International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

March-2018 Volume 5, Issue-2

Email:editor@ijermt.org www.ijermt.org

IMPLEMENTING BLOCK CHAIN BASED SECURED SYSTEM IN IOT ENVIRONMENT: A COMPISON WITH EXISTING APPROACHES

Gurpreet Singh
gurisingh0504@gmail.com
Guru Nanak Dev University, Amritsar

Abstract

The invention of the Internet of Things links millions of computers and sensors to one another, creating massive data volumes. Therefore, the existing communication and deployment environment in an IoT is covered with various security issues. Various attacks reduce the trust factor of using the application over an IoT from a user perspective. There is various research work, where security approaches have been discussed for IoT. Existing approaches towards securing IoT mainly use an authentication-based approach, key management, privacy preservation, fault tolerance-based approach, an explicit mechanism for resisting specific attack. Apart from this, performing sophisticated security operations over devices with low-end processing capability is not practical. Another prominent security issues in IoT is the little emphasis on security standards. The proposed study's core aim is to construct an intelligent framework that can streamline an IoT's communication demands more securely for resisting lethal adversaries. Security in the communication process is developed by harnessing the potential features of blockchain. Our main objective is to evaluate the proposed system's strength by comparing it with existing encryption approaches widely used/preferred in the existing IoT environment. The proposed system realizes the potential security feature of blockchain, which is considered the most suitable secure communication system in an IoT, by incorporating further improvement towards it for better results.

1. INTRODUCTION

Internet of Things(IoT) is a repository of many interconnected objects, services, persons, and devices that can converse, share data, and knowledge to obtain a common purpose in different areas and applications. IoT has many implementation areas like transportation, agriculture, healthcare, energy production and distribution. An IoT system consists of several functional blocks to assist different system utilities such as sensing, identifying, actuating, communicating and managing. Figure 1 shows the components of IoT devices.

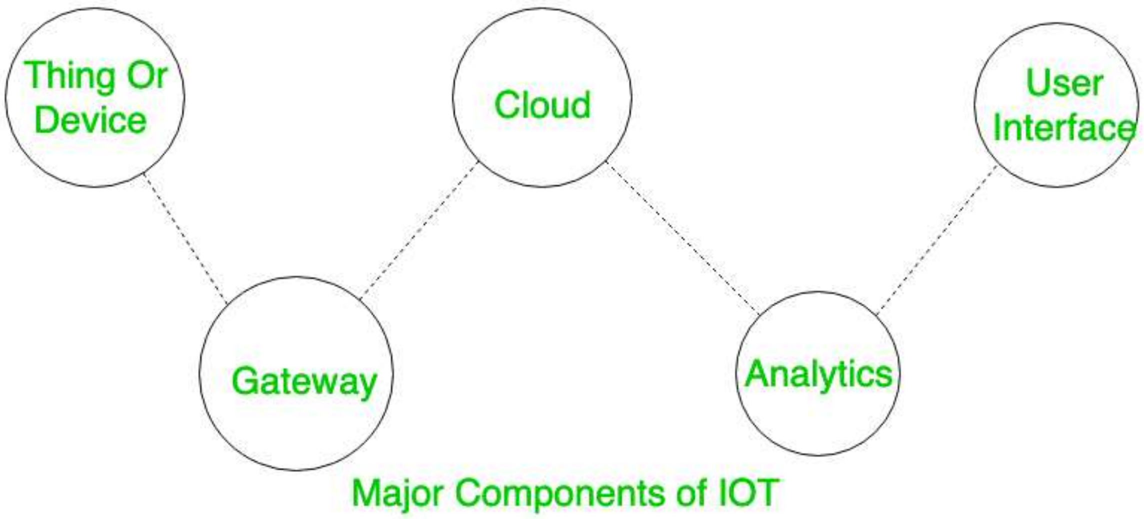

Figure 1: Components of IoT devices

The devices in the IoT system offer activity in sensing, actuating, controlling, and monitoring the process. IoT devices can share information with other devices which are connected and apps or gathers information from other devices. It analyzes the information locally or sends data back-ends to remote servers or cloud-based systems for data processing, or executes other tasks locally and certain IoT network activities depending on time and space constraints. An IoT device may consist of multiple wired and wireless interfaces for communicating to other devices. It contains I/O sensor interfaces, internet connectivity interfaces, interfaces for memory and storage, and audio/video interfaces. IoT devices can also be of different types such as wearable sensors, smart watches, LED lights, and automobiles.

