IMPLEMENTATION OF IOT SYSTEM USING BLOCKCHAIN SECURITY ANALYSIS FOR MALICIOUS ATTACK AND INTRUSION PREVENTION

[1]M. PRAVEEN KUMAR, [2]DR. T. SWARNALATHA
[1]Research Scholar, Shri Venkateshwara University, Rajabpur Gajraula, Amroha, U.P, India.
[2]Professor, Department of CSE, RSR Engineering College, Nellore, Andhra Pradesh, India.

ABSTRACT: The number of smart devices or IOT devices either it may be a smart phone, smart home, tablet or any wearable devices are connected to internet are increasing day by day. Due to this numerous number of security threats are searching for loopholes that are ready to exploit any type of network. Security threats have become critical challenges against the back-drop of recent rapid raising advancements of IOT technology that demands continuous and responsive action. As a demanding technology Internet of Things (IoT) needs best information security features for effective IOT smart city and technological activity development. In this paper an Implementation of IoT system using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention is presented. The block chain distributed behavior makes this system more immune and robust for a single failure. A Zero-Knowledge proof technique is applied for preventing the third party from checking user's original information. Integrity validation test and avalanche effect technique is processed for block chain, MD5 and SHA-256 which results the proposed block chain technology has better security.

KEYWORDS: Block Chain, Internet of Things, Intrusion Detection, Malicious Attack, security threats.

I. INTRODUCTION

The IOT broadly refers to physical devices integration which can operate, accurate and communicating autonomously for optimizing and enabling new services over a wide range of area [1]. As a progressive industrial revolution, IoT provides ubiquitous connections between many objects to the internet [2]. While the architecture of underlying network is responsible to IoT devices functionality operations and connectivity [3].

Significantly the IoT encompasses the concepts of M2M (Machine to Machine communication), WSN (wireless sensor network) and D2D (device-to-device communication) [4], medium to low energy wireless personal area network and technologies corresponding to RFID (radio-frequency identification) [5]. IoT possibly produces several security issues due to the entrance and automated integration of several applications in IoT. Practically efficient security and serviceable mechanism is the utmost significant for maintaining the reliability of IoT devices and its interconnected networks. The infrastructures of IoT are unprotected during malicious behaviors [6] and majority of security loopholes are jamming attack, replay attack, DDoS (Denial-of-service) attack, malware propagation, intrusion, sinkhole attack, mischievous sequence attack, sensor attack and routing attack [7].

With recent developments in communication technologies and device fabrication, the IoT is expected to facilitate efficient resource management and pervasive sensing in applications like smart cities, health care, smart power grids, industry automation, intelligent spaces, etc. [8]. IoT will not only causes revolutionary changes which enhance the human life quality but also cause several security challenges corresponding to access control, system configuration, privacy and information management/storage, a condition that merits careful consideration [9]. One of the most challenging IoT issue is addressing the issues of privacy and security. One of the key pillars of IoT is Heterogeneity which can lead to security issues. Designing appropriate authorization and authentication solutions is the key aspect of security and privacy issues in resource constrained IoT. The users were attentive interms of security, privacy due to the smart IoT devices extensive growth. The networks are facing several cyber-attacks from great number of IoT devices. These IoT nodes were susceptible to different attacks and threats extremely.

Advancements in various IoT based applications like industry, agriculture, smart home, healthcare, transportation, smart home, etc. are inviting hackers indirectly to achieve sensitive useful data. The non-standard deficiency and implementation of appropriate methods, constrained resources for providing security in hardware and software creates loopholes in IoT networks. The primary features of complex networks are heterogeneity and large-scale devices that distinguishes IoT security issues from traditional networks and these features appearance makes IoT devices security more challenging.

The IoT infrastructure failure and crashes are directly affected through cyber-attacks and intrusions. System performance is degraded by smart device failures. The IoT device performance degradation will affect entire network control process due to new risk disclosing. Compared to traditional systems, the IoT based networks having low stability and very high range of risk that presents high probability of attacks and intrusions. In practice several security challenges are presented in IoT networks.

