Addressing Security and Privacy Issues of IoT using Blockchain Technology

Bhabendu Kumar Mohanta, *Member, IEEE,* Debasish Jena, *Member, IEEE,* Somula Ramasubbareddy, Mahmoud Daneshmand *Senior Life Member, IEEE,* and Amir H. Gandomi *Senior Member, IEEE*

***Abstract*—Internet of Things (IoT) is the most emerging technology in the last decade since the number of smart devices, and its associated technologies are rapidly grown in both industrial and research prospective. The applications are developed using IoT techniques for real-time monitoring. Due to Low processing power and storage capacity, smart things are vulnerable to the attacks as existing security or cryptography technique are not suitable. In this study, we initially reviewed and identified the security and privacy issue exists in IoT system. Secondly, as per Blockchain technology provides some security solutions. The details analysis, including enabling technology and integration of IoT technologies, are explained. Lastly, a case study is implemented using the Ethererum based Blockchain system in a smart IoT system and the results are discussed.**

***Index Terms*—IoT, Security, Privacy, Blockchain, Distributed, Cryptography.**

I. Introduction

CYBER attacks on Internet of Things has increased by 22% in last quarter asserted a report titled ”State of IoT Security”. The report suggested that some of the sectors like smart cities, financial and transport, have a maximum ranking in attacks scenario. Day by day, attacks are getting sophisticated and high-grade, which is a matter of concern. In the last decade, Blockchain technology is one of the emerging concepts accepted by both research and industry, having six principal characteristics decentralized, immutable, transparent, autonomy, anonymity, and open source[1]. Similarly, IoT is also one of the promising technical filed using lots of smart application are being developed. The sensors, intelligent devices, and actuators are used to implement IoT applications. In Fig. 1, some of the promising IoT based applications are shown. The basic architecture of the IoT system is three layers consists of the physical layer, network layer, and application layer. The authors in [2], discussed security issues present in each of the IoT architecture layer. In an IoT application, different heterogeneous devices are connected and communicated to each other. As most of the smart devices are low-end devices, they are more vulnerable to different attacks. So to implement IoT based smart applications required a lightweight algorithm for encryption/decryption, secure communication, and computation. The basic security goal that is CIA (Confidentiality, Integrity, and Availability) must be maintained by the application.

To make use of the smart IoT application trust management plays an important role. As the user shares his/her personal information in public platforms, privacy is a significant concern. The user will only build the trust to use the application if security issues are properly addressed. Some of the papers citeyan2014survey and [3], mentioned that trust is an important issue that needs to be addressed.

The contributions of the article are mentioned below:

- Initially, the layer-wise security issues are identified in IoT applications.
- The article described some of the work of IoT integration with Blockchain technology to address security and privacy issues.
- The Blockchain technology in term of addressing IoT security issues are identified and explained in details.
- The implementation in Ethereum platform for authentication of IoT devices explained along with the security analysis is given at the end.

II. Security and Privacy Issue In IoT

Since the developments of IoT technology, most of the traditional applications become IoT based smart applications. A lot of work has been done regarding architecture, the protocol of IoT based applications. The security and privacy issues still need to address. In Fig. 2 layer-wise security challenges are shown.As explained in paper[4], IoT techniques have security and privacy challenges. The device has a limitation, different attacks model for IoT based application in layer-wise also described. The IoT applications are developed using a framework in paper [5], the authors have identified 8 different frameworks and their security, privacy issue for developing applications. Security and privacy issues are the most challenging part to develop the IoT application like authentication, data protection in paper[6], the authors have explained the Blockchain, fog computing, machine learning can be used to solve the issue.

The authors in [7], proposed a secure framework for data collection for the smart healthcare system. In a smart healthcare system, intelligent devices are used to monitor the critical

B.K. Mohanta and D. Jena are with the Department of Computer Science Engineering, IIIT Bhubaneswar, Odisha, India, 751003 e-mails: C116004@iiit-bh.ac.in, debasish@iiit-bh.ac.in

S. Ramasubbareddy is with Department of Information Technology, VNRVJIET, Hyderabad,India,500090, e-mail: svramasubbareddy1219@gmail.com

M. Daneshmand is with the School of Business, Stevens Institute of Technology, Hoboken, NJ 07030, USA, e-mail: Mahmoud.Daneshmand@stevens.edu

A.H. Gandomi (corresponding author) is with the Faculty of Engineering Infromation Technology, University of Technology Sydney, Australia, e-mail: gandomi@uts.edu.au