The block of communication handles the interaction between devices and servers. In general, IoT communication protocols work in the data link layer, network layer, transportation layer, and application layer. An IoT framework performs multiple types of functions including application modeling services, computer management, data distribution, data processing and software discovery services. Control framework includes various roles for regulating an IoT system and searches into the underlying IoT system governance. Security mechanism offering features such as authentication, authorization, anonymity, the integrity of communications, the integrity of content and protection of data. In terms of usage, the application layer is the most important as it serves as an interface that offers the required modules to manage and track different facets of the IoT network. Application layer allow users to access the current stage of action, sometimes predicting futuristic prospects, and analyze the system status.

IoT tools and systems should be able to respond quickly to shift circumstances and take action depending on their working environments, the context of the user or sensed environment. For example, The security cameras will change their modes according to whether it is day or night. When any motion observed, cameras may switch from a lower to higher resolution modes and warn surrounding cameras to do likewise. The surveillance device, in this example, adapts itself depending on the environment and evolving circumstances.

IoT devices may have the ability to self-configure, allowing a large number of devices to work together to provide some functionality. These devices can configure themselves, set up networking and get the latest software upgrades with minimal user or manual intervention. IoT systems can adopt a range of interoperable protocols of communication and can connect with other systems as well as with networks. An IoT device has its own unique identity and identifier. IoT systems should have smart interfaces that respond to context, connect with users, and interact with the world. IoT device interfaces, in conjunction with the control, configuration and management infrastructure, allow users to query devices, monitor their status and remotely control them.

Usually, IoT devices are integrated into the network of information, which enables them to communicate and share data with other devices and systems. IoT devices can be dynamically discovered and have the ability to explain themselves to other devices or user applications. For instances, a weather monitoring node may describe its monitoring capabilities to another connected node for communication and data exchange. Integration into the information network makes IoT systems smarter in collaboration with the infrastructure, due to the intelligence of the individual devices. The sensor nodes acquire an awareness of the external background based on sensed information about the physical and environmental parameters. The decisions taken after that by the sensor nodes are context-aware. In a wide area, this function improves the entire network energy efficiency and thus extends the lifespan of the network.

IoT connects objects to sensors used for sharing, monitoring and management of data. Logically IoT has a layer of vision, a layer of movement, and a layer of an application. The layer of perception senses the information and submits it to the layer of application via the internet or network transmission. The sensor nodes are exploited in an unmanned environment that exposed to malicious attacks. The IoT is an evolving internet movement that encourages low latency, accessibility and globally dispersed resources. The IoT form fog nodes are cloud-assisted. The untrusted cloud practices the confidentiality of data through many cryptographic techniques. The security in three-layer architecture, i.e. user-fog-cloud [9], should now be ensured.

2. BLOCKCHAIN TECHNOLOGY

Blockchain is defined as a ledger which is unchangeable used to log information sections in a segregated way. It permits elements to communicate without a focal, believed outsider being available. The blockchain keeps an always developing assortment of information passages, stuffed together into information blocks. These squares are connected with cryptographic endless supply of the blockchain to the previous and future blocks. In the first kind of blockchain, these information records/blocks are; discernible by anybody, writable by anybody, and carefully designed by anybody. For instance, it permits decentralized exchanges and information the executives. On account of these properties, blockchain has a great deal of thoughtfulness regarding various applications. Also, blockchain makes smart contracts; contracts for self-activating that does not require any centralized authority.

