Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 3704-3712

ANALYSIS ON A HIGH LEVEL OF DATA SECURITY USING A NOVEL CHAOS-BASED CRYPTOGRAPHY BASED ON THE TRUSTWORTHINESS OF MOBILE AGENTS IN DISTRIBUTED ENVIRONMENT

[1]Sai Arjun Madikonda

[1]Btech, Gitam deemed to be University Hyderabad

ABSTRACT :

The mobile agent system offers a promising solution for distributed systems applications that require fault tolerance, performance, and reliability. When it comes to issues like security and network management, mobile agents' inherent intelligence and autonomy come in handy. It is usually possible to add new systems to mobile agent technology because of its interoperability and adaptability. In spite of the benefits of self-reliance and intelligence, mobile agents are vulnerable to security breaches. Security mechanisms are provided to ensure the mobile agent's data is secure. Chaos-based cryptography is a highly secure method of encrypting data. The mobile agent environment has not yet seen any testing of this technique. Mobile agents are being used to test a chaotic cryptography based on Chebyshev polynomials and ElGamal. Hybridization resembles the data encryption method known as "signcryption" in many ways. Theory shows that chaotic cryptography is impenetrable to most threats. Chaos-based cryptography ensures a high level of data security throughout the system's architecture. Using a new measure called "trust scoring," it helps mobile agents decide on an itinerary based on the platform's trustworthiness.

1. INTRODUCTION :

Internet is a necessary tool for modern communication, and as such, it bears the burden of ensuring high-quality service for both the sender and the recipient of messages. If the application requires data to be processed before it can be transferred to another party, then the communication process is a two-step process. The client has access to the data, which is then processed by a server running on a network of workstations. The end-user who has access to the system needs the processed data. It was introduced in the early 1990s as a means of transferring information between systems via machine-readable messages. Methods in the server can be invoked by the client using function calls in Remote Procedure Call (Tay and Ananda, 1990). Functions and objects are predefined in the Remote Procedure Call. This does not aid in the system's ability to be tailored to the needs of the user. Developing a technology that is autonomous, flexible, and can be customised was the result of this.

1.1 CLASSIFICATION OF MOBILE AGENTS :

The classification of software agents is shown in Figure 1.1.

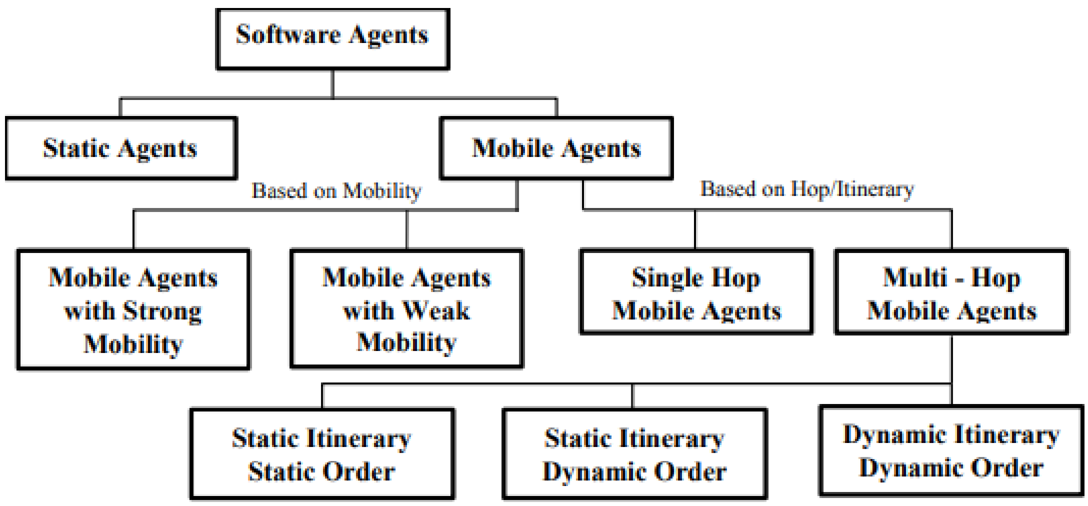

Figure 1.1 Classification of Software Agents

Static agents are intelligent software modules that reside inside a standalone system and perform tasks on behalf of a user. Mobile agents, on the other hand, are capable of travelling from one system to another. This capability of mobile agents makes them more usable by users to perform asynchronous and independent operations. A mobile agent is composed of three parts namely the code, state and data. The code contains the information on the computation which need to be performed by a mobile agent. The state refers to the current state of execution which the mobile agent is undergoing. Data refers to the data carried by the mobile agent from one platform/system to the other. A mobile agent requires a platform to get executed. The platform contains the resources required by a mobile agent to get executed. Therefore, it is required that the platform need to be compatible with the mobile agent to perform the task delegated to the agent.