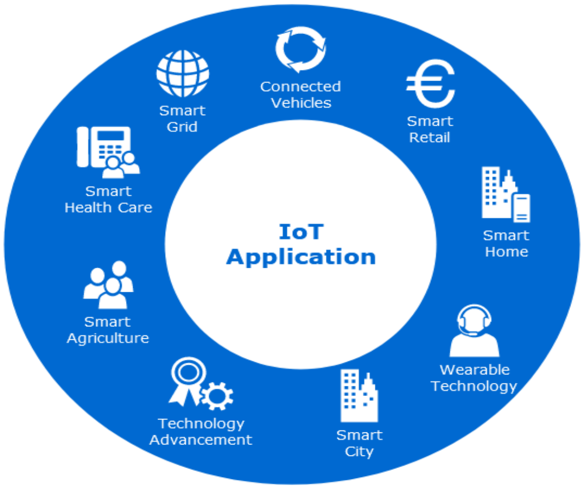


Fig. 1. Applications of Internet of Things (IoT)

patient. The smart devices are connected wireless or using wire. In some applications, devices are accessed remotely as well. For connectivity purposes, ZigBee, Bluetooth, or WiFi are used. Each of these devices is vulnerable to different types of attacks. As the IoT devices are resource constraint devices, existing security protocols, or algorithms are not suitable. For IoT devices, lightweight algorithms or protocols are needed. In this regard, the ECC based algorithm is proposed by the authors in [8] for IoT applications due to smaller key size requirements for computation. The IoT infrastructure is having three-layer such as physical, network, and application layer. The security issue is existing in each of these layers. The detailed description of security and privacy issues is explained in the following subsection.

A. Security challenges in IoT

In this subsection, the security challenges of the IoT applications are identified. IoT application mostly deals with three-layer architecture that is physical, network, and application layer. In the physical layer, devices are connected through the gateway. The hardware device has limited capability and vulnerable to the attacker. Changing the entire hardware component is not recommended if it gets hacked by the hacker. The system must address the security issue available in each layer.

1) Node capture attacks: As the smart devices are deployed in a different location as per the IoT applications. The attacker can capture the devices or replace them with the wrong device to get access to the network. In this type of physical attack, it is very hard to distinguish genius node and false node. This type of attack the attacker can get important information about the application. To make the network secure this type of attack need to be addressed.

2) Replay attacks: In a replay attack, the attackers intercept the message from the communication medium and later send the same message to the network. In an IoT, an environment attacker can hack the smart devices and send the data like the authorized node in the network.

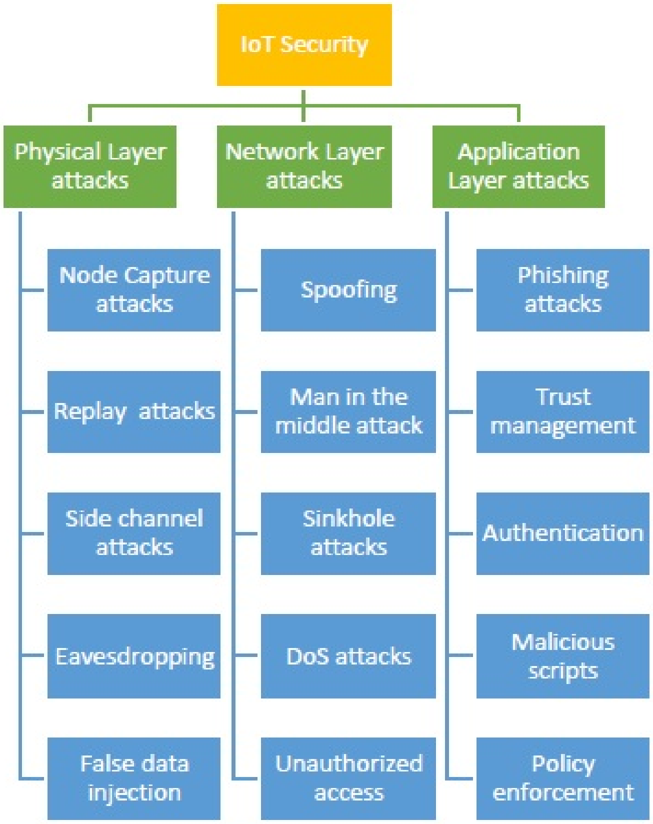


Fig. 2. Overall security issue in Internet of Things (IoT).

3) Side channel attacks: Side-channel attacks the attacker tries to get the plain text from the ciphertext. In this attack, getting the key using some time constant is important as most of the encryption techniques use key exchanges for encryption/decryption.

4) Eavesdropping: The eavesdropping attack occurs in an IoT scenario where smart devices are compromised. As the communication channel is not secure, the attacker can read the message communication between two devices. It like a passive attack where the adversary access the data from the not secure transmission medium.

5) False data injection: The sensors or smart devices deployed in a different location to read the environmental information. The sensors and smart devices are capable of capturing the information and forwarding it to the next layer. As smart devices are resource constraint, they are vulnerable to the attacker. The attacker tries to capture the device or read the value from the not secure communication medium and inject the false information to the network.

6) Spoofing: In the network layer, the attacker tries to gain access to smart devices. Once it gains access to the devices, the attacker behaves like a legitimate node in the network. The false messages are transmitted to the network.

