MAAMSIC: Multimodal Authentication and Authorization Model for Security of IoT Communication via GSM Messaging in Sub-Saharan Africa

Joan Nabusoba[1], Calvins Otieno[2] and Wilson Cheruiyot[3]

[1] Jomo Kenyatta University of Agriculture and Technology, P.O. Box 81310-80100, Mombasa
Kenya

- Publication link: https://link.springer.com/chapter/10.1007/978-3-030-73689-7_86
- Journal Details: Proceedings published by:
  - Advances in Intelligent Systems and Computing, which is now indexed by ISI Proceedings, DBLP. Ulrich's, EI-Compendex, SCOPUS, Zentralblatt Math, MetaPress, Springerlink.

Abstract. Internet of Things (IoT) which consists of heterogeneous devices is an enabling technology that can greatly improve the quality of lives in Sub-Saharan Africa. For instance, soil humidity and irrigation for e-agriculture, energy consumption, or even health data. As with technology, however, IoT has introduced security and privacy challenges. IoT devices create, transfer, process, and store sensitive data that must be protected from unauthorized access. Similarly, the devices and infrastructure linking with IoT and the IoT devices themselves are assets that must be protected. Though IoT devices are being adopted, there isn't wide access to GPRS In rural parts of Africa; hence users need to have access to technology that is seamless, viable, and easy to use. This paper introduces a Multimodal Authentication and Authorization Model for the Security of IoT Communication via GSM Messaging (MAAMSIC). The MAAMSIC introduces a secure server that will encrypt devices' data and the AT Commands from the IoT. The model is illustrated with a case study of a soil and moisture control system. The system will have a secure server to store data and send feedback to the user in case of any anomalies, as a way of fast mitigation. The system will also provide the availability of both Internet phones and simple phones that don't use the internet. To ensure that third-party apps don't read data from the smartphone, it will have an app to send commands, and the data will be encrypted with JSON Web Encryption.

Keywords: Internet of Things, GSM, JSON Web Encryption.

1. Introduction

Internet of things (IoT) is a new paradigm that relies on widely spread connected objects that cooperate to automate many everyday actions (Rak, Salzillo & Romeo, 2020). Innovations in IoT are improving lives in rural Africa. For example, to solve water problems, Ingram & Memon (2020) are utilizing IoT technology to scale water supply systems in sub-Saharan Africa for sustainable water supply.

According to BRCK, about 800 million Africans do not have internet access making internet coverage, especially in rural areas, low (brck.com). As much as the acquisition of phones is growing in Africa, smartphone adoption is modest. Common types of mobile devices owned are basic phones. Worldwide, sub-Saharan Africans report the lowest ownership rate of smartphones compared to any other geographic region. Additionally according to M-Kopa (https://m-kopa.com/impact/), one of the leading solar home system states that 75% of sub-Saharan Africa remains unconnected to the internet. Sending IoT data can use general packet radio service (GPRS), which is an advancement of GSM. However, since GPRS is not dedicated for transmission of IoT data due to weaknesses in power efficiency and coverage, GSM is preferred (Bima, Suryani & Wardana, 2020).

There is explosive development of IoT, spurring a massive demand for many smart devices to access the wireless networks concurrently (Priyanka et al., 2020). It is predicted that over 20 billion devices will connect to wireless internet by the end of 2020 (Xu, Hu & Li, 2020).

In addition to low network coverage, half of Sub-Saharan Africa does not have access to electricity, which consequently hampers GPRS equipment (Bakibinga-Gaswaga et al., 2020). The latter highlights how unstable GPRS is as a choice of IoT infrastructure, affecting its adoption.

Owuor, Laurent & Orero (2020) state that there is rapid increase in IoT applications in almost every area of our society. However, according to Franklin (2020), these increases of IoT startups fail to profit from their IoT innovations. This is due to security related problems during IoT development, which are often underestimated or overlooked (Selgert, 2020). Even with inadequate coverage of the internet in rural parts of Africa, smart farming innovations are still being implemented using IoT and wireless devices (Olivera-Jr et al., 2020).

The use of technology still presents security issues to the African continent. Despite network coverage challenges, Ndubueze (2020) suggested that the number of cybercrime and victimization incidents is on the rise. However, the African continent has been slow in responding to crime and disorder in cyberspace and is still establishing cybercrime legislations. Hence, this makes Africans vulnerable in cyberspace, without the assailants facing the consequences, since there isn't proper establishment and enforcement of cyber legislations (Ndubueze, 2020).