2. SECURITY ISSUES WITH MOBILE AGENTS :

Though usage of mobile agents seem to be so advantageous, it has its own disadvantages in the security perspectives (Jansen and Karygiannis, 1999). The threats over the mobile agent can be broadly classified as

1. Agent-to-platform attacks

2. Agent-to-agent attacks

3. Platform-to-agent attacks

4. Other-to-agent attacks

5. Other-to-platform attacks

Apart from agents and platforms, other factors like malicious software or insecure networks may also be a cause for the attacks in a distributed environment.

2.1 Masquerade :

Masquerade is an attack where an agent or a platform pretends to be an authenticated agent or platform respectively and performs an attack. Here, the agent or the platform represents itself to be an authenticated entity thereby has smooth access towards the resources. Using the access, manipulation of data is possible. This greatly affects the security services namely confidentiality, availability and integrity.

2.2 Denial of Service :

This type of attack may prevent the access of data or resource from the platform or the agent. This is achieved either by flooding the network or by corrupting an important module which helps to gain access towards a critical resource.

Unauthorised Access :

This is a very common attack which is most common in mobile agent platforms. A malicious mobile agent pretends to be an authorised one and obtains access towards the resources in the mobile agent platform. This may either be achieved by usage of false authentication codes or due to lack of an appropriate authentication mechanism with the mobile agent platform. In masquerading, the entity itself is morphed whereas, in unauthorised access, the mechanism of authentication is compromised.

Repudiation :

This is a denial of authorization attack which is initiated by the malicious agent. The malicious agent sends an unauthenticated data and denies the sending of data. Any communication of such kind is denied by the malicious agent.

Eavesdropping :

This is a type of spying attack. The malicious agent gains access towards the information from a legitimate agent or a platform and may tend to misuse the information, in future. This poses a threat to the confidentiality of data.

Alteration :

This involves the modification of data, state or code of the agent which is considered a threat to the integrity of the system.

Copy and Replay :

This is an attack which tends to reduce the trust over a mobile agent. A copy of the mobile agent is created and is send to a platform again and again, so that the platform may consider it as an illegitimate entity in the system thereby further denies access to the original mobile agent.

Tailgating :

The mobile agent has a part of malicious code attached to itself, pretending to be a part of the legitimate mobile agent. The malicious code will be a part of the mobile agent until it obtains access to the data and resources in the platform

It is mandated by the OSI Security architecture that any entity related to a network should afford to the requirements namely confidentiality, integrity, availability and accountability. Hence, it is a challenge to offer the mentioned security features to a mobile agent.

3. PROPOSED SYSTEM ARCHITECTURE :

3.1 INTRODUCTION :

The role of distributed systems has become vital to obtain faster access from diverse locations. The usage of mobile agents in distributed environment provides promising results due to the characterisation of adaptability and autonomy. When the major focus is on the data carried by the mobile agent, a cryptographic algorithm can be used to secure the data. It provides confidentiality and integrity to the data. The proposed system uses chaos-based cryptography to provide confidentiality and integrity to data. Moreover, the mobile agent carrying the data must also be secure. It is always an optimal strategy to avoid circumstances that cause malicious attacks. This can be achieved by the usage of a decision support system that recommends the platforms suitable for the visit of a mobile agent.

3.2 SYSTEM ARCHITECTURE :

The proposed system architecture is shown in Figure 3.1. The system is made up of the following components

