# Ratna Kumar Tripura

*by* Iftekhar Efat

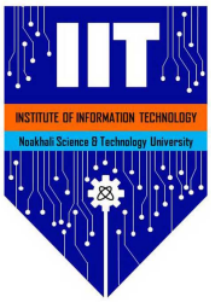
**Submission date:** 13-Mar-2022 12:38AM (UTC-0500)
**Submission ID:** 1782968731
**File name:** ASH1825042M.pdf (201.79K)
**Word count:** 1972
**Character count:** 10280

# Device Synchronization and Protection

*Name : Ratna Kumar Tripura*
**STUDENT ID : ASH1825042M**

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University




Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

**Abstract**

This paper addresses the problem of protecting distributed IoT units from network based attacks while still having a high level of availability. In particular we suggest a novel method where the IoT device execution state is modeled with a suitable high level application model and where the execution state of the application of the IoT device is "mirrored" in a cloud executed machine. This machine has very high availability and high attack resistance. The IoT device will only communicate with the mirror machine in the cloud using a dedicated synchronization protocol. All essential IoT state information and state manipulations are communicated through this synchronization protocol while all end application communication directed towards the IoT units is done towards the mirror machine in the cloud. This gives a very robust and secure system with high availability at the price of slower responses. However, for many non-real time IoT application with high security demands this performance penalty can be justified.

# 1 Introduction

In the near future, a very large number of IoT devices will perform critical security tasks in systems for industry process control, building automation, power control, healthcare etc. The correct operation of each of these units is crucial for the robustness of the system. Failure of a single critical component can give very severe consequences. Many IoT devices are resource constraint with respect to power, CPU capacity, memory etc. Hence, they are hard to protect from network based attacks such as Denial of Service (DoS) attacks, distributed DoS (DDoS). The main defense strategy against this type of attacks is restricting the communication interface towards the IoT devices which makes it both harder to perform attacks against the IoT device as well as limiting the consequences of successful attacks. However, this obviously has the drawback that the IoT devices might be harder to reach or the power consumption on the IoT devices goes up as the defense strategy requires more CPU cycles. Hence, there is a large need for solutions that find the right balance between availability and security of IoT devices. This paper addresses exactly this area by suggesting a novel principle for IoT protection with fairly high availability.

## 2 Background

All IoT devices are utilizing a unique device virtual machine mirror in a virtual infrastructure back-end system. The mirror is not a pure virtual machine copy of the IoT execution, but a high level machine that regularly synchronizes the essential IoT state with the corresponding state in the real IoT device. Furthermore, the mirror machine receives all direct requests targeting the real IoT device from the application domain, i.e. all traffic directed towards the real IoT device. This implies that the external world that wants to interact with the IoT devices in the system, always needs to communicate with their corresponding mirror machines only. No direct communication with the IoT devices themselves is allowed. The overall principle is depicted in Figure 3. In summary, the proposed system solution has the following main characteristics.

- During IoT device deployment, the IoT device is launched together with a dedicated "IoT mirror machine" in a cloud infrastructure.
- The IoT device runs a special synchronization protocol that keeps it synchronized with its corresponding mirror machine in the cloud.
- An end-application such as an end-user client or a backend application system that wants to exchange data or interact with an IoT device, does not have direct network access to the IoT device, but will always interact with the mirror machine in the cloud.
- When a request reaches the IoT mirror machine which requires direct execution on data sets belonging to the "real" IoT device, the mirror machine will be able to execute those instructions on the mirror machine data (local copy of the data objects from the IoT device) and respond to the request.
- An end-application might request an operation that cannot be performed on stored data objects values only.