Blockchain primarily used throughout the financial sector, however, more and more implementations are emerging for various areas. Traditional companies should find blockchain and extend blockchain to their sectors to improve their structures for instance, user reputations stored on the blockchain. The upcoming industry, at the same time, could use blockchain to improve performance, a startup for ride-sharing provides a transparent platform where riders communicate directly to drivers with the use of blockchain technologies.

2.1 Adoption of Blockchain for Enhanced Security in IOT

At present, blockchain technology is seen as the long-term security approach in an IoT because of multiple reasons. Blockchain induces information bound in the form of a block and are connected using cryptography. A chain of blocks is made where the Secure Hash Algorithm (SHA-512) hashed value of preliminary data (or block) is retained in one block along with transaction data in tree form and timestamp. Blockchain is characterized by stability, traceability, process integrity, Security, and faster processing. However, there is a variously reported limitation of blockchain, i.e., higher energy consumption, immutable data, self-maintenance dependency, higher cost, and the concept is still in the nascent stage of development. However, this limitation can be overcome if there is enough focus on the encryption mechanism used in liking blocks.

3. PROPOSED ALOGORITHM

3.1 Processing the IoT Flow Stream

Algorithm for reading the Jain flow stream in IoT (JFS)

```
Input: $\Phi$, $\psi$, $\rho$
Output: Si d and $\eta i^{d}$
Start
For m=1: n
    init Si and $\eta$ as null
    For d=1: (d+1) such that $d \leq D$
        read $\Phi i(d)=a.\ g(\Phi i^{d})$.
        $\Phi i \rightarrow u(\Phi i, \Phi i(d))$
        read $\eta i(d)=a^{-1}\ .(g(\psi i^{d})^{-1}).f1(Bk.\ c)$
        $\eta i=u(\eta i, \eta i(d))$
    End
    compute $Si^{d}$ and $\eta i^{d}=\chi(\rho,1-\rho)$
End
End
```

3.2 Mechanism to identify vulnerable Port

Pavan's Algorithm for Identification of Weak Port

```
Input: $\Phi$, $Si^{D}$, $\eta i^{D}$
Output: WP Start
For m=1: n
    read $\Phi i(d)=a.\ g(\Phi i^{d})$.
    If $Si(d) \geq Si^{D}$
        Compute $\eta i(d)=a.\ (1/g(sei)).\ f1(bk/dk)$
        If $\eta i(d) \leq \eta i^{D}$
            compute $\eta i,p(d)$
            For $\eta ip(d) \leq \eta i^{D}$
                Associate port to WP
            End
        End
    End
End
End
```

3.3 Mechanism for Identification and Resisting of Intrusion

Pavan's Algorithm for Detection and Prevention of Intrusion

```
Input: se
Output: $\gamma_{reg}$, $\gamma_{adv}$ Start
For m=1: n
    If $sein(k) \in seout(k)$
        $\sigma$=f2(cpkt_in cpkt_out)
        If $\sigma$<Th
    sein(k)$\in \gamma$reg
    End
    Else
    sein(k)$\in \gamma$adv
    End
End
```

4. RESULT & DISCUSSION

4.1 Comparative Analysis

This section discusses the comparative analysis of the proposed system with the existing system. The proposed system considers two existing systems to carry out a comparative analysis. The first existing system is conventional block methods and the second existing work considered in the proposed system is the recent work carried out by Rahman et al.. The justification behind adopting this existing is because of a similar aim with the proposed study, i.e., securing SDN and IoT systems using a distributed mechanism. The outcomes of comparative analysis are as follows:

