Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 4 (2023) 782 - 790 ISSN Media Electronic: 2580-0760

A Security Architecture for Mobile Computing-Based IoT

Farina Mutia[1], Eugene Ario Suradilaga[2], Raymond Giovadius[3]
[1,2,3]Department of Engineering and Information Technology, Master of Information Technology, Swiss German University
[1]farina.mutia@student.sgu.ac.id, [1]eugene.suradilaga@student.sgu.ac.id,[1]raymond.giovadius@student.sgu.ac.id

Abstract

The Internet of Things (IoT) is a complex technology with various applications that have become a vital part of our everyday life. The amount of Internet of Things and linked devices continues to rise. In terms of bandwidth, service availability, security controls, cyber-attacks and privacy problems, transporting the huge data created by these IoT devices to the cloud offers concern and challenges comprising of intermittent connection, service unavailability, data loss at rest, in use and in motion, unhardened device and server, unpatched device and server and exploitation vulnerabilities. Mobile computing (MC) is a strategic solution to tackle these difficulties by offering flexible data processing and storage to end users, increase security controls and with customized IoT devices for varied geographic locations. This paper is providing a complete description of the IoT architecture's components. After that, it elaborates on similar security threats and potential cyber-attacks in the context of mobile computing-based IoT and suggested solutions. In conclusion, we provide a secure mobile-computing-based architecture design for IoT applications.

Keywords: mobile computing; mobile computing – based IoT; internet of things (IoT); security architecture.

1. Introduction

IoT refers to the present connection of network architecture consisting of various physical devices/assets coupled with networked sensors/devices that are capable of creating, collecting, and transferring various data among themselves. As a consequence, an increasing number of sensors/devices/things are networked through IoT, and will produce massive amounts of data that need further processing and analytics to offer service providers and end users with insight. With traditional cloud-computing, all data must be sent/uploaded to a centralized server, and computation results must be sent back to the devices and sensors. This technique requires a large network bandwidth and costly data transmission fees [1].

A comparative analysis by M. Sarika, V. Kotak, and A. Durafe concluded that the majority of Internet of Things (IoT) devices continue to have basic limitations such as restricted memory space and battery life. To extend the battery life of a device, it is vital to balance power consumption by shifting energy-intensive computations to devices with more computational power and capabilities. Moreover, processing data at computer nodes placed near the end user will cut transmission time, hence saving energy use. In addition, network traffic influences the pace of data transmission in cloud-based services, and large network traffic results in lengthy transmission times, hence raising power consumption costs. This gives the benefit of a distributed computing architecture in a mobile computing and mobile machines may function in various places/locations using this design. The deployment of distributed computing nodes enables the offloading of traffic and computational demand from a centralized design and provides quicker response times for IoT applications and superior service quality compared to cloud computing. Lowering the total system latency and communication bandwidth consumption will enhance the overall system performance [2].

Furthermore, enhancing productivity by forcing workers to work efficiently and effectively from wherever they feel most comfortable. The Internet of Things can alter the productivity business. Otherwise, time would be wasted or spent traveling between places. In addition, it can access the most vital documents and information regardless of whether the channel or gateway of the computer system is guarded. In reality, growing telecommunications across numerous industries while avoiding wasteful expenditures. Locational flexibility and the versatility afforded by cellular computing is unique. This enables users to work from anywhere with an internet

Accepted: 18-02-2023 | Received in revised: 12-06-2023 | Published: 12-08-2023

connection. People operate concurrently without accessing fixed places. Mobility enables them to fulfil a variety of performance duties while conserving time on their principal work. Researchers will simply need to travel to their area to input data and feed it into the computer system, making research straightforward. This may also enable academics and field workers gather data from the field without generating undesired information [3].

Internet of Things (IoT) has gathered attentions in the industrial, technology and academic sectors, with IoT's potential serving as the primary purpose. This also guarantees a future in which all objects and technologies are linked and can interact with minimum human interaction. The ultimate objective of the Internet of Things is to enhance human existence by empowering all essential things in our surroundings to comprehend our every need and in our best interest without direct interactions [4].

As a consequence, the phrase "Internet of Things" lacks a general meaning; nonetheless, many studies have provided several definitions. Things have a virtual identity and personality, are integrated with smart-interfaces that promote interaction and link to the user's surroundings and social settings, and are able to converse and connect with one another [5]; This term is composed of two words: Internet is described as a worldwide network comprised of a highly diversified network that functions according to established communication protocols; meanwhile, the word "Thing" refers to any connected items through the same communications protocol (e.g. Internet) [6]; The IoT network environment is comprised of real and virtual objects, which become virtual when put in the virtual world. These objects are capable of sensing, analyzing, and processing data which are based on particular needs and integrated through communication protocols. These smart-objects/smart-things must have distinct virtual identities, as well as communicate through interoperable communication protocols [6].