II. IOT WITH BLOCKCHAIN

Ouaddah et al. [10] presented a comprehensive review of the current access control solutions in IoT based on Objectives, Models, Architecture and Mechanisms (OM-AM). Moreover, the paper presented taxonomy based on the authors' comprehensive review. The paper analyzed the strengths and weaknesses of access control models and protocols regarding the IoT environment. They presented a new type of transaction that is used to grant, obtain, delegate and revoke access based on access tokens. This is based on an Attribute-Based Access Control model. The authorization mechanism of Fair Access is based on authorization tokens, which provide access rights to a specific resource, identified based on its address and smart contract expressing its access control policies, to the requester or receiver.

Dorri et al. [11] proposed a lightweight architecture for securing IoT using private block chain technology. The presented solution uses an access control list for ensuring authorization and their

architecture encompasses three main models, namely smart homes, an overlay network and cloud storage. This solution stores the access control policies in the policy header of a local block chain and does not use a Proof of Work (PoW) consensus to validate blocks as all IoT devices in the smart home tier are controlled by the miner. They argued that the overheads of the solution are insignificant compared to its security gains. However, presented architecture is a smart home application-based solution, which is not a generic solution and may not apply to other IoT domains. Moreover, this mechanism does not support self-enforced access control policies.

Touati et al. [12] presented an activity control mechanism (a generalized version of context-aware access control) by focusing on user and system preferences to grant or deny access. They used Cipher text-Policy Attribute-Based Encryption (CP-ABE) and a finite state machine for dynamic access policy adaptation.

The author of [13] highlights various challenges in IoT based systems and identifies the following areas for research are scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security, privacy, and human-in-the loop. IoT has two major requirements in terms of security: trust and control that are difficult to achieve the large size of the given network. Although public key infrastructure (PKI) techniques have proven themselves for large-scale systems (e.g. global payments system) as a security solution, key management in an IoT environment may not be feasible due to resource constraints.

Kaiwen et al. [14] presented a hybrid role- and Attribute-Based Access Control model to target large-scale dynamic users by keeping policy integrity intact. They presented a mechanism to resolve policy conflicts and redundancy. Granting permissions and role management are still the responsibilities of the administrator in the presented model. The "Levenberg-Marquardt Back propagation (LM-BP)" neural network model was presented by Yang et al. [15] to establish intrusion detection system for IoT network. The LM-BP has higher intrusion detection rate as well as lower false detection rate as compared to "Particle Swarm Optimization Back propagation (PSO-BP)" and conventional back propagation neural network models.

III. IOT SYSTEM USING BLOCKCHAIN SECURITY ANALYSIS

The frame work of IoT System using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention and its operational analysis is shown in below Fig. 1.

