Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks

Dr. D. Sivaganesan,
Professor,
Department of Computer Engineering,
PSG Institute of Technology and Applied Research,
Coimbatore, India.
Email: sivaganesan@psgitech.ac.in

Abstract: Utilization of smart applications in various domains is facilitated pervasively by sensor nodes (SN) that are connected in a wireless manner and a number of smart things. Hazards due to internal and external attacks exist along with the advantages of the smart things and its applications. Security measures are influenced by three main factors namely scalability, latency and network lifespan, without which mitigation of internal attacks is a challenge. The deployment of SN based Internet of things (IoT) is decentralized in nature. However, centralized solutions and security measures are provided by most researchers. A data driven trust mechanism based on blockchain is presented in this paper as a decentralized and energy efficient solution for detection of internal attacks in IoT powered SNs. In grey and black hole attack settings, the message overhead is improved using the proposed model when compared to the existing solutions. In both grey and black hole attacks, the time taken for detection of malicious nodes is also reduced considerably. The network lifetime is improved significantly due to the enhancement of these factors.

Keywords: Internet of things, blockchain, trust, sensor nodes, mist computing, energy efficiency

1. Introduction

The plethora of mobile and static devices like controllers, sensors and actuators have enabled providing services to the end-users anywhere and anytime through Internet-of-Things (IoT)

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

[1]. Resource management and other promising solutions are offered by these devices while enforcing reliability and quality in enterprise systems [2]. In complex applications of industry 4.0 to simple home automation, IoT has penetrated into all domains leading to a technological revolution due to the cognitive and embedded smart capabilities and intense communication between the devices. The notion of smart and massive augmented interconnection is affected largely by 5G, Wireless Sensor Networks (WSNs), mist and other such communication technologies [3]. The Sensor Nodes (SNs), that are smart and resource constrained entities of WSN provides a foundation for data collection in IoT. Low-powered embedded technologies, wireless communication, System on Chip (SoC), Micro Electro Mechanical Systems (MEMS) and various other technologies are used for developing the WSNs. Smart transportation, military and several other diverse application areas make use of this technology [4]. However, security vulnerabilities, network privacy, data interoperability risk, transparency, decentralization, network lifespan and such critical challenges have to be encountered by the devices. Gartner estimation suggested that IoT will enable interconnection of over twenty-five billion physical entities to be operating as a single network by 2021 [5]. The need for protection against attacks and misuse, proficient sharing, analysis, processing, transmission and capturing is high due to the sensitive and massive data generated by the IoT devices.

A data driven trust mechanism based on blockchain (DDTMB) is proposed in this paper which uses the data obtained from IoT devices to exemplify the resultant communication [6]. Anonymity, crypto-currency and other applications landscape the Information and Communication Technologies (ICT) of today to overcome their security issues by means of blockchain. Distributed mechanisms like decentralized trust and privacy are essential to ensure secure data transfer within the network in mist computing [7]. In mist-based IoT systems, a decentralized security solution is offered by the blockchain technology. In smart healthcare system, the malicious and compromised nodes are isolated from the network by executing consensus among mist nodes every time a new node joins the network [8]. In IoT systems with mist computing, the distributed nature and scalability are not met by the centralized mechanism. For this purpose, a secured and efficient environment is enabled by means of decentralized security solutions that is provided to mist computing setup through blockchain. For sustaining scalability, improving latency, protecting devices and saving energy, IoT is impacted by blockchain in a positive manner [9]. The cooperation between untrustworthy and

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

unknown entities is established by the blockchain technology. The recent cloud computing architectures demand authentication authority and central security which is not available and may be provided by the distributed nature of IoT.