A survey and research study by J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao presents mmong the technological components of contemporary ideas are sensor-based data collecting, data management, data processing, and the internet. It is essential to note that sensor-based hardware is used. This concept, according to its introductory and broad definition, is the widespread use of diverse objects or things for the example: sensors, actuators, RFID (Radio-Frequency Identification) tags and mobile phones, through a predetermined scheme, are able to interact with one another and work together to achieve common goals. [7]

Figure 1 is the three concepts related to IoT.

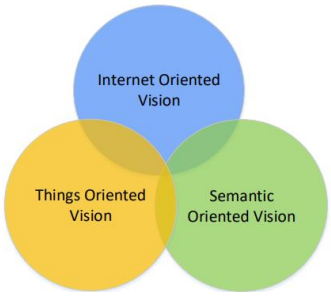

Figure 1. Three Vision Concepts [8]

The study of D.Singh defines Things Oriented Vision which contains references to sensors. It is essential to note that "things"-oriented long-term vision will rely on the sensor and its capabilities. Utilizing sensors and sensor-type embedded devices, users may collectively create vast volumes of data. Using sensor networks and RFID-based sensor networks, the RFI-based technological partnership will be administered. Utilizing embedded sensors and sensor-like devices, we may collectively create data. Future sensor networks will include RFID technology, sophisticated processing and sensing devices, and worldwide communication. This assertion is confirmed by the fact that sensors and expansive technologies such as RFID enable us to control anything [9].

Internet oriented vision. IP is the most used Internet protocol; consequently, the item must support IP. Real-time monitoring of sensor-based device or object attributes is possible. This is the foundation for embedded computing objects, which are microcomputers with computing capabilities.

The study of J. Franklin, G. Howell, V. Sritapan, M. Souppaya, and K. Scarfone defines IoT as Semantic oriented vision. The research was inspired by the thought that we would have a huge number of sensors and an abundance of data generated by these sensors. As a consequence, we will need to sort through a significant quantity of data, the most of which will be duplicates. Thus, it is vital to comprehend the raw data for a more accurate depiction and comprehension of the supplied information. In this instance, we will depend on technology to examine data, reducing interoperability issues associated with data interpretation [10].

2. Research Methods

The methodology use in this study is based on review of literatures. The result of analysis from the above-mentioned reviews are taken into considerations in developing the proposed model architecture based on suggested IoT architecture in relevant literatures[1], [11],

In Figure 2, it is explained step by step on the research methodology, we collect articles and read literatures

DOI: https://doi.org/10.29207/resti.v7i4.4950

related to IoT architectures and based on the type of current rising cyber-attacks and security threats, we identify relations, comparison and gaps (if any), to propose a secure IoT architecture for mobile computing [12].

Figure 2. Steps of Literature Review

In Table 1, the literature review from previous research is being presented includes the analysis of this study compares to previous research which covers main aspects of IoT security architecture. The comparative and gap analysis (include vulnerabilities) are indicated in Table 3, Table 4 and Table 5 as part of result.

A secure mobile computing (MC) has become an important trend in the improvement of both IT technology and business and industry. This has become a highlight in the IoT Industries [13].

2.1 Mobile Computing and other paradigms

This section focuses on mobile computing other computing paradigms. We compare mobile computing with other related computing paradigms.

Table 1. Literature Review (Previous Research)

Previous Research	Focus Orientation	Research Methodology	IoT Architecture	Security Assessment	Security Controls
A Survey of Security Architectures for Edge Computing-Based IoT(Fazeldehkordi and Groni) [1]	Security Architecture Design and Review	Survey and comparative analysis	Yes	No	No
A Review Paper on Internet of Things(IoT) and its Applications,(Sarika et all)[2]	IoT definition and paradigms	Comparative analysis	No	No	No
A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges (A.Riahi Sfar et all)[4]	IoT security analysis	Study case	No	Yes	Yes
Internet of Things (IoT) System Architecture and Technologies(A. El Hakim)[5]	IoT architecture diagram	Literature review	No	Yes	Yes
A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. (Lin et all)[7]	IoT security architecture and privacy controls	Survey and comparative analysis	Yes	No	No
The Internet of Things Vision: A Comprehensive Review of Architecture, Enabling Technologies, Adoption Challenges, Research Open Issues and Cntemporary Applications (Olanweraju et all)[8]	IoT architecture, technologies and applications	Literature review and comparative analysis	Yes	No	Yes
Vetting the Security of Mobile Applications (Ogata et all)[14]	Mobile security assessment and controls	Literature review and comparative analysis	No	Yes	Yes
Internet of Things Security (Samer)[15]	IoT security assessment and control	Literature review	No	No	Yes
Internet of Things: A Literature Review (Madakam et all)[16]	IoT definitions and technologies	Literature review	No	No	No
IoT Security Challenges and Issues (Muthuswarmy and Ganapathi)[17]	Literature review and comparative analysis	IoT security assessment and review	No	Yes	Yes
This Study	**IoT definition, literature review, security architecture, assessment and controls**	Literature review and comparative analysis	Yes	Yes	Yes

