A Trust Based Reputation Model For Secure Multi Agent Communication In Open Environment

**Patrick Kinyua Gikunda and
Dr. Elisha Opiyo Omulo**

University of Nairobi

Outline

- Problem background and definition
- System architecture
- Objectives
- Research outcome and their significance
- Results outcome and explanations
- Conclusion
- Future work
- Author line of interest

Background to the problem

❖ More than **seventy six million** households risk of losing their money through vulnerable networks as indicated by <u>Jessica</u> , <u>Matthew</u> and <u>Nicole</u> (2014)

❖ As MAS application evolve confidential and secure data is put at risk as reported by Evan (2014) more than 4.5 million records were stolen from health facility. Attackers use sophisticated malware to issue attacks and this calls for more comprehensive, flexible and robust secure measures

❖ The open and dynamic nature of MAS as described by Reza, Hakimi and Zahra (2012) has made it a challenge to operate MAS in a secured environment for information transaction

❖ The latest Sony theatre systems interruption and data stolen as reported by Jessica (2014) on The New York Times Newspaper shows how critical it is to come up with robust secure system communications

Problem

Many multi agents interaction use trust/reputation models for secure communication, but they fail to properly evaluate trust in an Open Environment when agents start to behave in an unpredictable way
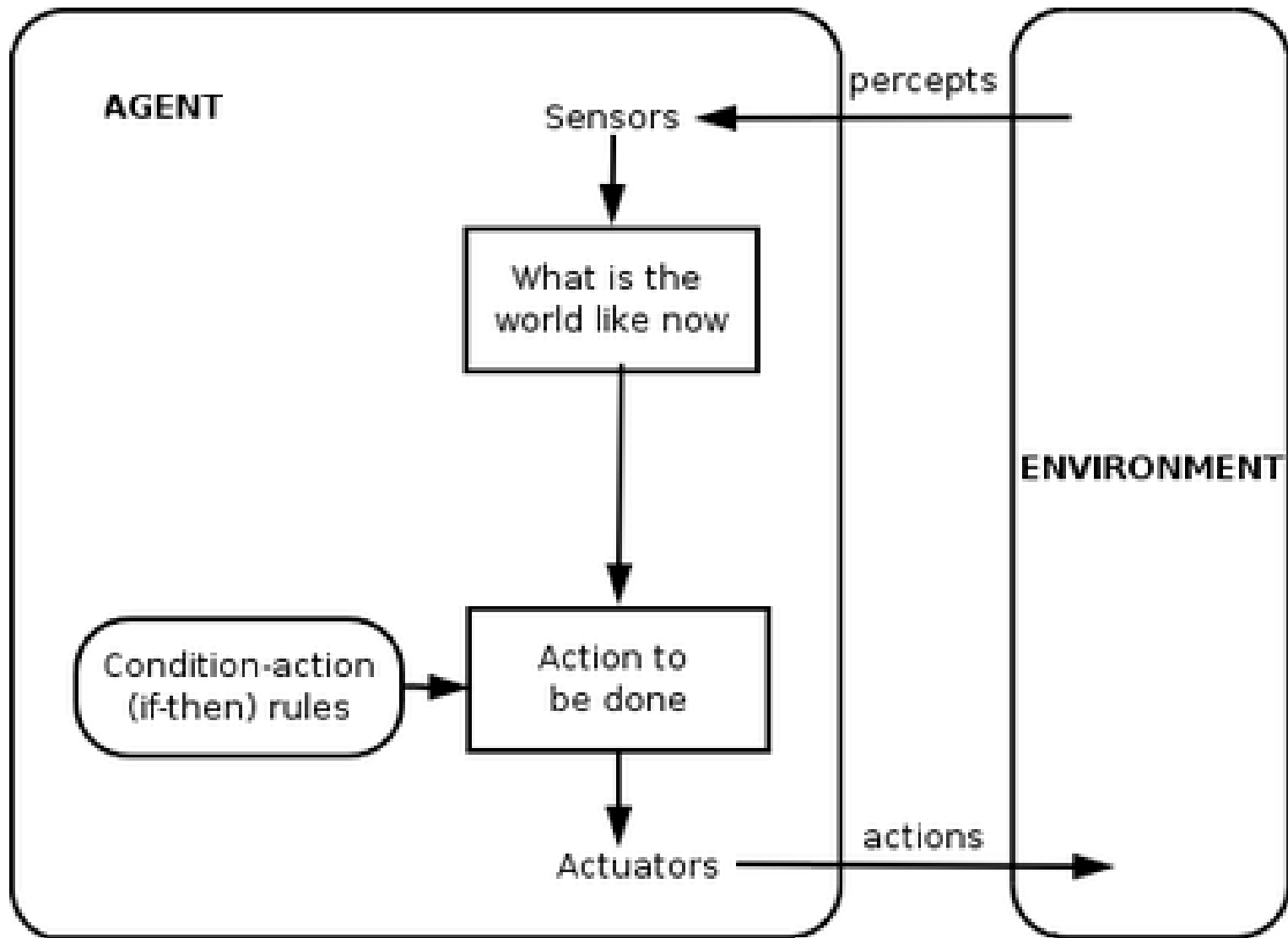
System Architecture
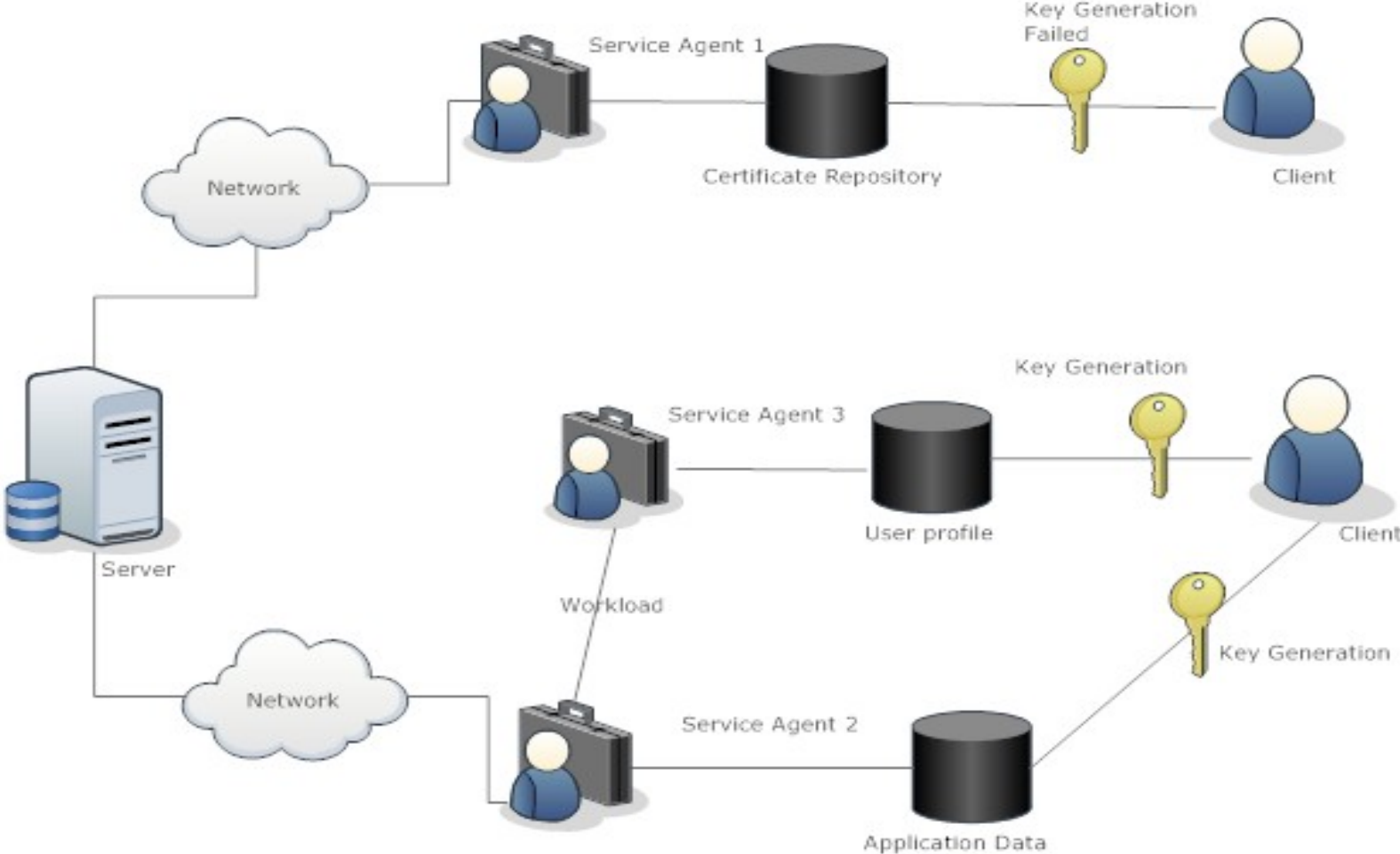
Objectives