7) MITM attack: In Man In The Middle (MITM) attack, the attacker tries to attack the communication medium when the data is on transit. They watch the data packets running through the medium try to draw some pattern or insights which is very vulnerable to the victim. This type of attack is two types of active and passive attacks.

8) Sinkhole attacks: The sinkhole attack is one of the routing attacks in IoT applications. As the message is transmitted through different routes between two nodes, it creates network traffic to breakdown the network. The type of attack compromises the node in the network. This attack also reduces the performance of the network protocol.

9) DoS Attacks: The denial of service attack is a type of cyber-attack in which the attacker utilizes the assents of the system. It tries to overflow the server with a large sum of traffic. As a result, it will unable to use the full amount of bandwidth resources, although it doesn't result in a loss of crucial data that costs a huge loss of the victim.

10) Unauthorized access: The attackers target the resource constraint devices connected to the IoT applications. As most of the devices connected using a different gateway. The attacker tries to capture authorize credential using different attacks. Once get the personal credential, the attacker access the network information.

11) Phishing attacks: IoT application has a lot of users. Every user has their own identity, they access the information of the smart devices or control them using the application layer. The attacker tries to important information about smart users/smart devices by sending a false message or email.

12) Trust management: A Trust management issue in the application layer is a challenging task. As IoT based application to monitor and manage the environment in real-time users, share personal information into the network. During computation in a decentralized environment, information is share and broadcast to the network. So trust management issues will arise among the nodes in the network. If any node behaves maliciously in the network, it must be identified by the network. So proper trust management is essential in the IoT system.

13) Authentication: An IoT application consists of intelligent devices, sensors, actuators, and some smart devices to monitor as well as do the computation. The data or information are capture by the smart devices and forward to the next layer for processing and computing. Once the computation is done, the corresponding event is trigger by the network node. For secure and efficient computation, actual data are required from the sensors. If the sensors or intelligent devices get capture by the attacker or an attacker part of the network, then the system becomes corrupt. For this, each and every device must be registered or authenticate to the network. Authentication is one of the important issues in any IoT application.

14) Malicious Attack: In IoT applications, smart devices are vulnerable to the outside world due to insecure communication channels and wireless connectivity. An attacker can inject o malicious code in the device through application and the device might be compromised.

15) Policy enforcement: In IoT application policy is one of the essential security concerns so that user can use the smart devices. As per requirement of the application sufficient police must be develop to protect the user privacy.

Data Collection
Data Aggregation
Data Analytics

Fig. 3. Steps of information gathering in IoT application

B. Privacy Challenges in IoT

The basic IoT architecture consists of three layers physical, network, and application layer. In the physical layer, numerous IoT smart devices are deployed in an application. These devices collect a huge volume of data from the environment. The data collections as shown in Fig. 3 of IoT application are performed in the following three ways:

- Collection: This is the first step where sensors and smart objects collect the raw data and forward it for processing.
- Aggregation: In this step, collected data are combined to get the information for further processing.
- Analytics: In this step, as per the applications, actual or meaningful information is extracted from the aggregate data by doing the different analysis through some techniques.

While data collection and processing is a critical part of IoT application, but privacy issues are raised in these data collection steps. For example, IoT enables the hospital system if the attacker gains information about the patient details, then it creates a set of the patients. Similarly, in smart city applications, if the user location and travel details are leak or capture by the attacker, then it raised privacy concerns. Privacy preservation techniques are needed to be designed to overcome the privacy issue in IoT system.

III. Critical Work on IoT security and Privacy using Blockchain

In the last decade grown of IoT devices and its use cases is significant. As smart devices are resource constraints in nature, there are vulnerable to the different types of attacks. In a centralized architecture, a single point of failure is one of the primary issues. During data communication and computing, applications face different security issues in each layer. So in recent time research community use the Blockchain a decentralized technology to address some of the security and privacy issues. Table I shows some of the work done by the research community to address the issue like trust management, secure storage, authentication, privacy preservation, and access control in details. From the literature survey, it was understood that Blockchain could be utilized to solve some of the security and privacy issues associated with IoT. In this work, we have tried to address how some of the security and privacy can be solved using Blockchain technology. An in-depth analysis is given in section V.