DOI: https://doi.org/10.29207/resti.v7i4.4950

Mobile Computing, being the most effective and convenient time-free communication tool, mobile devices (smartphones and tablet PCs) are becoming an ever-increasing element of human existence. Mobile apps, which operate on devices and/or distant servers across wireless networks, provide mobile users a comprehensive experience with a variety of services. The fast growth of mobile computing (MC) has become an important trend in the improvement of both IT technology and business and industry. In terms of their resources (such as battery life, storage, and bandwidth) and communication capabilities, mobile devices confront several obstacles (mobility and security). Insufficient resources significantly impede the enhancement of service quality.

Distributed computing design provides benefits to cellular computing. This design permits decentralized operation of mobile machines. Poor resource limits, communication delay the balance between autonomy and dependency (common to all distributed systems), and the necessity for mobile clients to adapt quickly to changing settings are disadvantages of cellular computing. Because to these limitations, cellular computing is less appropriate for applications with low latency or endurance requirements, although it is acceptable for data processing in certain geographic regions [18].

Fog computing is the process of decentralizing a computer infrastructure via the placement of nodes between the cloud and edge devices. This placed the data, storage and applications closer to the user/IoT devices where the data must be processed; as a result, a fog will be produced outside of the centralized cloud, lowering the needed data transmission times for data processing [19].

In contrast to traditional cloud computing, fog nodes are situated near to IoT source nodes, resulting in much decreased latency. With fog computing, node locations are not as centralized as cloud data centers. Fog nodes are separated geographically. With fog computing, security is accomplished at the edge or fog node locations, while in cloud computing, security methods are given at cloud data center locations [7].

Cloud computing has enhanced access and application possibilities for computer, storage, and network infrastructure[12]. The cloud offers infrastructure as a service, platform as a service, and software as a service [18]. Depending on the requirements of the application they are constructing, application developers might use the different services. The original goal of cloud computing was to provide users with access to computer resources for remote usage. While cloud computing has helped accomplish this objective, accessing cloud-based services may take a considerable amount of time, which is incompatible with some applications that requires low latency. The expansion in the number of connected devices and data generated requires the deployment of cloud resources close to the area where data is generated. Due to the increase need for high-bandwidth, low-latency, geographically locations, and sensitive data, computational models that might take place close to linked devices must satisfy the aforementioned characteristics [12].

Mobile cloud computing has provided access and application possibilities for mobile, processing, storage, and network infrastructure [12]. Based on the demands of the application they are building; application developers may take use of the available services. The original goal of mobile cloud computing was to provide users with access to computer resources wherever they were. Mobile cloud computing has achieved this objective, accessing cloud-based apps may take a considerable amount of time, which is incompatible with some mission-critical applications that need very low latency. The expansion in the number of connected devices and the amount of data generated at the network's edge necessitates the deployment of cloud resources close to the point where data is generated [1].

2.2 IoT Architecture

The network layer connects the network to servers, intelligent objects, and network devices. Its capabilities arealso used in.the transmission and processing of sensor data. The application layer is responsible for delivering applications services to end users. By clicking a button, a smart home application may, for instance, switch on a coffee machine [18].

The three-layer design demonstrates the core notion of the Internet of Things; however, it is not suited for IoT research since most IoT research focuses on the Internet of Things' finer components rather than the underlying concept. One of the designs is the five-layer architecture, which covers business and processing layers. The first through fifth levels are, in order, "perception," "transportation," "processing," "application," and "business." The perception and application layers operate similarly to the three levels of the architecture. As seen in Figure 3, the connections of the three- and five-layer design is explained in details [20].

The transport layer transports data resulted from sensors between the processing and.perception layers, using networks communications such as WIFI, Local Area Network, Bluetooth and others Processing are known as "middleware layers" since they.include.middleware functionality. In this layer, data/information are processed, managed, stored, and analysed by this connected layer. The business layer oversees the whole of the IoT system, including business, security controls, data privacy, and application management [21].

DOI: https://doi.org/10.29207/resti.v7i4.4950

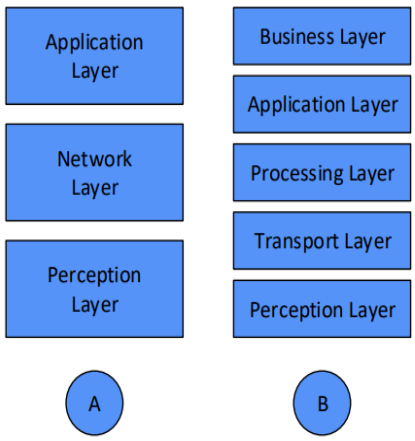

Figure 3. Three and Five Layers Architectures [7]

As demonstrated, the overall architecture of MC may be deduced from the notion of MC. In Figure 4, a base station creates and manages the connection and functional interface between the mobile device and the network. A mobile user's requests and data, for the example: ID and location are delivered to a central processor linked to a server that delivers mobile network services.