2. Related Works

Several literature exist with respect to mobile codes, blockchain and trust mechanism. Based on the number of packets forwarded and the number of packets delivered, a trust mechanism is setup to address the issues of selective forwarding and blackhole attacks [10]. In large deployments, the direct trust assessment leads to move message overdue reducing the scalability of the model. In IoT networks with Routing Protocol for Low power and Lossy Networks (RPL), a trust-aware, time-based solution is provided to address the insider attacks [11]. The energy efficiency of this mechanism is less as the recommendation uncertainty was ignored. The wormhole and greyhole attacks are addressed by trust-based tools. The blackhole attack may be mitigated in IoT devices with the help of trust routing mechanisms based on RPL. The trust of IoT nodes can be assessed using a reputation-based approach. A hybrid Intrusion Detection System (IDS) has been introduced for clustered WSNs [12]. On the basis of node conduct for the dynamic adaption of trust values and increase association among trusted nodes, an adjustive distributed trust technique is introduced. The cluster of associates are allocated greater trust scores from false nodes. The recommendation of these nodes influence the trust precision of this model.

Certain researchers worked on distributed trust mechanisms [13]. The trust methods of blockchain, accountability and transparency factors do not bias the aforementioned procedures. The trajectory resemblance, incident timelines and transmission frequency of reputation administration affects the subjective logic version, blockchain and smart contract association with vehicular systems during the reputation supported significant data exchanging scheme [14]. In vehicular systems supported by blockchain, the scale of reputation is used for computing the credibility of switched over messages with the help of a distributed trust administration plan [15]. The block affirmation scheme consists of a distributed trust mechanism and an IoT affable agreement algorithm in the IoT based Lightweight Scalable

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

Blockchain (LSB) model. End-to-end trust is not furnished by the existing blockchain schemes available for IoT applications [16]. This is due to the failure to capture data among the inter-node transmission among all nodes or to enhance the trust of IoT data.

3. Proposed Work

Great chaos and interruption is caused by the increasing sensors connected together as IoT networks. Processing and analysis of the voluminous data generated by these sensors is performed at the mist or cloud server. The unnecessary delay and latency is not addressed in a timely manner by the cloud-based infrastructure. However, the latency issue of the IoT devices is mitigated in a distributed manner by means of mist computing. Multi-hop technique is used for transmission of the sensed information. Dropping of few or all data packets may be performed when greyhole or blackhole or other projecting internal attacks compromise the intermediate nodes. Ensuring constant data flow in a reliable manner is essential as the situation is highly sensitive. Internal attacks are mitigated extensively by means of security measures based on trust. However, single-point-of-failure issues are faced by the conventional trust-based mechanisms due to their centralized nature and inability to address the scalable nature of such infrastructure. The single-point-of-failure issues are mitigated and scalability is met through the decentralized solution provided by blockchain technology. Providing a decentralized, authentic, unaltered and unforged trust value is the major role of blockchain in this work.

Adverse outcomes may be caused by the forged trust values. Fatal consequences may be caused due to the malicious node in a smart healthcare scenario if false trust value causes it to look legitimate leading to a blackhole attack where the sensed data may not reach the destination. Hence, it is essential to ensure sensed data to reach the health specialists in a timely and appropriate manner for specific actions to be taken. In centralized trust-based mechanisms, the single-point-of failure issue cannot be mitigated, which is overcome by the decentralized trust mechanism. The IoT infrastructure and their scalable nature is also met using this model. Encryption, anonymity and other such attributes are provided by the blockchain platform in an efficient manner. The security tokens, itineraries of mobile codes, IDs of devices and other

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

such trustworthy data collection are stored along with the trust value using an immutable distributed ledger by this technology. Genuine trust assessment and accuracy may be ensured by the blockchain platform.

The proposed DDTMB model based trust assessment helps in satisfying four major objectives namely. Reliable and trusted communication is enabled for detection of malicious nodes by designing and developing a reliable trust based model. The underlying SNs and their trustworthiness must be monitored effectively by the system despite sparse or congested situation. Gathering the details, calculation of trust values, saving the calculated trust values, and such trust assessment related processes may be affected by the robustness and ability of the model to resist threats. Computation, control, information collection and other related overheads must be reduced making the model energy efficient. Multi-mobile codes may be utilized for elimination of redundant transmission of messages and casting low message overhead. The network lifetime is improved by depletion of intermediate node energy and elimination of excessive control traffic generation caused by the frequent message exchange.