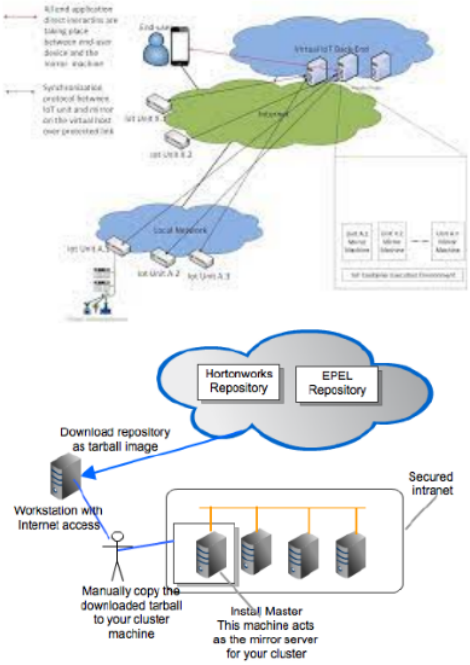
# 3 Methods

We discuss three different aspects that constitute the core of our solution:

- The design and principle for the mirror machines in the virtualized infrastructure.
- IoT device and mirror machines deployments.
- IoT device to mirror machine synchronization.

1. Mirror machine design: The basic principle of our solution is based on a design with a "mirror machine" that operates at a virtual back-end infrastructure (a cloud).

Figure 1: IoT device and Mirror machine




2. IoT device and mirror machines deployments: The solution consists of the following main deployment steps:

- Develop the data object model, IoT device model and define shared commands and realize a mirror machine (binary).
- Launch the mirror machine on suitable available computing resources. This can be done in the form of a Java virtual machine, a system virtual machine or an application running in a cloud environment.

- Configure the Mirror machine and the IoT device with shared credentials that allow them to set up secure connections during their synchronization process.
- Install and start the IoT device.
- Once installed, the IoT device connects to its mirror machine and makes sure it can establish a secure authenticated connection with its mirror machine. If this succeeds, the IoT device is ready for use.

3. Once installed, the IoT device connects to its mirror machine and makes sure it can establish a secure authenticated connection with its mirror machine. If this succeeds, the IoT device is ready for use. In the descriptions, we use the following notations:

   - We denote an arbitrary IoT device in the local network by u.
   - We denote the mirror machine corresponding to u by mu.
   - We denote the command queue at mu by qm.
   - We denote a data object set used by the mirror machine and the IoT by D
   - We denote the data objects at mu in D which are changed since the last synchronization attempt by dm.
   - We denote the data objects at u in D which are changed since the last synchronization attempt by du.
   - We denote the parameter at u determining the time between two consecutive synchronization attempts by t

Mirror Machine procedure:

1. The mirror machine, mu, is deployed on the system (see Section III-C ) and the sets dm and qm are both empty.
2. The mirror machine waits for requests from connecting IoT clients or from synchronization requests from u.
3. If a new IoT client request arrived the following applies:
   - If the request was authorized (allowed according to the IoT mirror machine security policies), the request is accepted and executed.
   - All data object changes which are the result of the request in step 3.a are marked and the set dm is updated.
   - All requests that results in commands that are not possible to execute on mu are transformed to commands and put on the command queue, qm.
   - Jump to Step 2.
4. If a new synchronization request from u arrives, the following applies:

- The request is authenticated using the pre-installed credentials shared with u and if it comes from any other device but u, it is refused (move back to step 2).
- mu sends all updates in the set dm to u.
- mu sends all the pending commands in qm and the command queue is cleared.
- mu waits for a data set update commands from u. If such commands are received, the set D is updated to match the corresponding set at u.
- mu waits for an end to the ongoing synchronization session with u.
- Execute any of the commands that are pending in the command queue which are due to the ongoing connected client r

2

IoT unit procedure:

1. The IoT device is deployed on the system (see Section III-C) and the set du is set to empty.
2. The IoT device starts a timer, tc = 0.
3. If tc ¿= (t) the following applies:
   - u uses the pre-configured network address of mu to make an authenticated new secure synchronization connection attempt to mu (using a suitable protocols such as TLS or DTLS for instance).
   - u requests the set dm and all the updates to the objects in this set from mu and based on this information it updates its own internal data objects in the set D.
   - u requests all pending commands in the queue qm from mu.