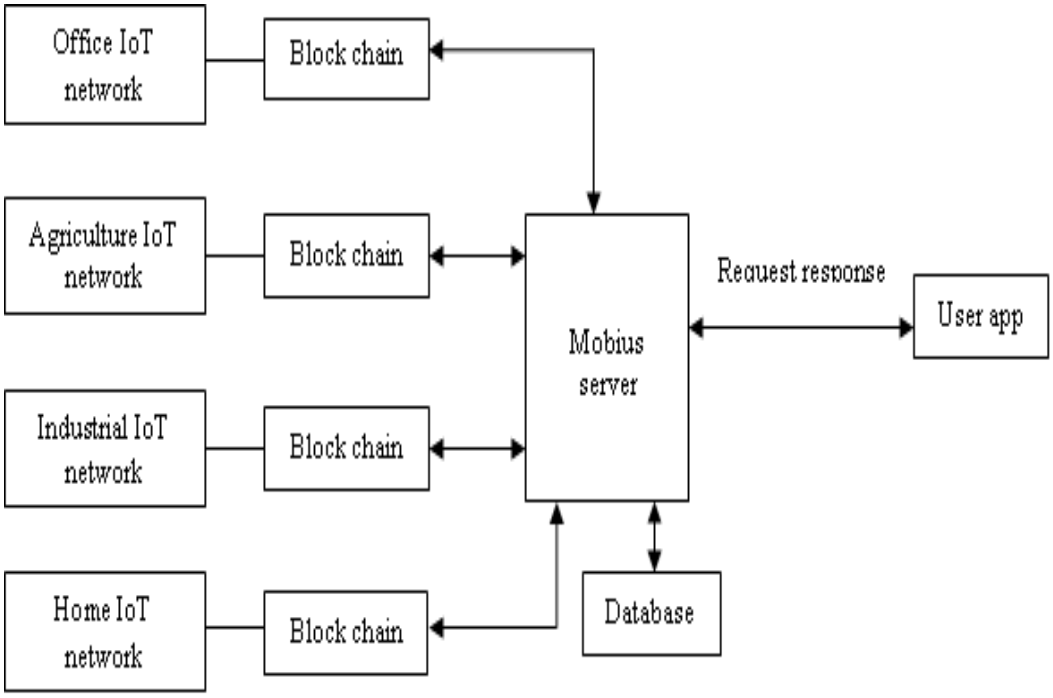

Fig. 1: FRAMEWORK OF IOT SYSTEM USING BLOCKCHAIN SECURITY ANALYSIS

In the network, every IoT device is connected to a block which is having timestamp, data and hash value. Basically hash is a unidirectional function that is fed to device data message #M1 of various length, message contains a definite messages set, M1, It will generate a digest of that message with a fixed and predetermined bit length, n1. Hence the function of hash belongs to device#1, h1 is represented as:

$$h_1: M_1 \rightarrow \{0,1\}_2^n, with\ \ h_1(m_1) = m_1'$$

In the same manner it is generated for device #2 to N:

$$h_2: M_2 \rightarrow \{0,1\}_2^n, with\ \ h_2(m_2) = m_2'$$

$$h_N: M_N \rightarrow \{0,1\}_2^n, with\ \ h_N(m_N) = m_N'$$

In the environment of presented system, open server platform of Mobius IoT is utilized for implementing a system which will share the sensor information from device to application and applied it to the server of block chain. Etherium's smart contract is utilized in block chain environment for putting the power data over the network of block chain thus all users will prove it and reliability is increased. Utilizing the created smart card with the proof function of Zero-Knowledge, utilized the anonymity-enhanced block chains for preventing data or account information from being disclosed. The configuration of system including Office IoT network,

Agriculture IoT network, Office IoT network and Office IoT network. There are 4 kinds of devices which can produce transactions by placing the data in a smart contract of block chain. Provided a decentralized security system utilizing block chain for IoT based network since there are several drawbacks in centralized security techniques. This block chain technique has several security benefits compared to traditional defense system like high integrity, third party security is not involved, secured communications and peer-to-peer authentication and many more.

The user sends 'device ID', 'password' and 'user ID' are utilized as the password of block chain smart meter via Mobius server for registering member. In the block chain the Mobius server asks a new account with the password from transmitted information of a member and account address response is received. Device ID, user ID is stored by Mobius server and account address is transmitted to member application in the database. In block chain smart contract is selecting the addresses of account which are in the server's database. After creating the block, the user transmits the member ID to Mobius software for retrieving the process and server retrieves uploaded data to the block by matched block chain address in the database, displays the data in the user application.

The Zero knowledge proof is a proof technique where information is known without exposing any information. Zero knowledge proof concept is introduced in block chain, which can prove a work or transaction without disclosing the transaction information or virtual money information to outside world. It is a proof technique that satisfies the properties like Zero knowledge, impracticality and completeness.

Integrity Validation using Block chain Degree Centrality:

In the network each connected device shares the same data which is updated into a block chain. The block chain DC (degree centrality) measurement is useful for validating the integrity and it can be represented as

$$DC(d) = \frac{degre\ (d)}{N}$$

Where degree (d) defines neighborhood devices, N defines total number of devices.

Integrity Validation using Block chain Betweenness Centrality:

On the basis of shortest path measurement the Betweennesss Centrality (BC) is measured. For every device in the IoT network pair$(v_1, v_2) \in G$, there is a link or connectivity that constitutes minimum weights or minimum number of links. A device BC is calculated as number of connections linked via device:

$$BC(d) = \sum_{i}^{N} \sum_{j}^{N} \frac{S_{ij}(d)}{S_{ij}}$$

Where N is the total number of devices, S_{ij} is number of shortest paths between the devices d_i and d_j and $S_{ij}(d)$ is the number of shortest paths that are connected through device under situation.

In the presented system when a third party or verifier knows user address only then the amount of processed work is investigated by the block. This is the individual data infringement issue because it will analyze user work pattern. If an hacker is at second crime risk like theft since the user can observe whether the house is empty or not. Hence in this paper a method is presented for protecting personal data of presented system through applying a Zero Knowledge proof technique which can prove that data is correct without giving data to the verifier. For preventing unauthorized access, the IoT based network devices keep authorization and authentication information. The data and information security is validated effectively and efficiently by utilizing block chain because it maintains data integrity.