Adaptability, management of resource efficiency and scalability is improved while reducing the network overhead and producing accurate global trust based on trust assessment using a decentralized approach. If there is a proliferation in the number of SNs or devices connected, the performance of the mechanism does not deteriorate thereby ensuring and improving scalability of the model. The growing demands of the network are met by initiating multi-mobile agents. The latency may be improved by using in-time trust assessment and dynamic itinerary creation and initiation of mobile codes for augmenting the WSNs dynamic nature for improved detail gathering. During the exchange of trust related data among SNs, the network congestion may be lowered. The SNs close to the mist nodes are resource constrained where the calculations are rambled. Figure 1 provides the structure of the proposed model.

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

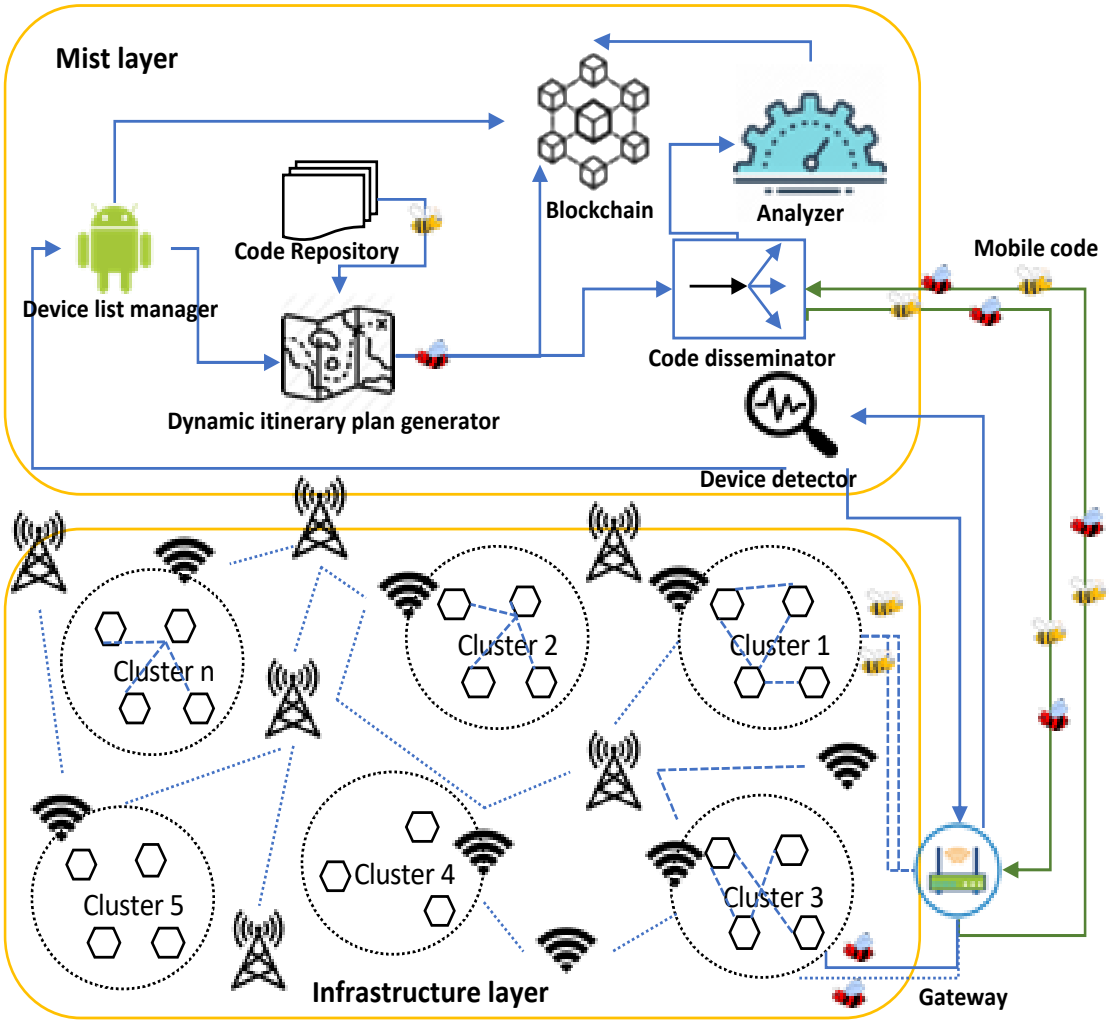

Fig. 1. Trust based data collection model with Mist layer for IoT network

4. Results and Discussion

The fundamental requirement for diagnosis and testing is simulation. In WSNs and networking domain, this has become a standard in an undoubted manner. However, addressing the requirements for deployment in real-world scenario may be challenging due to insufficiency. In order to address the gaps in simulation, it is crucial to design experimentation in real world scenario. A blockchain based simulator that provides the essential values of specific parameters while fulfilling the requirements does not exist to the best of our knowledge. In order to understand the underlying systems in a functional manner, test-bed experiments are conducted. Certain conditions and behaviors that would be missed during simulation can be observed by this procedure. The experimental setup consists of five nodes of which one is an actuator,

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