TABLE I
LITERATURE WORK

References	**Focus Point**	Contribution
[9] [10]	Scalable access Management	In IoT application, to meet the consensus in the network algorithm, need to be lightweight. The authors proposed a PoBT mechanism with less computation for validation and creation of blocks in the Blockchain network. Similarly, Lightweight Scalable Blockchain (LSB) is another method already proposed by the authors for IoT devices scalability in a smart home application.
[11] [12]	Trust Management	Trust is one of the critical factor in IoT application. The user share personal information in network for processing and computation where trust is critical factor. Example like smart city or smart healthcare system personal information are share in the network.
[13]	Secure Storage Management	The authors in this paper proposed an "BeeKeeper" in IoT system based on Blockchain technology. In the proposed system, nodes can perform the homomorphic encryption and process for further computation. Any node in the network become leader if wish for. malicious activity are also identified using this proposed method.
[14][15][16]	Authentication	Internet of Things smart device is communicated to each other without human intervention. Confidentiality, integrity, and availability are the primary security mechanism in any system. The authentication of the device is needed to maintain the integrity of information in the network. It also essential to authenticate all devices to prevent the network from unauthorized access. Centralized authentication is not suitable in the IoT system. The research community already proposes some of the decentralized authentication techniques for IoT devices.
[17] [18]	Privacy preservation	In an IoT application, data are collected from the sensors. In the data analysis phase, information needs to extract without revealing the privacy of the users. Privacy preservation is a vital issue that needs to address during data processing. Some work has done to address privacy-preservation in the Blockchain network by doing encryption in the data.
[19] [20]	Access Control	Access control is a major factor in IoT application as a large number of devices are connected and communicate with each other. So a secure access policy is needed to guarantee the use of smart devices. The existing access control policy is not suitable for IoT devices. In in Paper [19] and [20] authors proposed a light-weight access control policy using Blockchain network.

IV. Architecture and functionality of Blockchain

The Blockchain is basically a decentralized, distributed, immutable and share digital ledger which stores valid transaction in peer-to-peer network. The valid transactions are store in block with timestamp after mining process is done by the miner node. Each block stores the previous block hash value along with others attribute shown in Fig.4. The Blockchain uses SHA-256 and elliptic curve cryptography (ECC) for data integrity and authentication. The Fig.5 describe the elliptic curve digital signature algorithm used in Blockchain system. In a Blockchain network nodes are connected in mesh like topology. Each node in the network carry two keys: a private key and a public key. The public key is the unique address use to encrypt the message by the node in the network. The private key is used to sign the transactions and also to decrypt the message receive from others node.Depending upon the uses Blockchain network is divided into public(permissionless) and private(permissioned) types.

The key pair of a Node N_1 is associated with a particular set of Elliptic curve domain parameters DP = (q, FR, a, b, G, n, h). E is an elliptic curve defined over F_q , and P is a point of prime order n in E(F_q), q is a prime. Each Node N_1 does the calculation, key generation and message signing with ECDSA.

Algorithm 2: ECDSA Key Generation

```
Result: $K_{pri}^{N_1}$: $N_1$ $'$s private key, $K_{pub}^{N_1}$: $N_1$ $'$s public
        key
P = A point of prime order n in E($F_q$)
$K_{pri}^{N_1}$ = rand() % n - 1 + 1;
$K_{pub}^{N_1}$ = $K_{pri}^{N_1}$ * P;
```

For verifying the signature (r, s) of node N_1 on the message M_1, Node N_2 obtains an authenticated copy of N_1 $'$s domain

Algorithm 1: Calculate Total White Space

```
Result: Calculate the total white space
WSCalculation(Root)
if $R_{LL}$ then
    WSCalculation($R_L$)
    WSCalculation($R_R$)
end
$R_D = R_{LD} + R_{RD}$
```

Algorithm 3: Message Signing using ECDSA

```
Result: The signature for the message $M_1$ is the pair
        of integers (r, s)
  Input: Message $M_1$, domain parameters DP = (q, FR, a, b,
  G, n, h)
  begin:
  k = rand() % n-1 + 1
  if $r \neq 0$ then
      $x_1$ = rand() % q - 1
      k*P = $x_1$
      y = $x_1$ mod n
      r = $x_1$ mod n
      Calculate $k^{-1}$ mod n
      s = $k^{-1}$ H($M_1$) + $K_{pri}^{N_1}$*r
      if $s = 0$ then
          go to begin
      end if
  else
      go to begin
  end if=0
```