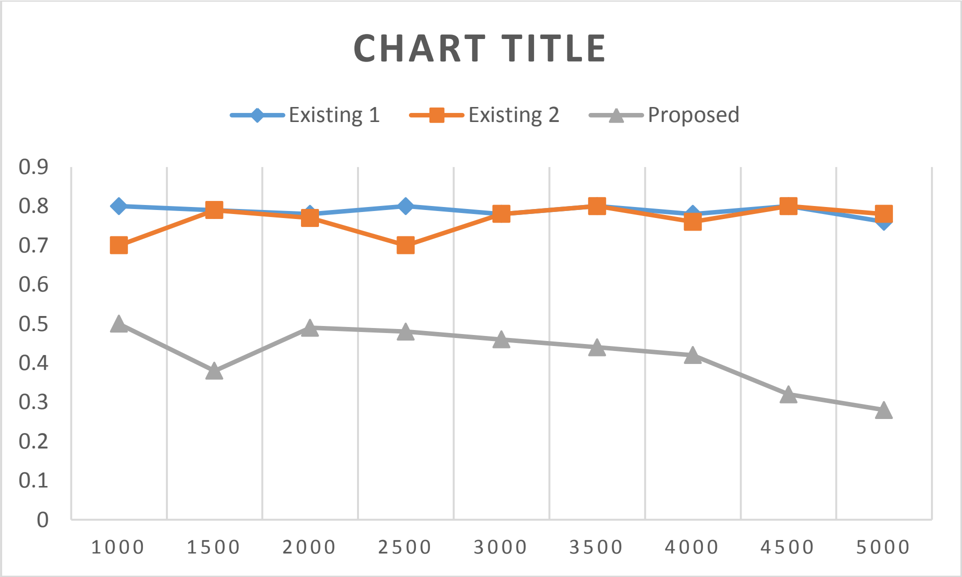

Figure 2: Comparative Analysis of Overhead

The outcome shown in figure 2 represents that the proposed system offers significantly lower overhead than both the existing approaches. Overhead is directly linked with security factors, too, as higher chances of flooding attacks are possible if overhead becomes high. The justification behind this outcome is-*Existing1* uses a conventional centralized scheme of blockchain, which introduces a higher amount of resources to perform authentication of the blocks from the servers. There is no significant change in overhead performance for Existing1, which represents that they are not sufficient to deal with the malicious data flow of unknown type generated from a heterogeneous network form. To some extent, *Existing2* offers slightly better performance in contrast to *Existing1*; however, they introduce a mechanism to perform a selection of cluster head where heterogeneity concept is not adopted, and this leads to slightly un-applicable towards large deployment of the heterogeneous network in IoT. On the other hand, the proposed system exhibits an excellent performance of overhead reduction as the complete information used from the data flow is used with higher precision, which leads to a reduction in the cost of resource involvement while performing advanced monitoring of the adversarial behavior. Therefore, the proposed system offers better overhead.