another is a mist node and rest of them are SNs. The network does not contain any malicious node in the initial stage. At the next level, the functionality of the network is observed on introduction of a malicious node. Two mobile codes are generated and initiated for the two itinerary plans by the mist nodes. Neighbor trust-based mechanism (NTBM), Mobile Code-driven Trust Mechanism (MCTM) and the proposed DDTMB model are compared for the greyhole and blackhole attack scenarios for several iterations. Random malicious nodes are created during each iteration. The proposed mechanism is verified in terms of consistency by means of these iterations. For each iteration of these mechanisms, the functionality and effects are noted. The average value of the iterations is considered to evaluate the performance of the model.

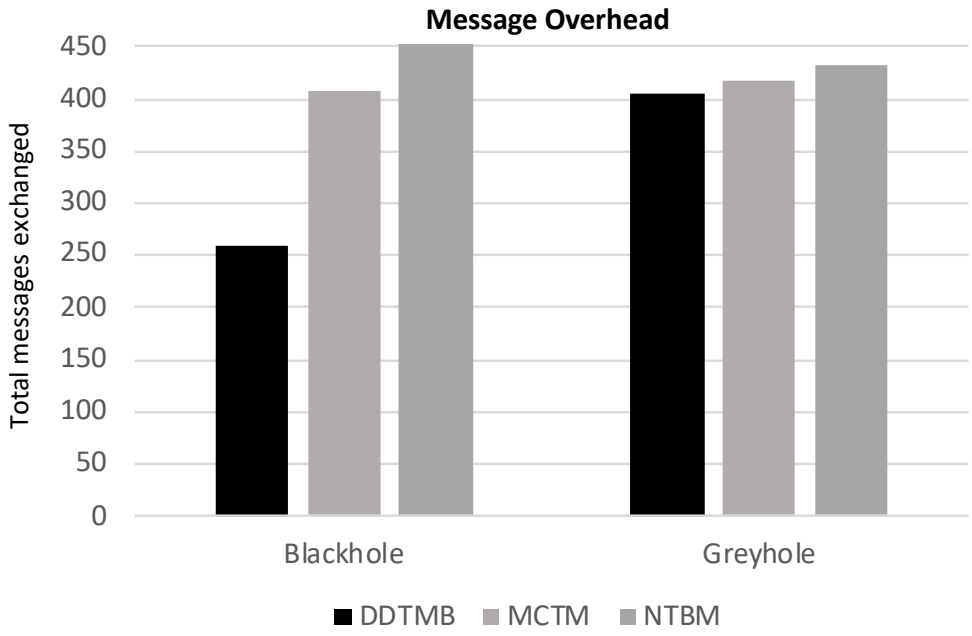

Fig. 2. Comparison of message overhead under grey and black hole attack simulation

As messages are exchanged, the message overhead is determined by the message exchange ratio between any two nodes of the network. In case of NTBM, MCTM and DDTMB, the average message overhead ratio is as represented in figure 2. In blackhole attack scenario, there is a considerable increase in the message overhead and a comparatively smaller increase in the greyhole attack scenario. The messages exchanged by the proposed model is also smaller compared to the other schemes for both greyhole as well as blackhole attacks. When compared

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

to the single mobile code based model, the multi-mobile model offers better performance. The comparison of time taken for detection of malicious node under various attack scenarios for the aforementioned models is represented in figure 3. The assigned itineraries and their details are fetched by the multi mobile codes. Smaller mobile code size, reduced congestion of network traffic and lower exchange of messages are the benefits of the proposed system.