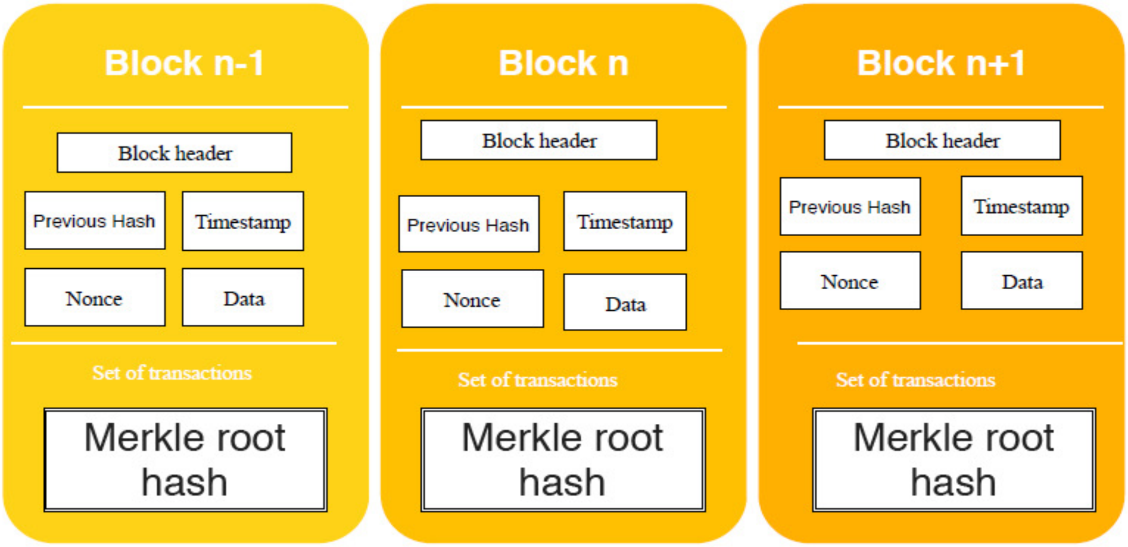


Fig. 4. Blockchain basic transaction details

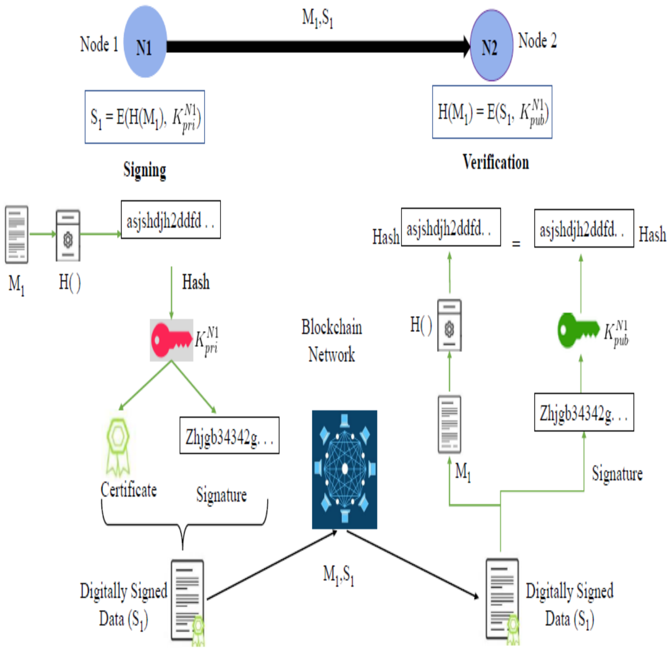


Fig. 5. Digital signature apply for user identity.

parameters DP = (q, FR, a, b, G, n, h) and public key $K_{pub}^{N_1}$ and do the signature verification using ECDSA.

Algorithm 4: Signature Verification using ECDSA

```
Result: Accept or Reject the Signature
  if 1 $\leq$ r $\leq$ n-1 & 1 $\leq$ s $\leq$ n-1 then
    w = $s^{-1}$ mod n
    Calculate H ($M_1$)
    $u_1$ = H ($M_1$)*w mod n
    $u_2$ = r*w mod n
    $u_1$* P + $u_2$* Q = $(x_0, y_0)$
    v = $x_0$ mod n.
    if v == r then
      accept the signature
    else
      reject the signature
    end if
  end if=0
```

V. Impact of Blockchain for IoT

In paper [21], the authors discussed the layer-wise security issue, like low-level, intermediate-level and high-level. Similarly paper also addressed the protocol and communication challenges in IoT and its solution approach in terms of Blockchain. In paper [22], authors study the different security aspects of IoT applications and integrate how digital ledger information will be stored securely using Blockchain. The authors in [23], proposed an efficient Blockchain-based distributed model integrate with the Internet of Things which provide security and privacy.

Blockchain technology has some consensus algorithm exists which are already described by the researcher. The consensus algorithms are Proof of Work (PoW), Proof of Burn (POB), Proof of Stake (PoS), Raft, Practical Byzantine Fault Tolerant (PBFT), Paxos, etc. The authors in [24] described in details about the distributed consensus algorithms. In the Blockchain system, consensus algorithm is important to maintain the transparency and make the decision efficient as multiple nodes

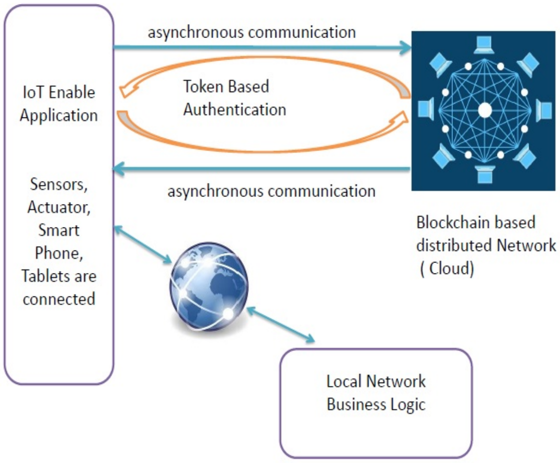

asynchronous communication
IoT Enable Application
Token Based Authentication
asynchronous communication
Sensors, Actuator, Smart Phone, Tablets are connected
Blockchain based distributed Network (Cloud)
Local Network Business Logic

Fig. 6. Proposed Blockchain based solution architecture.

involves in the decision-making process. In IoT applications, real-time decision and monitoring is done. To ensure the integrity of the data and to have trust among the nodes, Blockchain is used to authenticate and authorization purpose outside the IoT network.