IV. RESULTS

When the data is collected through various networks are disclosed directly by the block chain, it might violate user privacy and damages user properties. In presented system public key is generated through proving Zero-knowledge which is stored for maintaining the confidentiality without disclosing the privacy information. Further original information will be stored over the server for availability maintenance can be utilized.

The integrity validation is tested utilizing block chain technology, message digest 5 (MD5) and SHA-256 (secure hash algorithm 256). Integrity validation simulation for block chain, SHA-256 and MD5 using degree centrality is shown in Fig. 2. As represented in Fig. 2, block chain has high integrity compared to SHA-256 and MD5. Similarly, Fig.3 represents another integration validation simulation for SHA-256 and MD5 and block chain using betweenness centrality. In this case also, the block chain represents higher integrity than SHA-256 and MD5.

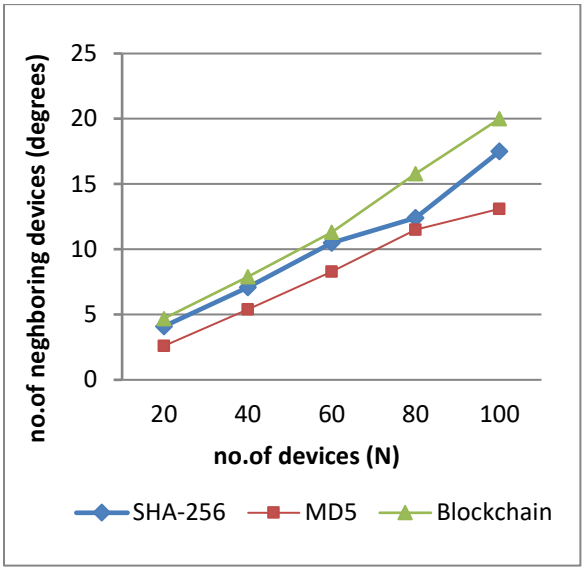

Fig. 2: INTEGRITY VALIDATION USING MD5, SHA-256 AND BLOCKCHAIN DEGREE CENTRALITY

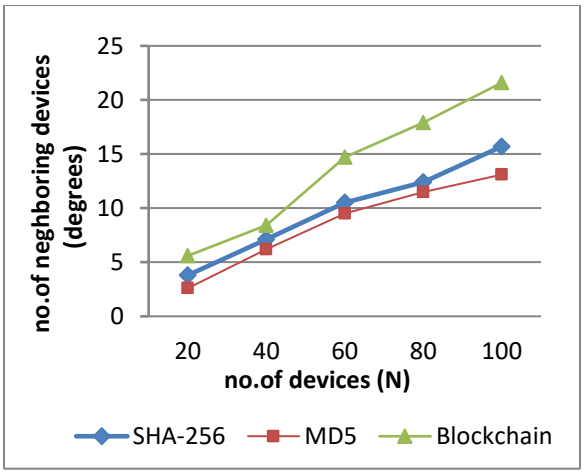

Fig. 3: INTEGRITY VALIDATION USING MD5, SHA-256 AND BLOCKCHAIN BETWEENNESS CENTRALITY

The data produced from IOT devices including sensor data, transactional data, network flow data and log information which is validating through cryptographic hash algorithms. From the Fig. 2 it is clear that block chain provides better results as an integrity validation technique compared to SHA-256 and MD5. The information of block chain is shared as a peer-peer network, if any update or change reflects a variation in all shared devices in the network.

Based on integrity technique the block chain technology maintains information similarity and records in the network devices after validation because intrusion is updated and healed through validating the block chain. The technology of block chain has developed as vital and indispensible element for secure transaction based on the communications of IoT.

Observation of hash function avalanche effect which is utilize for every IoT system. The obtained results are tabulated in Table 1. From Fig. 4, it is observed that blockchain hash function has great avalanche effect compared to SHA-256. Block chain provides better hash results because a small variation in input produces a significant variation in its output, which signifies that block chain has high security level than SHA-256.