The objective of this paper was to construct a multimodal technique for securely sending and receiving data from IoT systems using GSM in sub-Saharan Africa (MAAMSIC).

We run exhaustive experiments using both real and simulated data to evaluate whether the MAAMSIC can send and receive data securely. The experimental analysis shows that MAAMSIC is capable of sending and receiving data from verified users to the IoT, and rejecting and flagging unverified users for further action.

The paper is organized as follows: related work, requirement and system design, evaluation, conclusions, and further work.

2. Related Work

Recently, Waghmare et al., (2020) integrated IoT and GSM with a transformer to monitor and protect it. Their system uses a microcontroller and is monitored using GSM technology. The microcontroller gets initialized, and C code is compiled and uploaded to the Arduino board from a USB port. The transformer values are then compared and checked against the preset values that are fed in the Arduino. Examples of these values include voltage where, if an overvoltage occurs, its relay starts to operate. Its values are displayed on an LCD screen, and messaging is done using GSM technology. In the presence of any abnormality, transformer details are updated on a webpage, and an alert text message is sent. Although the system utilizes a GSM communication network with low investment and operation costs, no data protection or security of the transformer is proposed. If any, it is undisclosed.

Antonio et al., (2020) propose an IoT platform for the benefit of rural African farmers. The platform has an IoT sensing platform that provides the state of the soil information like moisture, light, air temperature, color, and texture. The system's hardware is housed in a specially designed casing for easy assemblage and protection, deployment, and transport. While the solution targets rural farmers, there isn't any security of data implemented to ensure that the user data is not acquired maliciously.

Sigu et al., (2020), in collaboration with the International Cancer Institute, are utilizing IoT to support oncology clinics in the rural areas of Kenya. Cancer patients get the information needed from the physician without going to the clinic facilities. Patients are monitored, and access information in real-time reduces costs and improves the patient outcome of treatment. Patients are also trained through an online module. Remote monitoring is beneficial to prevent lengthy hospital durations and readmissions. The use of technology has proved to have a significant impact on cancer patients in rural sub-Saharan Africa. The application of this technology, however, lays minimum emphasis on the security of sensitive data of patients. No frameworks or information about how the patients' data security has been mentioned.

With the era of the use of informational renovation to enhance performance in water pipelines, Priyanca et al., (2020) proposed integration of Internet of Things to monitor pressure, viscosity, pumping station parameters and other external parameters. The paper shows how the Internet of Things has progressed the industrial element of monitoring and intellectual control of the pipeline systems. The IoT system proposed is a smart module to enhance efficient data communication. The system module however, isn't clear on its security of its data, if any.

3. System Architecture

The system comprises three major modules:

An IoT sensing platform with a soil moisture sensor detects the moisture content and sends signals to initialize crops' irrigation. Signals from the device are sent through the GSM network. A water level sensor is added to monitor the amount of water in the irrigation tank. The water level sensor is connected to the server. This is to ensure that users can make requests through their phones to monitor the water level through the SMS Gateway.

The server software is written in PHP and hosted on a server. The server will be connected to an SMS gateway provider to receive messages from the device and communicate it to the user. The server will ensure that the user is registered and has a verified phone number and device before sending and receiving commands. The server also ensures that users are authenticated, and messages are sent and received securely. Additionally, to mitigate issues arising, the server will notify the user if the device is offline. Since the users' phone numbers are verified and linked to a specific device ID that only the server knows, SIM card replacement fraud and impersonation are restricted.