Based on the original agent and customer data maintained in the database, mobile network operators may offer authentication and authorization to mobile users. Thereafter, requests from clients are sent over the Internet. These services are produced in the cloud utilizing virtualization, and cloud architecture concepts for the example : web, application, and database servers[10].

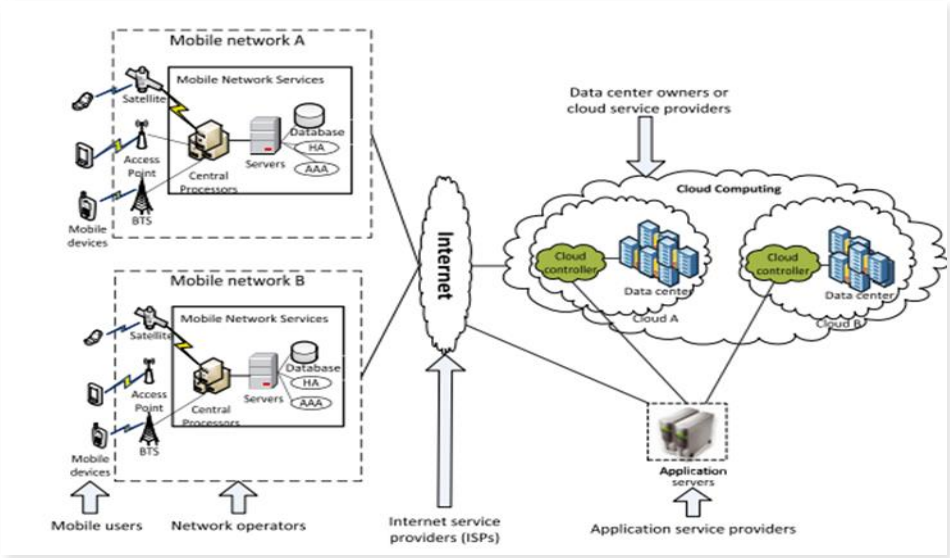

Figure 4. General Mobile Computing Architecture [12]

Mobile computing security threats in common mobile OS (e.g. Android and iOS). Google (Android) and Apple (iOS) offer closed environments that are secured and controlled, there are possibility of user exposed to cyber-attacks, some of the cyber-attacks are explained [21].

Phishing in a mobile app: Criminals might avoid app market source code inspections by building an app that operates as a browser window to a phishing website. These applications are designed in combination with the phishing website to offer the user with a smooth experience.

Crypto miner code: A huge rise in the number of apps including crypto miner code without the user's knowledge. The code ran regardless of whether the app was active and drained the phone's power constantly[14].

Advertising fraud: This is unexpectedly one of today's most profitable criminal businesses, and mobile applications seem to play a key part in this stealthy crime[22].

Malware: Smartphone capabilities are increasingly nearing personal computers, and cyber-attacks such as: extortion and theft of personal/company information is targeting mobile-users. Hackers are primed to strike, and there are a multitude of avenues via which malware may be disseminated; the Mobile Iron Report lists these and other malware concerns[23]. Android GMBot: Malware that tries to deceive users into giving their login information. Ace Deceiver iOS malware: Malware designed to steal an Apple ID. Marcher Android malware: Malware that masquerade as a bank website in an attempt to steal users' login information. Backdoor families: Trojanized programs distributed through the Google Play Store and concealed inside other sorts of applications. Mobile miners are applications distributed by spam e-mail or SMS that use the computing power of mobile smartphones. Fake programs: A genre of malicious apps that imitates popular and helpful applications and, once installed,

DOI: https://doi.org/10.29207/resti.v7i4.4950

requires mobile verification or refers the user to a URL with instructions.

3. Results and Discussions

3.1 Result

Based on the computing paradigms, please find the result of comparative analysis of a security architecture for IoT computing. Table 2 explained the comparison between IoT computing paradigms and the gap and issues found on each computing approach. This study selected mobile computing based because it is providing a more secure environment and an end to end security control implementation to prevent potential cyber-attacks[21].

Table 2. Comparative Analysis of IoT Computing Paradigms

Computing	Edge	Fog	Mobile-Cloud /	Mobile (This Study)
Nodes Location	Close	Remote-based	Remote-based	Close
Scope	Endpoints via LAN	Fog devices	Cloud data-centre	Endpoints via LAN
Application	Less resource	High resource	High resource	Less resource
Processing	Edge-computing	Fog devices	Cloud computing	Edge-computing via API
Data Collection	Same device	Not same device	Not same device	Same device
Mobile Access	No	No	Yes	Yes
Security Controls	More secure and implemented end to end	Depending on fog devices and cloud provider	Depending on cloud provider	More secure and implemented end to end

Based on the assessment of mobile security computing threats, please find below security countermeasures for mobile computing based IoT:

Application Design: security controls should be enforced on the respective application services (server). Application service (server) should verify that connecting clients uses an up-to-date version of the mobile app. The solution should support configuration to allow/disallow functions to be made available on the mobile platform. E.g. certain sensitive data or functions should only be accessible via Web Portal.