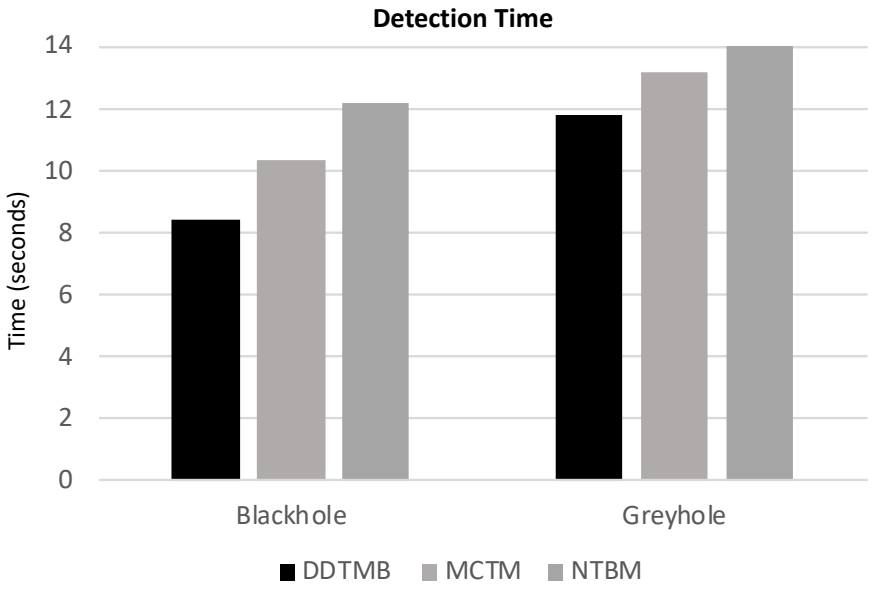

Fig. 3. Comparison of detection time for malicious node under grey and blackhole attack simulation

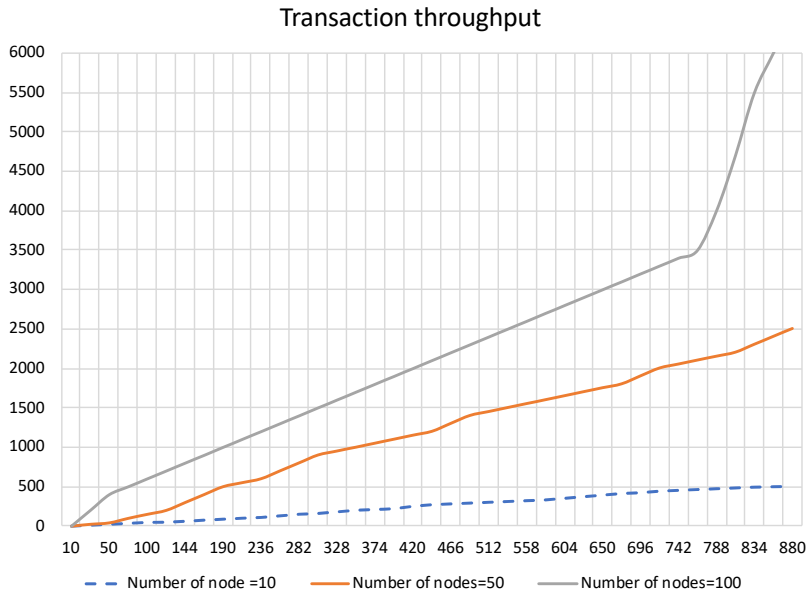

Fig. 4. Estimation of transaction throughput in the proposed DDTMB model

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

In the blockchain, an efficient and scalable degree of transactions recoding is termed as throughput. As the number of connected nodes increase, the system must not deteriorate and work invariably to be referred to as scalable. The mechanism is executed for various number of nodes to compare the throughput and estimate the scalability of the model. Figure 4 represents multiple transactions of a single node in the blockchain for specific time duration. The proposed model requires the same amount of time despite the increase in number of transactions.