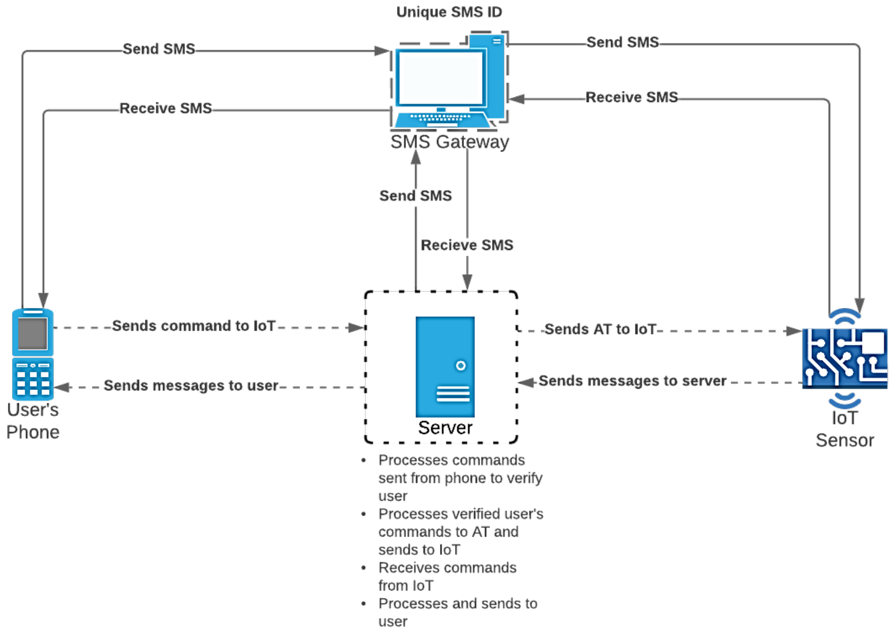

Fig.1. MAAMSIC architecture

The users are connected to the device via the server through their verified mobile phones. They can join either via smartphones or the simple phones that do not have any access to the internet. For smartphones, the user uses a Flutter app whose data is encrypted with JSON Web Token (JWT) and JSON Web Encryption (JWE) to prevent third-party apps from reading user information. For simple phones, the user will send SMS to a specific SMS code, which will concurrently send commands to the server. The server then verifies the user and relays the command to the device. The server also sends feedback to the user from the device.

3.1. Server App

The server consists of a database module that stores data on user details and device details. It has a web app that comprises five main modules: Authentication, Message Processing Module, SMS Gateway, and IoT connector module.

The Authentication Module ensures that the user is registered and verified; their phone numbers that will be \used to send SMS through commands are verified and are linked to the device(s) ID. When a user sends a message, the Authentication Module immediately checks whether the user is verified and connected to a device or devices. The Authentication Module sends a letter to the user in case there is a malicious attempt to send commands to their device. These attempts are also saved in a server with a list of these issues.

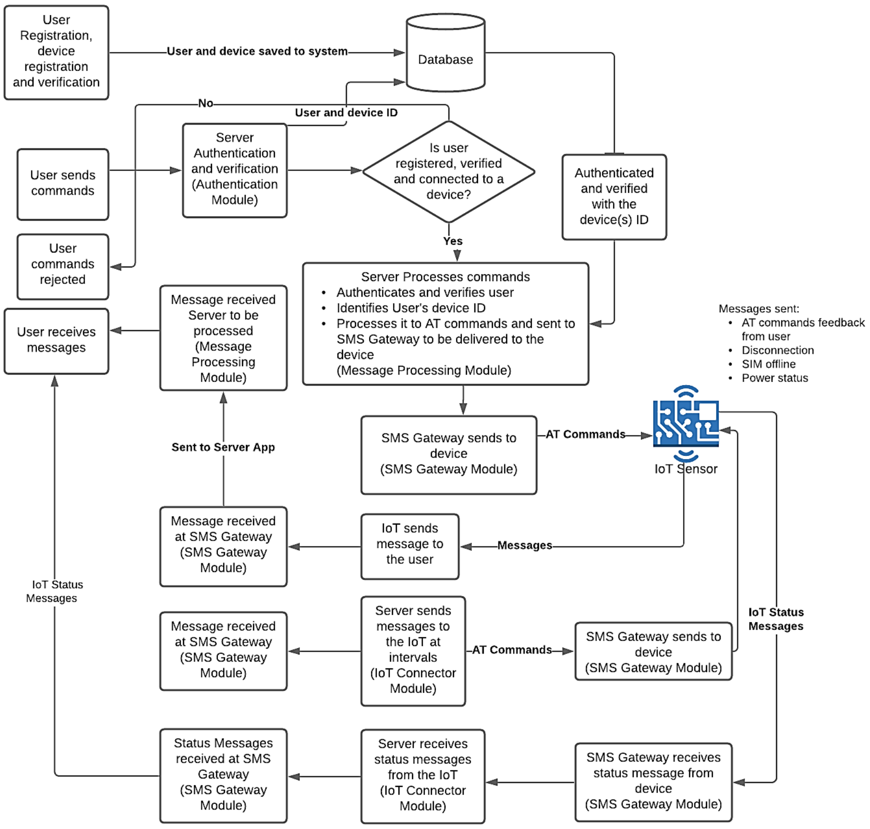
User Registration, device registration and verification
User and device saved to system
Database
No
User and device ID
User sends commands
Server Authentication and verification (Authentication Module)
Is user registered, verified and connected to a device?
Authenticated and verified with the device(s) ID
Yes
User commands rejected
User receives messages
Message received Server to be processed (Message Processing Module)
Server Processes commands
• Authenticates and verifies user
• Identifies User's device ID
• Processes it to AT commands and sent to SMS Gateway to be delivered to the device
(Message Processing Module)
Messages sent:
• AT commands feedback from user
• Disconnection
• SIM offline
• Power status
SMS Gateway sends to device (SMS Gateway Module)
AT Commands
IoT Sensor
Sent to Server App
Message received at SMS Gateway (SMS Gateway Module)
IoT sends message to the user
Messages
IoT Status Messages
Message received at SMS Gateway (SMS Gateway Module)
Server sends messages to the IoT at intervals (IoT Connector Module)
AT Commands
SMS Gateway sends to device (SMS Gateway Module)
IoT Status Messages
Status Messages received at SMS Gateway (SMS Gateway Module)
Server receives status messages from the IoT (IoT Connector Module)
SMS Gateway receives status message from device (SMS Gateway Module)