User Authentication and Session Management: authentication should be performed by the application service (server) prior to granting access to the service. Authentication should be performed by the application service (server) without sending users' authentication credentials to the mobile app. The application service (server) should terminate the existing session when the user logs out or the session idle timeout after a pre-defined period of time.

If platform biometric authentication (e.g. Touch-ID, Face-ID etc.) is supported, please describe how it is implemented (e.g. are there any logon credentials stored on device to facilitate the authentication). Biometric authentication, if any, is not event-bound (i.e. using an API that simply returns "true" or "false"). If the mobile application supports a locally authentication application access password, for access to the mobile application, please describe the mechanism and include information on how the password is secured on the device.

Secure Coding, Code Quality and Build Setting: the mobile app should be signed and provisioned with valid certificates. The mobile app should be released with settings appropriate for release build (e.g. non-debuggable etc.). Debugging symbols should be removed from native binaries i.e. Symbol stripping options should be enabled when the mobile app is compiled for release. Debugging code should be removed. The mobile app should always catch and handles all possible exceptions. Error handling logic in security controls implemented in the mobile app should deny access by default. Security features or runtime protection offered by the compiler should be activated

Resiliency Against Reverse Engineering: The mobile app should provide a secure keyboard (or keypad) whenever sensitive data (e.g. Personally Identifiable Information/PII etc.) is entered. The mobile app should detect and disallow the use 3rd party keyboards whenever sensitive data are entered.

The mobile app should detect the presence of widely used reverse engineering tools, for the example code injection tools, hooking-frameworks, code tampering and debugging-servers. The mobile app should detect and responds to, tampering of executable files and critical data. Code obfuscation should be implemented on the mobile app.

In the result of assessment of security countermeasures, we included the security controls in the security architecture. As shown below in Figure 5, the architecture is segregated into three layers comprising of the IoT layer, the server layer, and the mobile layer, with additional controls and network segregations. This architecture also addressed the potential cyber-attacks for mobile computing and implement security countermeasures.

Figure 5 shows the segregation layers. IoT layer consists of devices, terminals and smart machines that monitor the functioning of services, activities, or devices. It also includes IoT sensors, IoT actuators, IoT controllers and gateways for IoT configurations, allowing the storage and management for IoT devices.