A. Solution Approach using Blockchain

Internet of Things (IoT) consists of smart thing capable of sensing and processing in real-time. As the devices are resource constraint devices doing complex computation or applying cryptography algorithm is not suitable. So the light weight algorithms are essential for IoT devices. As explained in section II, several security issues are existing in IoT system. To make the real use of IoT concept security issue need to be addressed. One of the solution approaches is using Blockchain technique. As shown in the Fig.6,IoT enable application using the wireless or wired devices are connected. Initially, all the smart devices connected to the applications need to have authentication in the outside network that is Blockchain network. Once devices are registered, they can perform different activity as per their features locally. Similarly, users are also required to authenticate in the Blockchain network initially. After that, they can monitor or access the different smart object present in the network. The authors in paper [14], proposed "Bubble of trust" for authentication of the IoT devices in the decentralized network. Similarly, in paper [25], the authors proposed "DecAuth" a decentralized authentication technique using Ethereum platform for IoT devices. The proposed work suggested that only authentication and authorization need to be done in the Blockchain network.

- Authentication and authorization should not be localized and should be kept outside of IoT network.
- Blockchain-based authentication will add trust to the IoT applications.
- Latency issue of Blockchain will not impact BAU(Business as usual) operation in IoT network.
- Only new device addition or new user addition would require Blockchain operation.
- Scaling of the IoT network will be strictly controlled through Blockchain permission.

B. IoT Applications a Blockchain Solution Approach

Blockchain is not always the first choice in every IoT applications. The existing centralized database system is suitable for some IoT applications. Before using the Blockchain technology, the designer must see some of the criteria like centralized/decentralized system, nodes are trusted to each other or not, information need to share among all peer or not. No doubt that in an IoT application, a huge number of devices is deployed for information gathering. So to avoid the system throughput, devices could be made into different clusters and assign with a high-end system like fog device to process and compute this information. Finally, all fog nodes communicate with each other by applying some business logic to come to the final decision. Blockchain has a different type like public, private, permissionless, permissioned depending on the architecture, and demand of IoT application system can be built. Then using smart contract and consensus algorithm computation and computing can be done in a distributed way avoiding the third party. The business logic is written in terms of smart contracts and deploys in the network, which will execute independently. The security challenges are avoided using a digital signature, timestamp, and encryption technique in the business logic. Table II described the details about Blockchain solution for some of the security issue in IoT application.

VI. Experimental Setup and Results analysis

The security and privacy issues in IoT like non-repudiation, data integrity, data privacy and authorization, secure communication, and secure unique identification are addressed using Blockchain technology. For implementation purposes, Ethereum open-source platform is used. Initially, a smart home environment is built based on IoT enable technology. As shown in Fig.7 different gas level (MQ6, MQ9, MQ135,etc.,), and temperature DHT22 sensor connected to the Raspberry Pi device in the room. The Raspberry Pi device is used to collect the data from sensors devices and performed computation in a distributed architecture. The Ethereum platform is installed in a laboratory system. Authentication of the node is performed on the client-side, using Ethereum' web3.js. Each device is assigned with a unique address accessible globally. The IoT device identity is controlled by the user's master account that is used for the management of accounts. The authors used Ethereum Blockchain connected to an Ethereum wallet account provided by ganache, which is a test Ethereum network provided for development purposes. The decentralized "Decauth" authentication technique [25] is used to authenticate all the intermediate devices. Once all the devices are connected to the distributed Blockchain network using the hashing and cryptographic concept transaction are made immutable and available to all user. In the Ethereum platform, login and registration pages are created. The registration page, devices are registered and assigned with a pair of keys; one is the unique address accessible globally. In the login page device