Fig.2. Software architecture block diagram

The Message Processing Module handles received and sent messages. When a user sends a command to the device, it is verified through the auth server. After successful verification, their message is processed into an AT command and sent to the device through the SMS Gateway Module. When an IoT sends feedback or information to the user, the message is sent via SMS to the Message Processing Module through the SMS Gateway. The message is processed and the user connected to the device identified. The Message Processing Module then sends a feedback SMS to the user through the SMS Gateway.

SMS Gateway Module is the one that sends and receives messages which are first processed in the server. When the user sends a message to the device, the SMS Gateway sends the message to the server for verification at the authentication module. After verification and processing, the SMS Gateway sends the message to the device's SIM card in the form of AT commands. The message from the device is first received by the SMS Gateway, and then sent to the Message Processing Module. The device sending the message is identified with the user connected to the device. The Message Processing Module then sends a feedback message to the user through the SMS Gateway.

The IoT Connector Module sends several messages to the IoT through the SMS Gateway to ensure that it is online and check its status. Messages are sent in intervals. A user can also check this to ensure that the device is online. The moment the IoT Connector module doesn't receive a message from the device, a message is sent to the user, and the issue logged in the system. All this data is stored in the database for querying and retrieval.

3.2. Hardware

The soil moisture control system's hardware for irrigation consists of a GSM Arduino board, soil moisture sensor, and water level sensor. The board is programmed to send commands to the server and receive commands from the soil moisture sensor. The GSM chip is interfaced with the hardware. The chip is used to send and receive messages to control the system. The AT commands are sent and acquired through the GSM chip. A soil moisture sensor is used to detect the moisture content, which correspondingly sends SMS to the SMS gateway which is later on relayed to the user via the server. A water level sensor is used to indicate the amount of water left in the irrigation tank, and a 240V AC power supply drives the hardware.

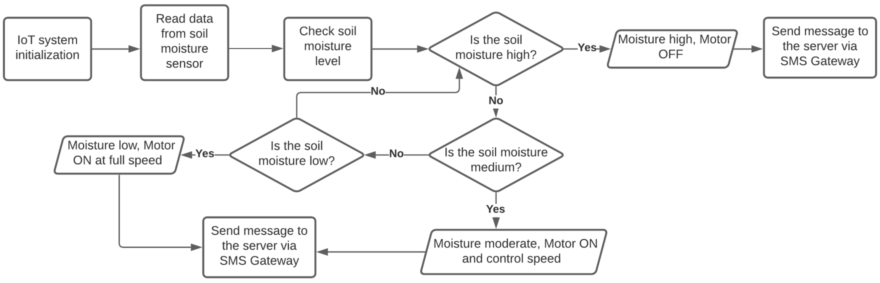
IoT system initialization
Read data from soil moisture sensor
Check soil moisture level
Is the soil moisture high?
Yes
Moisture high, Motor OFF
Send message to the server via SMS Gateway
No
No
Is the soil moisture medium?
No
Is the soil moisture low?
Yes
Moisture low, Motor ON at full speed
Yes
Moisture moderate, Motor ON and control speed
Send message to the server via SMS Gateway