DOI: https://doi.org/10.29207/resti.v7i4.4950

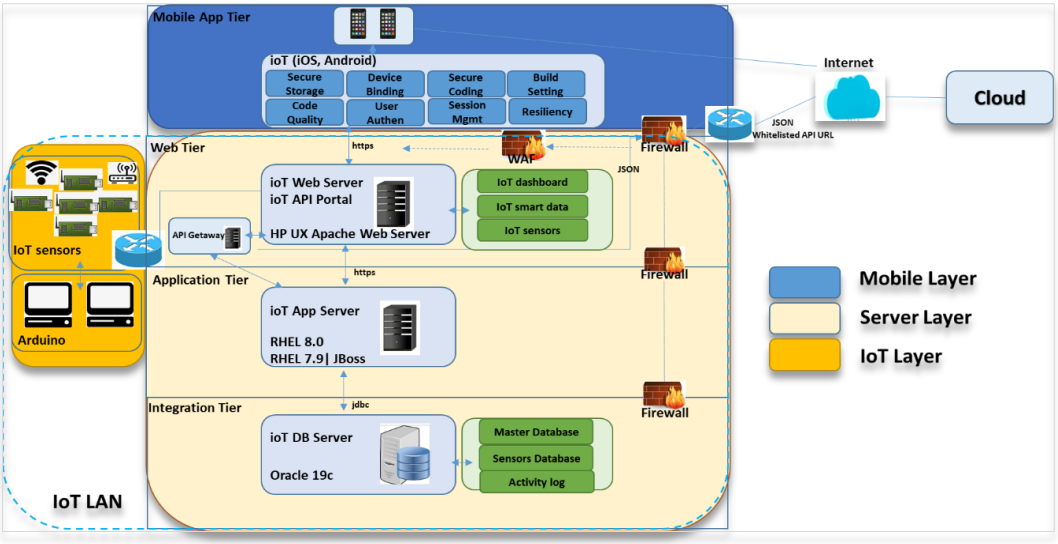

Figure 5. Security Architecture for Mobile Computing Based IoT

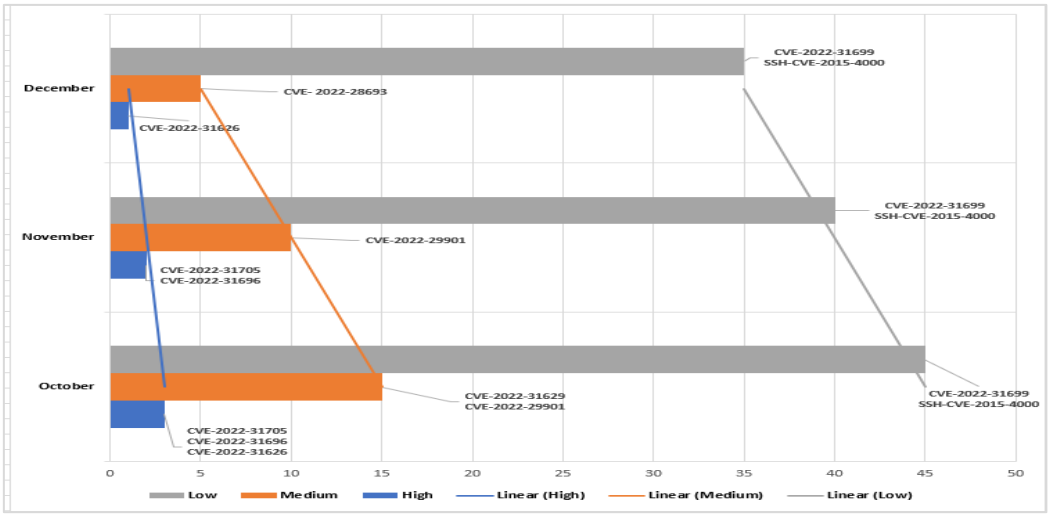

Figure 6. Vulnerability Assessment Result

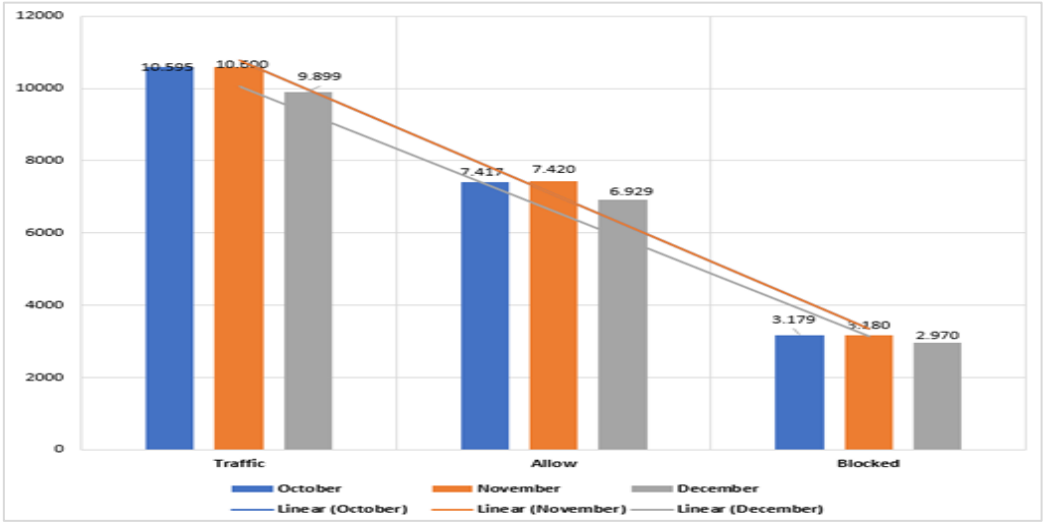

Figure 7. IPS Traffic Result

DOI: https://doi.org/10.29207/resti.v7i4.4950

Server layer is the core of IoT architecture consisted of servers (web, application and database) and responsible for processing, and transmitting IoT layer data flow. In addition to server security and privacy protection, the server layer also provides cognitive computing and data analysis.

Mobile layer is the foundation of the mobile computing based IoT architecture and responsible for receiving and processing data flow from the server layer to the mobile. In addition, the mobile layer offers services with time-constraints for the example: mobile security and secure coding, secure intelligent dashboard, real-time follow-up activities, data analysis and real-time control. In the IoT and server layer, hostnames are scanned and analyzed to ensure the security controls implementation and network segregations. In Table 3, it shows the servers zone location in the architecture and status of the scanning.