1. Mobile agent

2. Data platform

3. Server platform and

4. Trust monitor

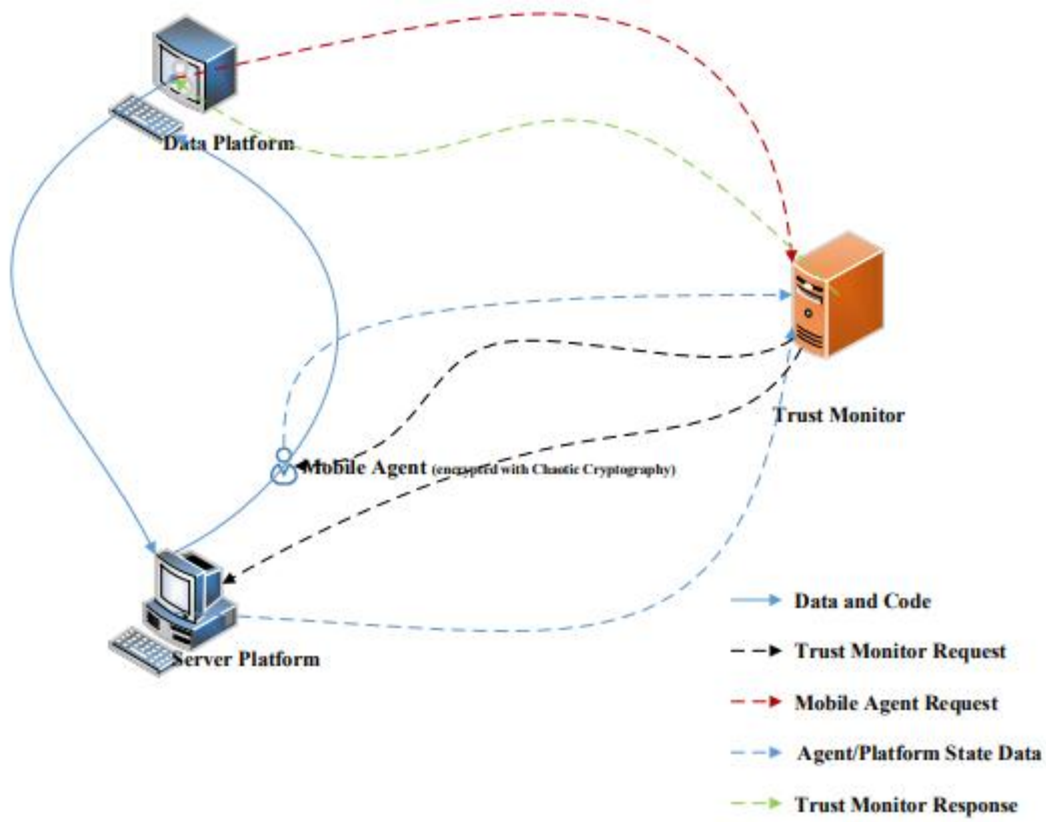

Figure 3.1 System Architecture

3.2.1 Mobile agent :

The data required to be processed by a system or data platform is carried by the mobile agent specified in the architecture. The modified Chebyshev polynomial cryptosystem, a variant of chaos-based encryption is used to encrypt the data carried by the mobile agent. It is less possible to guess the key or crack the key using brute-force or any cryptanalytic technique, in a system where chaos-based encryption technique is deployed for security. The cryptographic processes namely encryption and decryption consume more time, unlike other encryption schemes. Therefore, this system suits applications which handle sensitive and classified data.

3.2.2 Data platform :

The user directly interacts with the data platform, which is mostly available with the client system. The user may send request to various other platforms through mobile agents to collect the data required for processing. The term "data platform" should not be confused with the functionality. Since it originates the mobile agents responsible for data collection, it is termed data platform. For example, the user needs a comparative statement of the cost of a particular product. The mobile agent which originates from the data platform carries the specification of the product and travels through each server platform. During the itinerary, the mobile agent collects the data required by the data platforms from each server platform. The collected information is processed and the comparative statement is displayed to the user, by the data platform.

3.2.3 Server platform :

The server platform contains the data or resource required by a data platform. The server platform is a static agent and acts as a repository of data. Data platform, with the help of the mobile agents, collect the data available with the server platform.

3.2.4 Trust Monitor :

Trust monitor is responsible for maintaining the trust score, a measure to assess the server platforms. Trust monitor is highly protected and has the data pertaining to each transaction with respect to a server platform. The data platforms, at the time of originating the mobile agent, communicates with the trust monitor, to set the itinerary for the mobile agent. In case of dynamic itinerary, the mobile agents themselves communicate with the trust monitor to obtain advisory note over the next hop.

4. A CHAOTIC APPROACH FOR SECURE DATA TRANSFER USING MOBILE AGENTS :

The platform from which a mobile agent originates is termed home platform and the other platforms which the mobile agent visits are termed foreign platforms. The migration of a mobile agent from one platform to another is termed a hop. A mobile agent visits multiple platforms by multiple hops, which is planned either statically or dynamically. This plan for visiting various platforms is called an itinerary. The itinerary, in other terms, may be defined as the travel plan of a mobile agent. Figure 4.1 gives an illustrative outline on the basic terminologies related to mobile agent technology.