The main objective of this project is to formulate a reputation model for effective and secure agents communication in an open environment.

Research outcomes and their significance

The goal of this project is to find methods that allow to building complex secure systems composed of autonomous and heterogeneous agents whose, while operating on local knowledge and possessing only limited abilities, are none the less capable of communicating securely in an open environment

Experimental Simulation

- STR to denote successful transaction rate. STR results were delivered from testing tool "nexpose"

- STR results as below:

A table below was used for recording the results over Open Environment;

Number of Clients	Number of Agents	Secure	STR(%)
5	5	Yes	100
3	6	No	78
1	10	Yes	92
5	7	No	85
1	10	Yes	98

Results Explanation

- **Secure STR Average on Internet = 290/3 = 96.6667%**

- **Non-Secure STR Average on Internet = 163/2 = 81.5**

- From above result it is clear that messages among agents over internet which are secured have the highest probability of being delivered to the intended destinations

Results Conclusion

From above result it is clear that messages among agents over internet which are secured using our model have the highest probability of being delivered to the intended destinations securely.

Conclusion

- In this paper we have described a generic trust computation model for multi-agent systems. Our model can be tuned to the meet the requirements of a specific application. For example our model can be used in electronic markets and e-commerce environments (like Amazon Auctions, eBay, OnSale Exchange) where buyers rate sellers regarding their purchase after they make a transaction. Sellers might attempt to raise their trust value (hence reputation) by creating fake buyers and fake transactions. So, in such scenarios our model can be applied to filter out potential bad sellers.

Further Work

- A study can be conducted to allow extensive tests of the model. This will help in evaluating the model in terms of data transfer speeds, stability, network load and robustness.

Author's immediate line of interest

Technology innovation solutions in developing Countries in Africa; Use of MAS to help maximize Tax collection in Developing countries in Africa.