# 4 Results

So that the present paper gives very high protection of sensitive IoT devices such as resource constraint and battery driven devices. This is accomplished by the fact that a device will never accept any network session which it has not initiated itself and as it will only interact directly with its corresponding mirror machine in the virtual back-end 1. Instead, it receives all its data and operation requests through synchronization operations with the mirror machine. Hence, all attacks targeting sensitive IoT devices must be launched either against the synchronization interaction protocol or against the mirror machine instead of the real IoT device.

# 5 Conclusion

The synchronization and mirror machine based protection principle described in this paper gives a very high network attack protection level for distributed IoT units, which do not have strict real-time requirements. The most vulnerable IoT units are battery driven and/or resource constraint units. These are also units typically not having strict real-time requirements. This implies that the solution is useful in a very large set of distributed IoT use-case scenarios where resource constraint IoT units need to be protected from network based attacks. On the other hand, more powerful distributed IoT units with realtime requirements will not benefit from using the suggested approach, but these also have other rather efficient means for protection against network based attacks.

## Acknowledgements

This research is conducted in direct supervision of the Software Evaluation and Re-Engineering Research (SERER) Lab.

---

# A Appendices

This is a short appendix, just included as an example.

# References

[1] Kai Fan, Shangyang Wang, Yanhui Ren, Kan Yang, Zheng Yan, Hui Li, and Yintang Yang. Blockchain-based secure time protection scheme in iot. *IEEE Internet of Things Journal*, 6(3):4671–4679, 2018.

[2] Christian Gehrmann and Mohamed Ahmed Abdelraheem. Iot protection through device to cloud synchronization. In *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 527–532. IEEE, 2016.

[3] Jinping He, Chengxiong Mao, Jiming Lu, and Jiawei Yang. Design and implementation of an energy feedback digital device used in elevator. *IEEE Transactions on Industrial Electronics*, 58(10):4636–4642, 2011.

[2] [1] [3]

# Ratna Kumar Tripura

ORIGINALITY REPORT

| 87% | 87% | 78% | 7% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | docplayer.net<br>Internet Source | 46% |
| 2 | soda.swedishict.se<br>Internet Source | 34% |
| 3 | v1.overleaf.com<br>Internet Source | 5% |
| 4 | global.oup.com<br>Internet Source | 2% |
| 5 | www.coursehero.com<br>Internet Source | 1% |

| | | | |
|---|---|---|---|
| Exclude quotes | On | Exclude matches | Off |
| Exclude bibliography | On | | |

# Ratna Kumar Tripura

PAGE 1

**Article Error** You may need to use an article before this word. Consider using the article **the**.

PAGE 2

**Prep.** You may be using the wrong preposition.

**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

PAGE 3

**Missing ","** You may need to place a comma after this word.

**Article Error** You may need to use an article before this word.

**Missing ","** You may need to place a comma after this word.

PAGE 4

**Prep.** You may be using the wrong preposition.

**Article Error** You may need to use an article before this word.

**Missing ","** You may need to place a comma after this word.

**Missing ","** You may need to place a comma after this word.

**Proofread** This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 5

**Article Error** You may need to use an article before this word. Consider using the article **the**.

**Run-on** This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

**Proofread** This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

**Frag.** This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

**S/V** This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

**Article Error** You may need to use an article before this word.

**Missing ","** You may need to place a comma after this word.

PAGE 6

**Run-on** This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

**Possessive** You may need to use an apostrophe to show possession.

**Proper Noun** If this word is a proper noun, you need to capitalize it.

**Run-on** This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

PAGE 7

**Missing ","** You may need to place a comma after this word.

**Run-on** This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

**Article Error** You may need to remove this article.

PAGE 8

**Missing ","** You may need to place a comma after this word.

**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 9

**Article Error** You may need to use an article before this word.

**Article Error** You may need to use an article before this word. Consider using the article **a**.

PAGE 10

**Prep.** You may be using the wrong preposition.

**Confused** You have used **A** in this sentence. You may need to use **an** instead.

PAGE 11