Fig.3. Hardware architecture

3.3. Software Implementation

Server

The server is written in the HyperText Preprocessor (PHP) framework called Yii. It is hosted in a secured and shared hosting for demonstration. The server uses an SMS gateway provider to send and receive SMS through a short code. The server has a user registration module where the user is registered and authenticated to ensure data integrity. After the user is registered, the details are added to the server, including their device(s) SIM card number and ID. They further verify their phone number via a token sent to them through a short URL to activate their account. The IoT device has a GSM chip with SIM card, and this information will be stored in the server. The admin then assigns the device to a verified user in the server, and the user can proceed to send commands and receive information from the device through the server.

When a server receives an SMS or a command from a specific phone number, the server will know the device ID associated with that user. The server then sends the message to the device. Moreover, when the device sends the message back to the server, the server will identify the user who owns the device and send it.

Mobile Application and Encryption

The user can install the mobile application to send and receive commands from the device through the server. This is for the case of those who own smartphones. The smartphone app is developed with Flutter and data is encrypted by JSON Web Token (JWT) and JSON Web Encryption (JWE). JWT and JWE technology is needed in the authentication process and access rights security (Royani & Wibowo, 2020). A user sends an encrypted message to the server, which decrypts it into a command that is sent to the IoT through the SMS gateway. Responses are sent back to the mobile application through the authentication and authorization module, which encrypts the message using JWE. The mobile app, upon verification of the source of the message, decrypts the message and displays to the user. Data, which cannot be decrypted, is rejected by the receiving party.

4. Evaluation

MAAMSIC is evaluated by testing the mobile app and the IoT server. The mobile application has two login systems to emulate the MAAMSIC architecture and the phishing app. Both the modules have the SMS sent and received from the IoT. The user can send and receive SMS from the IoT through the server. The MAAMSIC application has a list of commands a user can directly send to the emulated IoT to control and operate it and control the moisture by turning the motor off or controlling the speed. The user can check the status of the IoT as well.

Table 1. Performance of Basic MAAMSIC operations.

Request	Time	Phone subjects	Response
Get IoT Status (ON/OFF)	7.63	Registered phone	Command accepted. IoT status connected
	7.89	Unregistered phone 1	Command rejected, unidentified
	7.89	Unregistered phone 2	Command rejected, unidentified
	7.89	Unregistered phone 3	Command rejected, unidentified
Turn on motor	8.32	Registered phone	Command accepted, motor ON
	8.96	Unregistered phone 1	Command rejected, unidentified
	8.96	Unregistered phone 2	Command rejected, unidentified
	8.96	Unregistered phone 3	Command rejected, unidentified
Turn off motor	8.92	Registered phone	Command accepted, motor OFF
	9.01	Unregistered phone 1	Command rejected, unidentified
	9.01	Unregistered phone 2	Command rejected, unidentified
	9.01	Unregistered phone 3	Command rejected, unidentified
Control motor	8.60	Registered phone	Command accepted speed in-
	8.89	Unregistered phone 1	Command rejected, unidentified
	8.89	Unregistered phone 2	Command rejected, unidentified
	8.89	Unregistered phone 3	Command rejected, unidentified

User's requests are issued on both registered and unregistered phone numbers to access the IoT device by sending messages. The messages sent are received by the server app which consists of authentication, message processing, SMS gateway and IoT connector modules. If a user is using a simple phone without GPRS, the phone number is processed to check whether the user is registered and verified, and is connected to an IoT device. If the user's phone number is unverified, the command sent through the SMS is rejected. In the case of a smartphone, the mobile app is encrypted by JWT and JWE to ensure that messages sent and received aren't read by third-party apps. In both cases if an IoT device is attempted to be accessed by an unregistered phone number, a message is sent to the registered phone number for further actions. A flag is also raised on the server to block requests from the unregistered phone number.

Messages received by registered and verified numbers are processed by the server system to be commands and sent to IoT, which then returns feedback messages to the user.

MAAMSIC may produce large amounts of data and receive many requests and responses, making it require a large processing capacity surpassing the capacities available for this implementation.