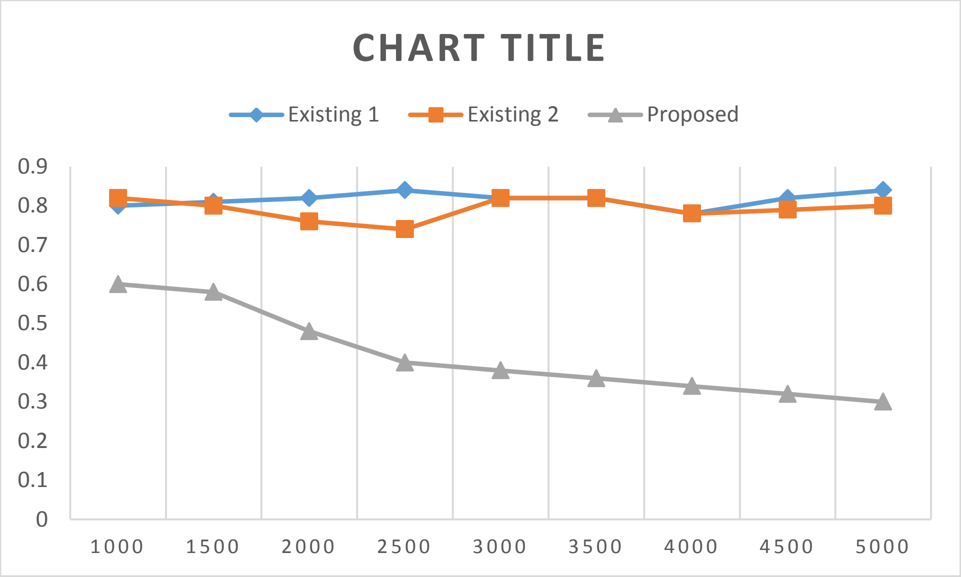

Figure 3: Comparative Analysis of Delay

Delay is another performance parameter used for assessing the performance of the proposed system. A lower delay will eventually represent better performance from both the communication and security viewpoint, which can be seen for the proposed system curve in figure 3. A closer look at the proposed system curve shows that delay is significantly reduced with increased iteration, where the number of requests from the switches is increased. It will mean that the proposed system offers better management of all the switches' requests and evaluates those concerning speed and equivalency score, which is not that difficult to compute. Once it is computed, its information is updated to the SDN controller. Progressive updating demands only assessing the conditional checks, making the process quite faster in monitoring and preventing the harmful data flow. This causes significant delay reduction where an increase of request has no impact on its performance. However, similar performance cannot be expected in the existing system. The conventional blockchain used in both the existing systems differs from the proposed system and its blockchain design discussed in Chapter-4. Hence, owing to the inclusion of an extra set of operation to perform authentication of the flow of iterative nature, both the existing system doesn't exhibit better delay performance.