TABLE II
POTENTIAL SOLUTION FOR SOME OF THE SECURITY ISSUE

Security issues	**Corresponding Solution**
Secure Unique Identification	In a Blockchain system, address use is a 160 bit of hash value. This address is a public key generated using the ECDSA algorithm. The total address space is equal to 2^{160} , which is nearly $1.47 * 10^{48}$. The address collision chance is 10^{48} . So in IoT application, each device could be assigned with a unique address accessible globally. This unique address could be assigned to the IoT devices easily, unlike IPV6 address space, which requires more computation power.
Secure communication	The IoT architecture message communication takes place using a protocol like MQTT, XMPP, AMQP, LPWAN, CoAP. These protocols are integrated with a security protocol like DTLS, TLS, and IPSec. However, they are still not suitable because of higher computation, key management, and key distribution in a centralized server.The Blockchain system, each node/device carries a pair of key, one is the unique address of 160bit, and another one is a private key. In the Blockchain network, no key management or key distribution needs to maintained, which increases the chance of applying more lightweight protocol. Even a smart contract is used to do the business logic in the distributed environment using the unique address.
Data privacy and authorization	Some application like smart healthcare, smart home, smart city information collected from the sensors is personal information, accessibility of this information need a proper access control mechanism.In a Blockchain-based network, smart contract plays a vital role in data privacy and authorization. The smart contract is a self-executable program. All the data access policy, time, and conditions are written in a smart contract for an individual or group of a user in the application. The smart contract provides the right to ownership of IoT devices and helps in the update, add, or decision-making process securely.
Non-repudiation	The Blockchain network node combines digital signature with the data it sends/broadcast in the network. As every message has a signature as a stamp in the message, no one can deny the authority of the message. It creates trust among the nodes in the network.
Data Integrity	Data integrity is one of the important issues in the IoT application. In most of the cases, data integrity is provided by the trusted third party in IoT applications. From the beginning of Blockchain systems, transactions are immutable means it's very difficult or near impossible to modify the recorded transaction in a Blockchain network. In a Blockchain network, data modification, delete, and edit is not possible.

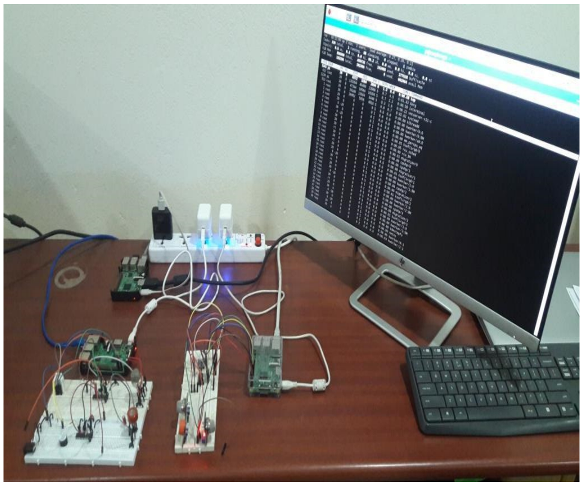


Fig. 7. Experimental Laboratory setup for smart IoT System.

can login using a unique address. Each transaction is broadcast in the network. The nodes in the network verify using the previous information stored in the digital ledger or Blockchain database. The three Raspberry Pi devices are used to process and performed computation in a distributed network. The smart contracts are developed for logic as per the application requirement. The solidity platform is used to write the code for a smart contract in the Ethereum network. One of the logic developed for smart home IoT application is to check the threshold value of the collected gas and temperature from different sensors. The network node does the verification and validation, and a smart contract is automatically run in the Ethereum platform. The outcome of the smart contract is broadcast in the network using the digital signature and encryption.

VII. CONCLUSION

IoT techniques are used to implement the different applications like smart city, smart home, smart transportation system, healthcare system, agriculture field, supply chain system. The innovation of smart things having wireless connectivity, storage space, and some processing power makes to use these devices in real-time. However, the IoT system having security and privacy issue present at a different level. This paper addresses the security and privacy issue present in the IoT system. As Blockchain being the distributed network and security is maintained. In this study, Blockchain is integrated with IoT and implemented using the Ethereum platform for testing purposed. Some sensors devices are used to create the IoT smart environment and devices are authenticated using DecAuth protocol in the Ethereum platform. Smart contracts are written and deployed in the Blockchain network for testing purposes.

REFERENCES

[1] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[3] G. Lize, W. Jingpei, and S. Bin, "Trust management mechanism for internet of things," *China Communications*, vol. 11, no. 2, pp. 148–156, 2014.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[5] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of iot frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[6] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[7] K. Jaiswal, S. Sobhanayak, B. K. Mohanta, and D. Jena, “Iot-cloud based framework for patient’s data collection in smart healthcare system using raspberry-pi,” in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*. IEEE, 2017, pp. 1–4.

[8] U. Satapathy, B. K. Mohanta, D. Jena, and S. Sobhanayak, “An ecc based lightweight authentication protocol for mobile phone in smart home,” in *2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2018, pp. 303–308.

[9] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, “Pobt: A light weight consensus algorithm for scalable iot business blockchain,” *IEEE Internet of Things Journal*, 2019.

[10] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Lsb: A lightweight scalable blockchain for iot security and anonymity,” *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[11] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, “Trustchain: Establishing trust in the IoT-based applications ecosystem using Blockchain,” *IEEE CLOUD COMPUTING*, vol. 5, no. 4, pp. 12–23, 2018.

[12] L. Xie, Y. Ding, H. Yang, and X. Wang, “Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets,” *IEEE Access*, vol. 7, pp. 56 656–56 666, 2019.

[13] L. Zhou, L. Wang, Y. Sun, and P. Lv, “Beekeeper: A Blockchain-based IoT system with secure storage and homomorphic computation,” *IEEE Access*, 2018.