5. Conclusion and Further Work

This work addresses a methodology for adding an additional layer of security while availing data to users in an IoT system design in sub-Saharan Africa using GSM. MAAMSIC architecture will be extended to support functionalities for dealing with more complex events and billing policies. Incorporating features that will enable it to scale and deal with the increased workload is essential for future work. A possible solution is deploying the MAAMSIC server in a dedicated cloud server with a strong RAM and large memory. MAAMSIC can also be transformed into multi-edged cloud architecture to deal with internal risks. The security of the IoT network to ensure that it handles risks due to malicious behavior of IoT is still an open issue. For further enhancement of this work, the model could be designed to utilize solar or wind energy as its source of power. This is a cleaner energy and will be a great source of power in rural areas where electricity is not reliable. The MAAMSIC could also be improved by use of Artificial Intelligence and audio processing for better accessibility for the disabled especially those with poor eyesight.

References

Alam, T. (2020). A middleware framework between mobility and IoT using IEEE 802.15. 4e Sensor Networks. *Jurnal Online Informatika*, *4*(2), 90-94.

Bakibinga-Gaswaga, E., Bakibinga, S., Bakibinga, D. B. M., & Bakibinga, P. (2020). Digital technologies in the COVID-19 responses in sub-Saharan Africa: policies, problems, and promises. *The Pan African Medical Journal*, *35*(38).

Bima, I. W. K., Suryani, V., & Wardana, A. A. (2020). A Performance Analysis of General Packet Radio Service (GPRS) and Narrowband Internet of Things (NB-IoT) in Indonesia. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *5*(1), 11-20.

Ingram, W., & Memon, F. A. (2020). Robustness of IoT-connected e-Taps for sustainable service delivery of rural water supply. *Water Supply*.

Nazareno, A. C., da Silva, I. J., Nunes, E. F., Gogliano Sobrinho, O., Marè, R. M., & Cugnasca, C. E. (2020). Real-time web-based microclimate monitoring of broiler chicken trucks on different shifts. *Revista Brasileira de Engenharia Agrícola e Ambiental*, *24*(8), 554-559.

Ndubueze, P. N. (2020). Cybercrime and Legislation in an African Context. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 345-364.

Oliveira-Jr, A., Resende, C., Pereira, A., Madureira, P., Gonçalves, J., Moutinho, R., ... & Moreira, W. (2020). IoT Sensing Platform as a Driver for Digital Farming in Rural Africa. *Sensors*, *20*(12), 3511.

Owuor, D. O., Laurent, A., & Orero, J. O. (2020, August). Exploiting IoT data crossings for gradual pattern mining through parallel processing. In *ADBIS, TPDL and EDA 2020 Common Workshops and Doctoral Consortium* (pp. 110-121). Springer, Cham.

Priyanka, E. B., Thangavel, S., Madhuvishal, V., Tharun, S., Raagul, K. V., & Krishnan, C. S. (2020). Application of Integrated IoT Framework to Water Pipeline Transportation System in Smart Cities. In *Intelligence in Big Data Technologies—Beyond the Hype* (pp. 571-579). Springer, Singapore.

Rak, M., Salzillo, G., & Romeo, C. (2020). Systematic IoT Penetration Testing: Alexa Case Study. In *ITASEC* (pp. 190-200).

Royani, M. R., & Wibowo, A. (2020). Web Service Implementation in Logistics Company uses JSON Web Token and RC4 Cryptography Algorithm. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(3), 591-600.

Selgert, F. (2020, September). Cynefin framework, devops and secure IoT. In *International Conference on Computer Safety, Reliability, and Security* (pp. 255-265). Springer, Cham.

Machine Intelligence Research Labs
Ancora Imparo
2008

CERTIFICATE

This is to certify that the following paper was presented online during the
16th International Conference on Information Assurance and Security (IAS 2020)
held on the world wide web during December 15 - 18 , 2020.

Paper ID: 30

Paper Title: MAAMSIC: Multimodal Authentication and Authorization Model For Security of IoT Communication via GSM Messaging in Sub-Saharan Africa

List of Authors: Joan Nabusoba, Calvins Otieno and Wilson Cheruiyot

Springer

Prof. Dr. Ajith Abraham
IAS 2020 - General Chair

Issued On: December 17, 2020