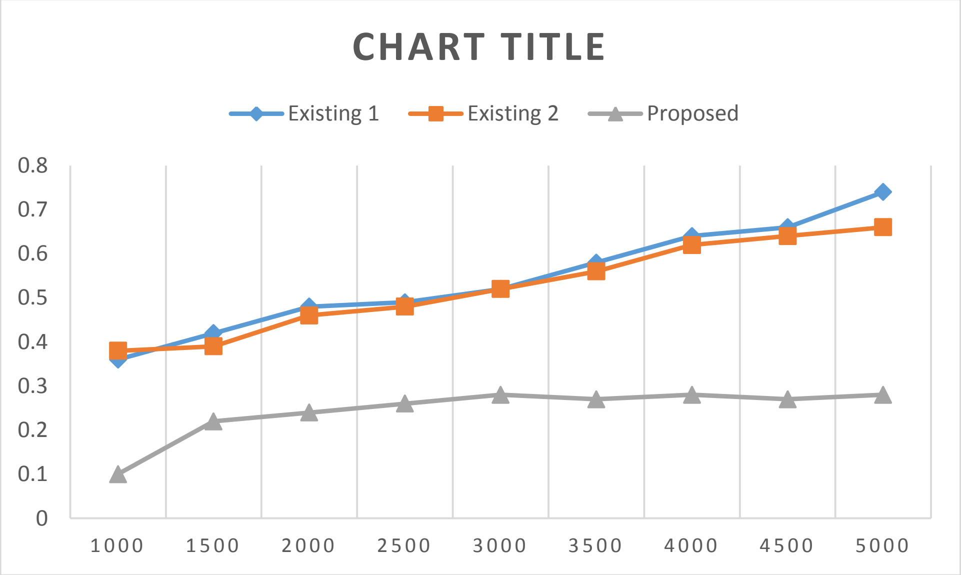

Figure 4: Comparative Analysis of Malicious Request Flow

Figure 4 highlights the comparative analysis of malicious request flow, which is calculated as several requests originated towards the SDN switch have been identified as malicious over some time. Once the malicious data flow is identified, the software agent reconfirms the legitimacy of the flow and updates it to the control. Interestingly when the control gets this update, it can offer direct mitigation of all unauthorized requests for all the switches connected to the SDN controller. Even if one of the switches is compromised, it doesn't make any difference as the SDN controller, after receiving this update, can interact with the compromised switch and intercept all forms of malicious data flow towards it. Hence, equivalent performance is shown by the SDN controller for its switches to resist malicious request flow. More preference is offered to catching hold of an adversary and less towards the malicious links in the existing system, which significantly consumes resources. There is no much scope of similar performance in the latter part of simulation when the nodes deplete more resources. Hence, both the existing system cannot be considered to show better security performance when exposed to a larger network with a heterogeneous communication domain. A higher degree of inclination towards the security based on node parameters is the prime cause of degradation of outcome for both the existing system. However, the proposed system emphasizes the link parameters and uses a statistical approach to formulate dynamic attacker behavior and hence more successful in resisting attacks.

5. CONCLUSION

The primary motivation of the proposed work is obtained from the study findings, where it is found that there is various threat model associated with blockchain where a majority of the attack is on the application and varied forms of approaches have evolved up. Maximum studies have focused on privacy, which eventually depicts that existing approaches do not fulfill other security features. The complexity associated with the existing system ranges from medium to high. It eventually states that there are still open issues connected with existing security approaches. It is strongly felt that to develop a cost-effective and robust security approach capable of offering maximum resistance, the existing system lacks relevant information. This article discusses a novel framework where the optimized performance towards security is carried out by a unique SDN design in IoT over an adversarial scenario of an unknown type. The chapter presents a vivid discussion of the model where its applicability towards a suitable environment of IoT is justified and can be claimed of offering a good balance between security and data propagation performance in contrast to frequently adopted security approaches.

REFERENCES

[1]. Alzoubi, Yehia & Al-Ahmad, Ahmad & Kahtan, Hasan. (2021). Blockchain technology as a Fog computing security and privacy solution: An overview. Computer Communications. 182. 10.1016/j.comcom.2021.11.005.

[2]. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K.: A survey on the internet of things (IoT) forensics: challenges, approaches and open issues. IEEE Commun. Surv. Tutor. (2020). https://doi.org/10.1109/comst.2019.2962586

[3]. Abbas, N., Asim, M., Tariq, N., Baker, T., Abbas, S.: A mechanism for securing IoT-enabled applications at the fog layer. J. Sens. Actuator Netw. 8(1), 16 (2019)

[4]. By, G.S.: More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. Publicado em Janeiro (2016)

[5]. Miloslavskaya, N., Tolstoy, A.: Internet of Things: information security challenges and solutions. Clust. Comput. 22(1), 103–119 (2019)

[6]. Pavithran, D., Shaalan, K., Al-Karaki, J.N., Gawanmeh, A.: Towards building a blockchain framework for IoT. Clust. Comput. 2020, 1–15 (2020)

[7]. Gatouillat, A., Badr, Y., Massot, B., Sejdic´, E.: Internet of medical things: a review of recent contributions dealing with cyber-physical systems in medicine. IEEE Internet Things J. 5(5), 3810–3822 (2018)

[8]. Khalid, U., Asim, M., Baker, T., Hung, P.C., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Clust. Comput. 2020, 1–21 (2020)

[9]. Pal, S., Rabehaja, T., Hill, A., Hitchens, M., Varadharajan, V.: On the integration of blockchain to the internet of things for enabling access right delegation. IEEE Internet Things J. 7(4), 2630–2639 (2019)

[10]. Xia, Q., Sifah, E.B., Agyekum, K.O.-B.O., Xia, H., Acheampong, K.N., Smahi, A., Gao, J., Du, X., Guizani, M.: Secured finegrained selective access to outsourced cloud data in IoT environments. IEEE Internet Things J. 6(6), 10749–10762 (2019)

[11]. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (IoT) security: current status, challenges and prospective measures. In: Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341. IEEE (2015)

[12]. Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.: Bubbles of Trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. 78, 126–142 (2018)

[13]. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun. Surv. Tutor. 21(2), 1676–1717 (2018)