Jamalipour, and K. S. Munasinghe, “Replay attack detection in smart cities using deep learning,” IEEE Access, vol. 8, pp. 137825–137837, 2020.
[11] B. Wang, M. Li, X. Jin, and C. Guo, “A reliable IoT edge computing trust management mechanism for smart cities,” IEEE Access, vol. 8, pp. 46373–46399, 2020.
[12] S. Murali and A. Jamalipour, “A lightweight intrusion detection for Sybil attack under mobile RPL in the Internet of Things,” IEEE Internet Things J., vol. 7, no. 1, pp. 379–388, Jan. 2020.
[13] C. Pu, “Sybil attack in RPL-based Internet of Things: Analysis and defenses,” IEEE Internet Things J., vol. 7, no. 6, pp. 4937–4949, Jun. 2020.
[14] S. Lu, L. Li, K.-Y. Lam, and L. Jia, “SAODV: A MANET routing protocol that can withstand black hole attack,” in Proc. Int. Conf. Comput. Intell. Secur., 2009, pp. 421–425.
[15] F. Qiu, F. Wu, and G. Chen, “Privacy and quality preserving multimedia data aggregation for participatory sensing systems,” IEEE Trans. Mobile Comput., vol. 14, no. 6, pp. 1287–1300, Jun. 2015.
[16] S. P. John and P. Samuel, “Self-organized key management with trusted certificate exchange in MANET,” Ain Shams Eng. J., vol. 6, no. 1, pp. 161–170, Mar. 2014.
[17] W. Fang, W. Zhang, J. Xiao, Y. Yang, and W. Chen, “A source anonymity-based lightweight secure AODV protocol for fog-based MANET,” Sensors, vol. 17, no. 1421, pp. 1–16, 2017.
[18] A. Ahmed, S. Abdulla, S. Iftiikhar, I. Ahmad, S. Ajmal, and Q. Hussain, “A novel blockchain based secured and QoS aware IoT vehicular network in edge cloud computing,” IEEE Access, vol. 10, pp. 77707–77722, 2022.
[19] A. Ahmed, S. Abdulla, M. Bukhsh, I. Ahmad, and Z. Mushhaq, “An energy-efficient data aggregation mechanism for IoT secured by blockchain,” IEEE Access, vol. 10, pp. 11404–11419, 2022.
G. NAGARAJAN (Senior Member, IEEE) received the B.E. degree in electrical and electronics engineering from MS University, in 2000, the M.E. degree in applied electronics from Anna University, in 2005, and the M.E. and Ph.D. degrees in computer science and engineering from Sathyabama University, in 2007 and 2015, respectively. He is currently a Faculty Member of the Department of Computer Science and Engineering, School of Computing, Sathyabama Institute of Science and Technology, Chennai, India. He has published more than 70 research articles in peer-reviewed journals, such as IEEE conference, ACM, Springer-Verlag, Inderscience, and Elsevier. He also has contributed 15 book chapters thus far for various technology books. He has authored and edited three books thus far and is focusing on some of the emerging technologies, such as the IoT, edge/fog computing, artificial intelligence (AI), data science, blockchain, digital twin, and 5G. His current research interests include computer vision, the IoT, 5G, edge/fog computing, artificial intelligence, machine learning, and wireless sensor networks.

ASMAA MUNSHI received the B.Sc. degree in computer science form King Abdulaziz University, Saudi Arabia, in 2004, and the master’s degree (Hons.) in internet security and forensic and the Ph.D. degree in information security from Curtin University, Australia, in 2009 and 2014, respectively. She is currently an Associate Professor with the Cybersecurity Department, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. She is also holding several positions of the Vice Dean (Female Section) of the College of Computer Science and Engineering, University of Jeddah. She is also a Supervisor of the Cybersecurity Department (Female Section) with the College of Computer Science and Engineering. She is also the Vice Dean of the Faculty of Computing and Information Technology (Female Section), Khulais Branch, University of Jeddah. Her research interests include computer forensic, information security, and the IoT.

K. VENKATA CHALAM (Senior Member, IEEE) received the bachelor’s degree in information technology, the master’s degree in computer science and engineering, and the Ph.D. degree in computer science and engineering, in 2005, 2008, and 2018, respectively. He has more than 14 years of academic experience. He is currently working as a Senior Researcher with the Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové, Hradec Králové, Czech Republic. He is a Sun Certified SCJP professional and has obtained Brain Bench certification in various disciplines. He has organized several workshops on J2ME, advanced java programming, web services, enterprise computing, web technology, and WSN (wireless sensor network) in his institution and has presented papers in web services at national and international conferences. He has guided a number of research-oriented as well as application-oriented projects organized by well-known companies like IBM. He has delivered more than 20 guest lectures in reputed engineering colleges on various topics. He has published several articles in peer-reviewed journals. His research interests include data mining, web services, semantic web services, distributed computing, and cloud computing.

WAFA ALMUKADI received the B.Sc. degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2004, the master’s degree in management information system from the University of Central Florida, Orlando, FL, USA, in 2007, and the Ph.D. degree in human-centered design from the Florida Institute of Technology, in 2017. She has more than 12 years of academic experience and is currently working as a Supervisor of the Software Engineering Department, University of Jeddah. Her current research interests include the Internet of Things, educational technology, wearable technology, and tangible user interface. She was a recipient of the Best Ph.D. Student Awards from the Florida Institute of Technology, in 2016.

MOHAMED ABOUHAWASH received the B.Sc. and M.Sc. degrees in statistics and computer science from Mansoura University, Mansoura, Egypt, in 2005 and 2011, respectively, and the Ph.D. degree in statistics and computer science from the Channel Program between Michigan State University, East Lansing, MI, USA, and Mansoura University, in 2015. In 2018, he was a Visiting Scholar with the Department of Mathematics and Statistics, Faculty of Science, Thompson Rivers University, Kamloops, BC, Canada. He is currently at the Departments of Computational Mathematics, Science, and Engineering (CMSE), Biomedical Engineering (BME), and Radiology, Institute for Quantitative Health Science and Engineering (IQ), Michigan State University. He is also an Associate Professor with the Department of Mathematics, Faculty of Science, Mansoura University. His current research interests include evolutionary algorithms, machine learning, image reconstruction, and mathematical optimization. He was a recipient of the Best Master’s and Ph.D. Thesis Awards from Mansoura University, in 2012 and 2018, respectively.