[14] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of trust: A decentralized Blockchain-based authentication system for IoT,” *Computers & Security*, vol. 78, pp. 126–142, 2018.

[15] C. Lin, D. He, N. Kumar, X. Huang, P. Vijaykumar, and K.-K. R. Choo, “Homechain: A blockchain-based secure mutual authentication system for smart homes,” *IEEE Internet of Things Journal*, 2019.

[16] A. Gauhar, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E. A. Qazi, and A. Ali, “xdbauth: Blockchain based cross domain authentication and authorization framework for internet of things,” *IEEE Access*, 2020.

[17] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, “Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, 2019.

[18] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, “An iot-oriented privacy-preserving publish/subscribe model over blockchains,” *IEEE Access*, vol. 7, pp. 41 309–41 314, 2019.

[19] O. Novo, “Blockchain meets IoT: an architecture for scalable access management in IoT,” *IEEE Internet of Things Journal*, 2018.

[20] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, “A novel attribute-based access control scheme using blockchain for iot,” *IEEE Access*, vol. 7, pp. 38 431–38 441, 2019.

[21] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[22] N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in iot,” *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[23] S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, and A. Khanna, “An efficient lightweight integrated blockchain (elib) model for iot security and privacy,” *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, 2020.

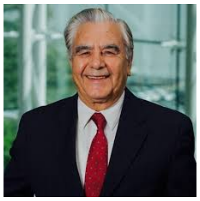
[24] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, “Study of blockchain based decentralized consensus algorithms,” in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, 2019, pp. 908–913.

[25] B. K. Mohanta, A. Sahoo, S. Patel, S. S. Panda, D. Jena, and D. Gountia, “Decauth: Decentralized authentication scheme for iot device using ethereum blockchain,” in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, 2019, pp. 558–563.

Bhabendu Kumar Mohanta received his B.Tech. and M.Tech. degree in Information Technology 2007 and 2012 respectively. Presently he is pursuing Ph.D in International Institute of Information Technology (IIIT) Bhubaneshwar. His research focuses are Information Security and IoT Security and Blockchain Technology.He has published more than 20 articles which include international conference and journal.

Dr.Debasish Jena received his B Tech degree in Computer Science and Engineering, his Management Degree and his M.Tech Degree in 1991, 1997 and 2002 respectively. He got his Ph.D degree from NIT Rourkela in 2010. He is currently working as Associate Professor in IIIT Bhubaneshwar. In addition to his responsibility, he was also IT, Consultant to Health Society, Govt. of Orissa for a period of 2 years from 2004 to 2006. His research areas of interest are Information Security, Cloud Security, IoT Security and Blockchain. His professional memberships include IEEE, ACM, ISTE, IACSIT, MIE (I), CSI, and OITS.

Somula Ramasubbareddy received the master’s degree in computer science and engineering in 2015. He is currently pursuing the Ph.D. degree in computer science with VIT University Vellore, India. His areas of interest are mobile cloud computing and big data analytics.



Dr.Mahmoud Daneshmand (Senior Life Member,IEEE) received the B.S. and M.S. degrees in mathematics from the University of Tehran, Tehran, Iran, and the M.S. and Ph.D. degrees in statistics from the University of California at Berkeley, Berkeley, CA, USA. He is a Co-Founder and a Professor with the Department of Business Intelligence and Analytics, and a Professor with the Department of Computer Science, Stevens Institute of Technology, Hoboken, NJ, USA. He has over 40 years of industry and university experience as a Professor, a Researcher, an Assistant Chief Scientist, the Executive Director, a Distinguished Member of Technical Staff, a Technology Leader, the Chairman of Department, and the Dean of School with Bell Laboratories, Murray Hill, NY, USA; ATT Shannon Labs—Research, Florham Park, NJ, USA; the University of California at Berkeley; the University of Texas, Austin, TX, USA; the Sharif University of Technology, Tehran, Iran; the University of Tehran, Tehran; New York University, New York, NY, USA; and the Stevens Institute of Technology.

Prof. Amir H. Gandomi (Senior Member, IEEE) received the Ph.D. degree in engineering from the University of Akron, Akron, OH, USA.

He was an Assistant Professor with the School of Business, Stevens Institute of Technology, Hoboken, NJ, USA, and a Distinguished Research Fellow with BEACON Center, Michigan State University, East Lansing, MI, USA. He is a Professor of data science with the Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW, Australia. He has published over 160 journal papers and five books which collectively have been cited more than 16 000 times (H-index = 58). He has been named as one of the most influential scientific minds and the Highly Cited Researchers (top 1%) for three consecutive years, from 2017 to 2019. He also ranked 18th in GP bibliography among more than 12 000 researchers. His research interests are global optimization and (big) data mining using machine learning and evolutionary computations in particular.

Prof. Gandomi has served as an Associate Editor, an Editor, and the Guest Editor for several prestigious journals. He is active in delivering keynote and invited talks.