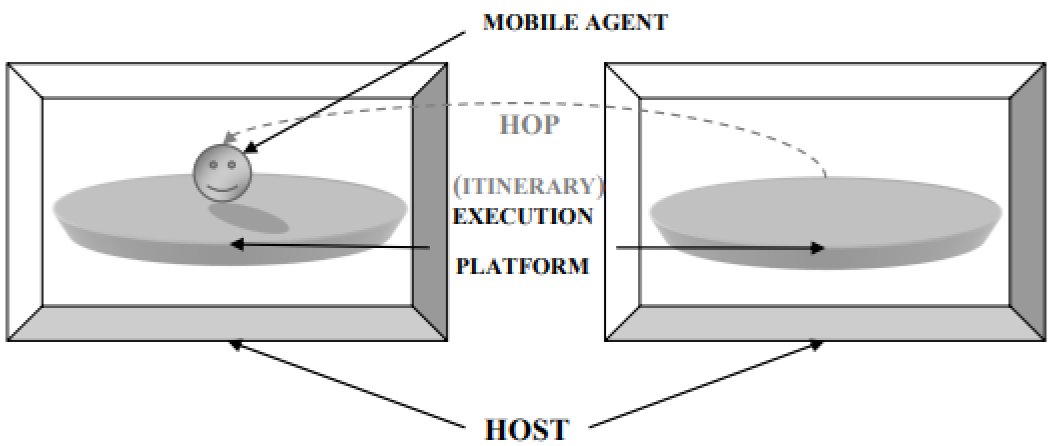

Figure 4.1 Illustration of mobile agent, platform, host, itinerary and hop

A mobile agent is made of three components namely the code, state and data. Code is the module which is effected with the migration from one system to another. The data required to be processed or shared, to achieve a particular task, is carried by the mobile agent. The current status of the mobile agent is contained in the state. Figure 4. 2 shows the various parts of a mobile agent.

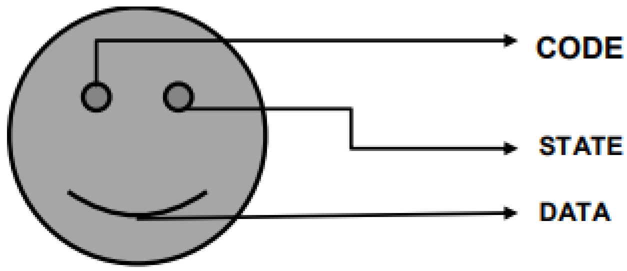

Figure 4.2 Parts of a mobile agent: code, state and data

In most cases, mobile agents act as means of carrying data from one platform to another. Mobile agents are either delegated with the rights of the owner or the execution rights are provided by the foreign platform.

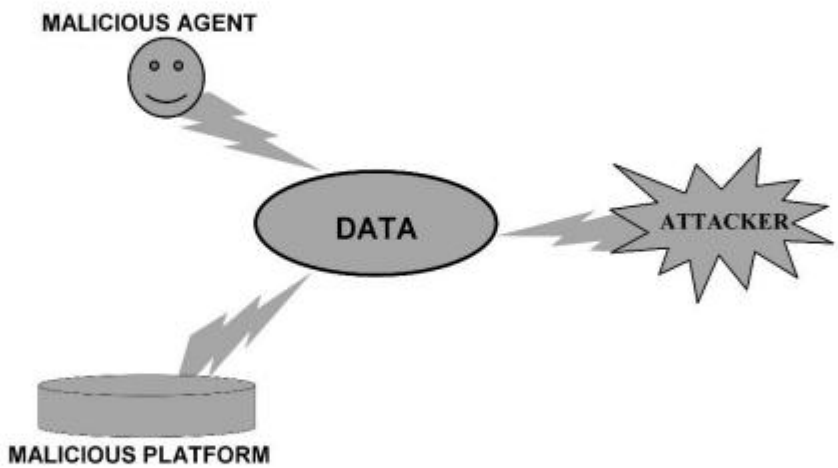

Figure 4.3 Vulnerability towards threats

A mobile agent is prone to a number of threats when introduced into open distributed environment. