Malware Analysis Framework Using Graph Theory

Pronaya Bhattacharya1[1] and Sudeep Tanwar[1]

[1]Affiliation not available

July 27, 2022

Introduction:

Malware detection is one of the leading security issues in Network Security paradigm. There exist different malware families. All of the families of malware are even not completely discovered[1]. In case of an unknown malware family of attack detection is various challenging tasks. In the current trend of malware detection used some data mining technique such as classification and clustering. The process of classification improves the process of detection of malware.

The chains are cryptographically auditable as they rely on Merkle root value and order-execute architecture in which blockchain network orders the transactions first using a consensus protocol and then executes them in the listed order in all

Peer nodes in a sequential manner. The hash in any i th block is computed as Hi =f(inputi, IDi,Timestamp, Hi-1)whereinputi istheinputdocument,IDi is the digital identifier associated with the document, Timestamp is the current timestamp value, and Hi and Hi-1 are the hashes of current and previous blocks, respectively.

Section 3 provides the technological aspects of integration of blockchain in MEC and designing of mining as a service (MaaS) in MEC architecture.

2 Overview of MEC Architecture

Modulars in MEC:

Network capability exposure modular securely provides network services like location, video/voice calling through the invocation of suitable application programming interfaces (API), thus providing platform as a service (PaaS)

The MEC Architecture:

A radio access network (RAN) is used at the lowest level of communication which facilitates the connections between the mobile devices and the edge network

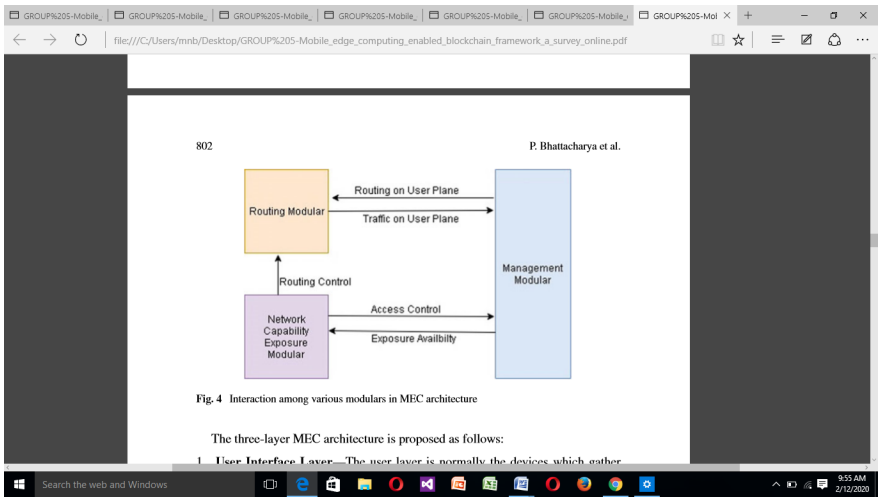

Fig. 4 Interaction among various modulars in MEC architecture

The three-layer MEC architecture is proposed as follows:

1. User Interface Layer —The user layer is normally the devices which gather data like mobile, IoT sensors, social networks, and big-data applications which normally communicate with RAN network the applications need to transfer huge data for the computation to the MEC edge servers.

2. MEC Servers— These MEC servers provide content offloading services where the useful content of the applications could be kept at servers and downloaded whenever required. This ensures resource optimizations and saves useful time.

3. Cloud Servers —The content which is only requiring heavy computations is forwarded to the cloud platform, and the results are shared back to the MEC server.

4. Artificial Intelligence Services: This framework is encapsulated in AI services. AI is the most used techcnology in diffenrt technological domain such as product management ,education ,automation etc[2-4].

At the top level, we have the cloud-based services for computations not possible at edge level, and one deployment is performed at cloud nodes[5]. content replicas are again maintained at MEC nodes to facilitate faster processing.

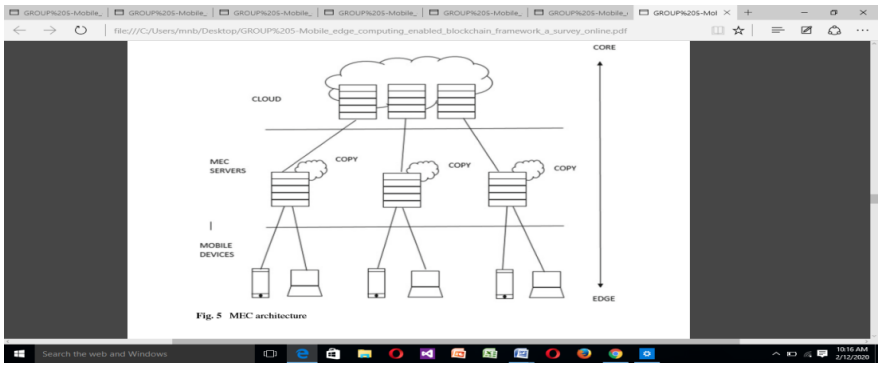

Fig. 5 MEC architecture

3 Blockchain Consensus and Mining in MEC Architecture

Security Issues in MEC Architecture:

MEC can be characterized into various forms such as on-premises, proximity, lower latency, location awareness, and network context information Some of them are listed in Table **1.**

Table 1 MEC security architecture issues

Security parameters	Services violation	Possible attacks
Confidentiality	Location aware services to the end-user	Interception, packet sr
Integrity	Multi-management domains, sharing identifications in cloud servers	Authentication from a
Availability	Compromised IoT sensors operating on cloud storing user data	Distributed denial-of-s
MEC server security	Physical security breaches, design flaws, configuration errors	DDoS Attacks, hijacki
Cloud virtualization security	Bot virtual machines created to drain out computational resources	Agent-based attacks, r
End-device security	Inject false values or information to systems	Injection attacks,comp

3.2 Blockchain-Based Solutions:

After the time period, the neighboring peers pack the transactions in a block mining is done by solving a difficulty based nonce called PoW. (22)

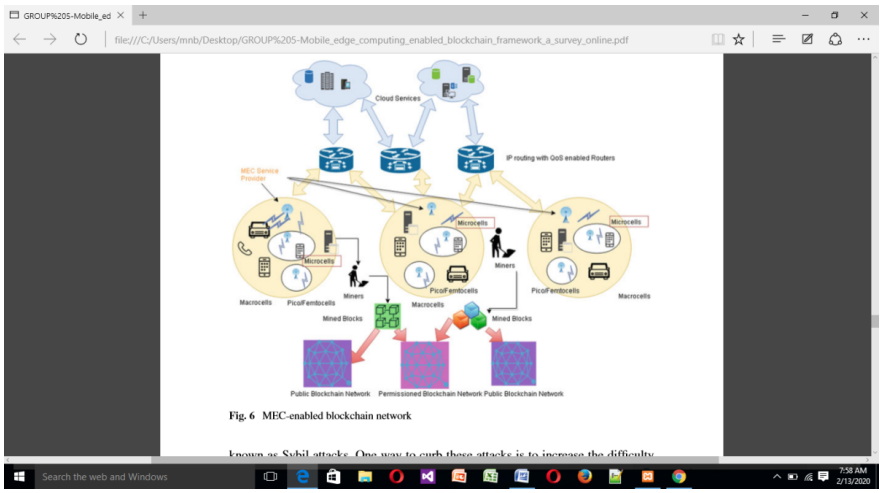

Fig. 6 MEC-enabled blockchain network

Designing Mining as a Service (MaaS) for Mobile Blockchain—Considering the requirementsforIoT-basedenvironments,authorsin[14]suggestedtheincorporation of many blockchain-based solutions that operate at low energy and lower communicationoverheads.SinceIoTdevicescombinemanylow-poweredsensorandactuator devices,exchangeofinformationovergeographicallydistributedenvironmentposes amajorchallenge.Further,thecomplexityoftheminingalgorithminlimitedenergy levels of the network becomes a challenging issue. (33)

4. Proposed Malware Detection Frameworks:

The role of miner nodes is to send a request for seeking computational power to the edge computing server, normally running the server version of blockchain API synchronized with the client-based API interface. (30)

The data recorded by the sensor nodes are first sent to the edge servers that will now run the client blockchain application, thus allowing the mining of nodes on edge servers, instead of sending data to cloud platforms.

(30)

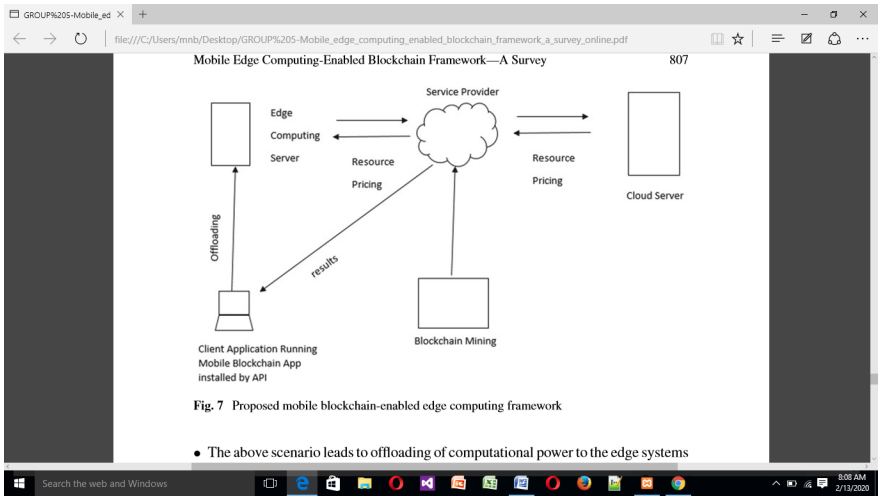

Fig. 7 Proposed mobile blockchain-enabled edge computing framework

In the above The resource-intensive PoW puzzles are solved by miners by taking resources from service provider; hence, the proposed architecture does not drain the limited energy or battery power of the mobile devices; thus, trust management is now added to the edge platform using blockchain network; and dually, the limited energy sources of the client node are also saved.

5 Conclusions and Future Work:

References:

[1] M. Ahmadi, K. Leach, R. Dougherty, S. Forrest, and W. Weimer, "Mimosa: Reducing malware analysis overhead with coverings," *arXiv preprint arXiv:2101.07328,* 2021.

[2] B. Namatherdhala, N. Mazher, and G. K. Sriram, "A COMPREHENSIVE OVERVIEW OF ARTIFICIAL INTELLIGENCE TENDS IN EDUCATION."

[3] B. Namatherdhala, N. Mazher, and G. K. Sriram, "ARTIFICIAL INTELLIGENCE TRENDS IN IOT INTRUSION DETECTION SYSTEM: A SYSTEMATIC MAPPING REVIEW."

[4] B. Namatherdhala, N. Mazher, and G. K. Sriram, "USES OF ARTIFICIAL INTELLIGENCE IN AUTONOMOUS DRIVING AND V2X COMMUNICATION."

[5] N. Mazher and I. Ashraf, "A Systematic Mapping Study on Cloud Computing Security," *International Journal of Computer Applications,* vol. 89, no. 16, pp. 6-9, 2014.