Table 1: COMPARISON TABLE FOR AVALANCHE EFFECT

Number of input change (bit)	Number of output change (%)	
	SHA-256	Block chain
1	92	96
2	96	98
3	94	95
4	91	100
5	95	96

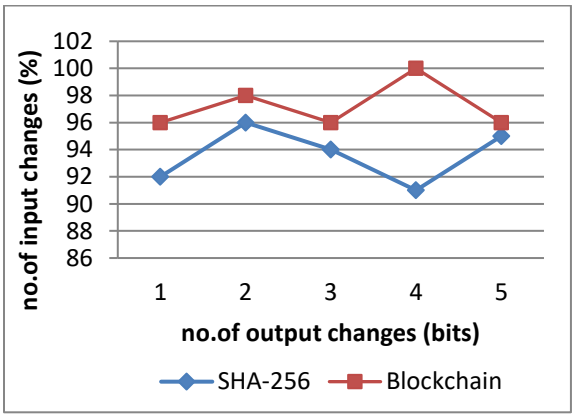

Fig. 4: AVALANCHE EFFECT ON THE HASH FUNCTION

V. CONCLUSION

In this paper, Implementation of IoT System using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention frame work is described. The block chain provides outstanding decentralized security system which is integrated and implemented into IoT based networks for defending from various threats, intrusions and attacks. A Zero-Knowledge proof technique is applied for preventing the third party from checking user's original information via block retrieval. Various tests have been performed and it is proved that IoT system utilizing block chain technique is solving the security issues which are arise in communication among IoT devices. Obtained results indicating that block chain as an integrity validation technique produces better results compared to SHA-256 and MD5. Because it has high security level than

IoT system with block chain technology thus data integrity was guaranteed. From the simulation results of testing attacks and avalanche effect observations it is cleared that IoT system with blockchain technique has greater security.

VI. REFERENCES

[1] Elang Dwi Saputro, Yudha Purwanto, Muhammad Faris Ruriawan, "Medium Interaction Honeypot Infrastructure on The Internet of Things", 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), Year: 2021

[2] Mansoor Syed Raza, Tang Zongsheng, Muhana Magboul Ali Muslam, "A review of human-to-machine and machine-to-machine approaches for internet of things", 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Year: 2021

[3] Diana Yacchirema, Carlos Palau, "Interworking of Onem2M-Based IoT Systems and Heterogeneous IoT Devices", 2020 XLVI Latin American Computing Conference (CLEI), Year: 2020

[4] Jianming Liu, Ziyan Zhao, Jerry Ji, Miaolong Hu, "Research and application of wireless sensor network technology in power transmission and distribution system", Intelligent and Converged Networks, Volume: 1, Issue: 2 , Year: 2020

[5] Laura Corchia, Egidio De Benedetto, Giuseppina Monti, Andrea Cataldo, Leopoldo Angrisani, Pasquale Arpaia, Luciano Tarricone, "Radio-frequency Identification Based on Textile, Wearable, Chipless Tags for IoT Applications", 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT), Year: 2019.

[6] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, Javier Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services", IEEE Communications Surveys & Tutorials, Volume: 20, Issue: 4, Year: 2018

[7] Zie Eya Ekolle, Kuramitsu Kimio, Kohno Ryuji, "Intelligent Security Monitoring in Time Series of DDoS attack on IoT Networks using Grammar base Filtering and Clustering", 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Year: 2018

[8] Shubaham Purri, Nirbhay Kashyap, "Augmenting Health Care System Using Internet of Things", 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Year: 2018

[9] B V Santhosh Krishna, T Gnanasekaran, "A systematic study of security issues in Internet-of-Things (IoT)", 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Year: 2017

[10] Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. Comput. Netw. 2017, 112, 237–262.

[11] Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in Iot. In Europe and MENA Cooperation

Advances in Information and Communication Technologies; Springer: Cham, Switzerland, 2017; pp. 523–533.
[12] Touati, L.; Challal, Y. Poster: Activity-based access control for IoT. In Proceedings of the 1st International Workshop on Experiences with the Design and Implementation of Smart Objects, Paris, France, 7–11 September 2015; pp. 29–30.
[13] J. A. Stankovic. 2014. Research Directions for the Internet of Things. IEEE Internet of Things Journal 1, 1 (Feb 2014), 3–9.
[14] Kaiwen, S.; Lihua, Y. Attribute-role-based hybrid access control in the internet of things. In Asia-Pacific Web Conference; Springer: Cham, Switzerland, 2014; Volume 8710, pp. 333–343
[15] Rajneesh Kumar, Shekhar Verma, G S Tomar, "Thwarting Address Resolution Protocol Poisoning using Man In The Middle Attack in WLAN", International Journal of Reliable Information and Assurance Vol.1, No.1, pp.8-19, 2013.