Table 3. Supporting Servers

Hostname	Operating System	Location	Result Scan
VEAXPID055	RHEL 8	Web-Zone	Success
VEAXPID053	RHEL 8	Web-Zone	Success
VEAXPID012	RHEL 8	Web-Zone	Success
VEAXPID057	RHEL 8	App-Zone	Success
VEAXRID111	RHEL 8	App-zone	Success
VEAXRID112	RHEL 7.9	App-Zone	Success
VEAXRID113	RHEL 7.9	Integration-Zone	Success
VEAXPID013	RHEL 8	Integration-Zone	Success
VEAXPID011	RHEL 8	Integration-Zone	Success
VEAXPID083	RHEL 7.9	Integration-Zone	Success
VEAXPID045	RHEL 8	App-Zone	Success
VEAXPID081	RHEL 7.9	IoT-Zone	Success
VEAXPID0J1	RHEL 8	IoT-Zone	Success
VEBXPID057	RHEL 8	Web-Zone DR	Success
VEBXRID111	RHEL 8	Web-zone DR	Success
VEBXRID112	RHEL 7.9	Web-Zone DR	Success
VEBXPID113	RHEL 8	App-Zone DR	Success
VEBXRID114	RHEL 8	App-zone DR	Success
VEBXRID115	RHEL 7.9	App-Zone DR	Success
VEBXPID116	RHEL 8	Integration-Zone DR	Success
VEBXRID117	RHEL 8	Integration-Zone DR	Success
VEBXPID118	RHEL 8	Integration-Zone DR	Success
VEBXRID119	RHEL 8	App-zone DR	Success
VEBXRID120	RHEL 7.9	IoT-Zone DR	Success
VEBXPID05X	RHEL 8	IoT-Zone DR	Success

Vulnerability Assessment (VA) is conducted in the security architecture to ensure the security controls are being implemented effectively and to identify the security vulnerabilities. Figure 6 shows the VA result with less high issues and the decreasing vulnerabilities with the cycle of patching conducted in monthly basis.

In the VA result, the details of vulnerabilities are explained in the Table 4. Table 4 shows the CVSSv3 score and rating. The CVSSv3 rating has been assessed based on the criticality of IT asset (e.g. servers).

From the CVE found, we can identify the vulnerability ID and suggestion for vulnerabilities remediation, please refer to Table 5 for the details.

Table 4. Vulnerabilities found in the VA scanning

CVE	CVSSv3 Score	CVSSv3 Rating
CVE-2022-31705	8.2	HIGH
CVE-2022-31696	8.8	HIGH
CVE-2022-31626	8.8	HIGH
CVE-2022-31629	6.5	MEDIUM
CVE-2022-29901	6.5	MEDIUM
CVE-2022-31699	3.3	LOW
CVE-2015-4000	3.7	LOW
CVE-2011-3561	1.8	INFORMATIONAL
CVE-2008-3259	1.2	INFORMATIONAL

Table 5. Vulnerability ID and Remediation

CVE	Vulnerability ID	Remediation
CVE-2022-31705	VMSA-2022-0033	Patch VMWare
CVE-2022-31696	VMSA-2022-0030	Patch VMWare
CVE-2022-31626	PHP Vulnerability	Upgrade version
CVE-2022-31629	PHP Vulnerability	Upgrade version
CVE-2022-29901	VMSA-2022-0020	Patch OS Version
CVE-2022-31699	VMSA-2022-0030	Patch OS Version
CVE-2015-4000	SSH Server	Use TLS 1.3
CVE-2011-3561	jre package	Upgrade version
CVE-2008-3259	OpenSSH	Use TLS 1.3

In addition, we performed traffic analysis in the Intrusion Prevention System (IPS) to ensure the security architecture is able to block and filter traffic. In Figure 7, its shown that decrease number of intrusion attempts.

3.2 Discussion

This study is focusing on the security controls on mobile computing based IoT focusing on secure coding, user authentication, session management, code quality, resiliency over reverse engineering with security technique implementation and application design. This study is limited to security controls over server and IoT layers. This section discusses open issues and possible research directions in the development of mobile computing based IoT:

Network Access Control: in addition to enhance link performance for mobile users, an efficient network access management optimizes bandwidth utilization. Cognitive radio is anticipated to be a solution for wireless access management in mobile communication environments.

Network Service: when requesting cloud-based services and resources, mobile users must be able to connect to cloud-based servers. Despite this, mobile users may encounter issues such as network congestion, network disconnection, and signal attenuation due to their mobility.

Interface: when mobile users must interact and communicate with the cloud, interoperability becomes a significant concern. Web interface is used between mobile users and the cloud. However, web interfaces may not be the secure option.

DOI: https://doi.org/10.29207/resti.v7i4.4950

4. Conclusions

With this study, we have provided an overview of IoT architecture with a mobile computing approach and its relationship to other similar computing paradigms, including fog computing, cloud computing, and others. We also explained the major security concern and potential cyber-attacks in mobile computing-based IoT, along with the countermeasures and solutions applicable to these attacks.

Then, based on relevant study accomplishments, we proposed a secure architecture for IoT infrastructure and several open issues that need to be addressed. The proposed design has considerable room for improvement.

Future research may concentrate on development of other concepts format with addressing the issues mentioned in the previous section. This study is beneficial to increase security controls and address potential cyber-attacks by implementing secure design and countermeasures in terms of developing mobile computing based IoT.

References

[1] E. Fazeldehkordi and T.-M. Grønli, "A Survey of Security Architectures for Edge Computing-Based IoT," *IoT*, vol. 3, no. 3, Art. no. 3, Sep. 2022, doi: 10.3390/iot3030019.