5. Conclusion

Accumulation and dispersion of data is performed widely using WSNs. Due to this reason, selection of trusted resources for data or information gathering is essential. The SN may become unreliable or may be seized by an attacker as they are data sources. In order to mitigate such attacks, it is crucial to incorporate trust mechanisms. Several factors such as restrained, distributed, scalable, mobile and diverse nature of the SNs are to be met by the while designing a robust trust-based security framework. Message, communication, computation, traffic congestion and scalability overheads may be faced by single-point-of failure problem in the centralized trust assessment techniques that are available. The network lifespan is threatened by these overheads as they deplete the energy of the SNs. A data driven trust mechanism based on blockchain is presented in this paper which uses the data obtained from IoT devices to exemplify the resultant communication. Message overhead and traffic congestion issues are overcome by generating dynamic itineraries based on the number of SNs for multiple mobile codes. Improvement in performance, optimized network lifetime, scalability, malicious node detection and mitigation of message overhead is demonstrated by this model. Blockchain based authentication and security during data transfer may be incorporated as a future direction.

References

[1] Huang, J., Kong, L., Dai, H. N., Ding, W., Cheng, L., Chen, G., ... & Zeng, P. (2020). Blockchain-Based Mobile Crowd Sensing in Industrial Systems. IEEE Transactions on Industrial Informatics, 16(10), 6553-6563.

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

[2] Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications, 143, 167-177.

[3] Yan, Z., Peng, L., Feng, W., & Yang, L. T. (2021). Social-Chain: Decentralized Trust Evaluation Based on Blockchain in Pervasive Social Networking. ACM Transactions on Internet Technology (TOIT), 21(1), 1-28.

[4] Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149-160.

[5] Altaf, A., Abbas, H., Iqbal, F., Khan, M. M. Z. M., Rauf, A., & Kanwal, T. (2021). Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks. Journal of Systems Architecture, 115, 102028.

[6] Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The security of big data in mist-enabled IoT applications including blockchain: A survey. Sensors, 19(8), 1788.

[7] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 100227.

[8] Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, 102022.

[9] Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2020). A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Mist computing. Transactions on Emerging Telecommunications Technologies, e4112.

[10] Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., & Yang, Y. (2020). Trust-based attack and defense in wireless sensor networks: A survey. Wireless Communications and Mobile Computing, 2020.

[11] Santos, A. L., Cervantes, C. A., Nogueira, M., & Kantarci, B. (2019). Clustering and reliability-driven mitigation of routing attacks in massive IoT systems. Journal of Internet Services and Applications, 10(1), 1-17.

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021

Journal of trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 01
Pages: 59-69
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.1.006

[12] Elnour, M., Meskin, N., Khan, K., & Jain, R. (2021). Application of data-driven attack detection framework for secure operation in smart buildings. Sustainable Cities and Society, 69, 102816.

[13] Al-Duwairi, B., Al-Kahla, W., AlRefai, M. A., Abdelqader, Y., Rawash, A., & Fahmawi, R. (2020). SIEM-based detection and mitigation of IoT-botnet DDoS attacks. International Journal of Electrical & Computer Engineering (2088-8708), 10(2).

[14] Suma, V. (2020). Automatic Spotting of Sceptical Activity with Visualization Using Elastic Cluster for Network Traffic in Educational Campus. Journal: Journal of Ubiquitous Computing and Communication Technologies June, 2020(2), 88-97.

[15] Sri, P. D., Luharuka, S., Somani, R., & Kulkarni, G. A. Technical Scrutiny of Block chain Technology Protocols and its Applications.

[16] Haoxiang, W. (2019). Trust management of communication architectures of internet of things. Journal of trends in Computer Science and Smart technology (TCSST), 1(02), 121-130.

ISSN: 2582-4104
Submitted:10.03.2021
Revised: 16.04.2021
Accepted: 25.04.2021
Published: 10.05.2021