**INFORMATION SYSTEM SECURTIY**

**ASSIGNMENT 5**

RESEARCH PAPER REVIEW 1

**Topic:** Privacy-preserving Blockchain based IoT Ecosystem using Attribute-based Encryption

**Name:** Ayesha Ausaf

**Roll No:** 17k-3867

**Section:** F

Over the years, IoT devices are being largely used by people in various fields, and most importantly in the critical applications, because of their beneficial characteristics. IoT devices makes it easier to solve critical problems, such as eHealth in real time, but such systems call for high security and privacy measures which is a little challenging to provide in IoT devices. Therefore, many researchers are trying to apply the concept of block chain to achieve their security and privacy goals in such IoT applications.

Moreover, the author states that some of the other researchers from the industry have proposed various solutions in the past to overcome this weakness. One of them is the work that proposed an enhanced blockchain technology suitable for IoT devices, and would’ve allowed end-to-end service for smart home application. Another one proposed a hierarchal structure to improve the consumption of resources and increase the stability of network. One other research paper proposed to use blockchain to process the sensors’ data gathered by IoT devices using 4G/5G network in a distributed manner. The most recent work eradicated the need of a centralized server to store sensors’ data and used blockchain’s technology to support the devices, and manage distributed sensor data in a similar way to crypto currencies.

Author is addressing that even though all the previously proposed methods support integrity and non-repudiation of data, as block chain makes data tempering impossible once the data has been saved in the block chain, but these methods fail to provide privacy and confidentiality of data or the IOT devices during the transactions; this makes IoT devices insecure to use in such critical systems.

The problem being addressed in this research paper is important because data security and privacy is a major concern in today’s world. A person’s data encapsulates his/her true identity, and we have advanced so much in technology that if that data is released in public, it can be misused or tempered for wrong reasons. So as service provider, it is our duty that when a customer provides his/her data, it should be kept confidential and under strict security. And it is the customer’s right that their data should not be shared with anyone else without his/her consent.

Keeping this in mind, the author has proposed a method that utilizes the modern attribute-based encryption (ABE) technique to deal with confidentiality and privacy of information and data shared in IoT ecosystems that are based on blockchain. Author quotes that ABE is a simple type of encryption which provides control of access and confidentiality through single encryption and has been recognized as a possible technology for sharing data among decentralized networks. Furthermore, the author claims that this proposed work is the first study that revamps the blockchain protocol to integrate ABE and gives an IoT ecosystem based on blockchain that preserves end-to-end privacy.

Author has then described the work he has proposed. He started off by mentioning the system model that has been assumed in the paper i.e. IoT network model. Following the steps of previous work that has been done for the same cause, author took a hierarchal approach. The system has a powerful cluster head for a given set of IoT sensors which performs operations like encryption and processing on the data it receives from the IoT devices.Furthermore, for incorporating ABE in the system, four parties will be involved; cluster head (data owners), blockchain miners (can be cluster heads or service providers), attribute authorities (AA) and distributed ledger.

Cluster head processes the data that he/she receives from the sensors and encrypts it before transaction. The encryption is done in such a way that the transaction can be viewed and verified by the particular blockchain miner who has the correct attributes. This will allow the cluster head to have a strong control over the data privacy. AA has the responsibility of verifying and issuing credentials for multiple miners and users according to their attributes (according to the decentralization ABE scheme taken from the literature). In this way, single point of failure can be avoided as the set of attributes can be monitored by different AAs.

De-centralized ABE has further five protocols; setup, AA setup, key issuing, encryption and decryption. In a nutshell, protocol takes an input of predefined security parameters, and system outputs its own parameters. Those system parameters are further used to generate key pairs which are then issued to a user/miner along with a set of attributes. In addition to this, encryption is applied on it by cluster head to send the cipher text to miners. Miners and users of blockchain use decryption algorithm to decrypt the cipher text. The decryption will only be successful if the attributes received satisfy the structure used to view cipher text.

Author has quoted some other alternate schemes of ABE that can be used and has explained how these schemes are built using mathematical expressions.

To support the proposed idea and convince readers, author has discussed in detail the three significant security benefits of using blockchain in IoT. The first one is that the sensor data that is being generated by IoT devices will be verified by multiple miners in the blockchain network. Moreover, data becomes untampered once it has been appended to the blockchain. Furthermore, since there is no server to store data at, miners can easily identify incorrect data. Lastly, miners can get additional rewards which they can avail later.

Author has also mentioned a possible problem that might affect the proposed system. Since ABE technique is being enforced, lesser number of people might qualify for verification as compared to traditional blockchain network, and this might jeopardize the security. In order to ensure that such thing doesn’t happen, the protocol will limit the number of miners and AA will have to wait. AA will then go through the miners’ attributes before issuing. Other than that, author has assumed that there are no other security vulnerabilities in the proposed design as it is well thought and studied. Author then compared the proposed model with the previous work that has been done, and found out that the model proposed is less complex than the previous ones, but it has greater computational cost. In conclusion, if multiple AAs are present, the time complexity of security subject slightly increases.

In a nutshell, author is confident that the proposed model will be highly beneficial as it gives privacy to transaction data during verification and in blockchain. Moreover, it will limit the data access and data miners can take a part in the mining process regardless of the attributes they have. Author has undoubtedly made the security better without ruining the fundamental security properties of blockchain. The model has been proposed after extensive research and numerical analysis has been done to support the claim. In future, this model can be further extended and the drawback of the computational overhead can be minimized.