[2] M. Sarika, V. Kotak, and A. Durafe, "A Review Paper on Internet of Things(IoT) and its Applications," p. 1623, Jun. 2019.

[3] "Advantages of Mobile Computing | Enhance Grade Level High," Jul. 20, 2020. https://elysiumpro.in/advantages-of-mobile-computing/ (accessed Nov. 06, 2022).

[4] A. Riahi Sfar, Z. Chtourou, and Y. Challal, *A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges*. 2017, p. 105. doi: 10.1109/SM2C.2017.8071828.

[5] A. El Hakim, *Internet of Things (IoT) System Architecture and Technologies, White Paper*. 2018. doi: 10.13140/RG.2.2.17046.19521.

[6] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap," *IEEE Access*, vol. PP, pp. 1–1, Dec. 2020, doi: 10.1109/ACCESS.2020.3047895.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. PP, pp. 1–1, Mar. 2017, doi: 10.1109/JIOT.2017.2683200.

[8] R. Olanrewaju, B. Khan, A. Hashim, K. Sidek, Z. Khan, and H. Daniyal, "The Internet of Things Vision: A Comprehensive Review of Architecture, Enabling Technologies, Adoption Challenges, Research Open Issues and Contemporary Applications," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 26, pp. 51–77, Mar. 2022, doi: 10.37934/araset.26.1.5177.

[9] D. Singh, *Developing an Architecture: Scalability, Mobility, Control, and Isolation on Future Internet Services*. 2013. doi: 10.1109/ICACCI.2013.6637467.

[10] J. Franklin, G. Howell, V. Sritapan, M. Souppaya, and K. Scarfone, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," National Institute of Standards and Technology, NIST Special Publication (SP) 800-124 Rev. 2 (Draft), Mar. 2020. doi: 10.6028/NIST.SP.800-124r2-draft.

[11] F. Ganz, D. Puschmann, P. Barnaghi, and F. Carrez, "A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things," *IEEE Internet Things J.*, vol. 2, pp. 1–1, Aug. 2015, doi: 10.1109/JIOT.2015.2411227.

[12] A. Kamilaris and A. Pitsillides, "Mobile Phone Computing and the Internet of Things: A Survey," *IEEE Internet Things J.*, vol. 3, pp. 1–1, Dec. 2016, doi: 10.1109/JIOT.2016.2600569.

[13] P. Dalal, G. Aggarwal, and S. Tejasvee, "Internet of Things (IoT) in Healthcare System: IA3 (Idea, Architecture, Advantages and Applications)." Rochester, NY, Apr. 01, 2020. doi: 10.2139/ssrn.3566282.

[14] M. Ogata, J. Franklin, J. Voas, V. Sritapan, and S. Quirolgico, "Vetting the Security of Mobile Applications," National Institute of Standards and Technology, NIST Special Publication (SP) 800-163 Rev. 1, Apr. 2019. doi: 10.6028/NIST.SP.800-163r1.

[15] A. Sameer, "Internet of Things (IoT) Security," Sep. 13, 2020. doi: 10.1109/NTICT.2020.P20.

[16] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *J. Comput. Commun.*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.

[17] S. Muthuswamy and P. Ganapathi, "IOT Security Challenges and Issues – An Overview," Feb. 2016.

[18] A. Sallow and H. Shaikha, "Mobile Cloud Computing: A Review," Feb. 2019.

[19] A. Yousefpour *et al.*, "All One Needs to Know about Fog Computing and Related Edge Computing Paradigms," *J. Syst. Archit.*, vol. 98, Feb. 2019, doi: 10.1016/j.sysarc.2019.02.009.

[20] M. J. McGrath and C. N. Scanaill, "Key Sensor Technology Components: Hardware and Software Overview," in *Sensor Technologies: Healthcare, Wellness, and Environmental Applications*, M. J. McGrath and C. N. Scanaill, Eds., Berkeley, CA: Apress, 2013, pp. 51–77. doi: 10.1007/978-1-4302-6014-1_3.

[21] P. Weichbroth and Ł. Łysik, "Mobile Security: Threats and Best Practices," *Mob. Inf. Syst.*, vol. 2020, p. e8828078, Dec. 2020, doi: 10.1155/2020/8828078.

[22] M. Tripathi, J. Gajrani, and V. Jain, "Mobile Security: Attacks and Prevention - Security in Mobile Communication," 2017, pp. 43–59. doi: 10.4018/978-1-5225-2342-0.ch003.

[23] C. Forrest, "New MobileIron report details most common mobile threats and blacklisted apps," *TechRepublic*, Aug. 02, 2016. https://www.techrepublic.com/article/new-mobileiron-report-details-most-common-mobile-threats-and-blacklisted-apps/ (accessed Nov. 06, 2022).

DOI: https://doi.org/10.29207/resti.v7i4.4950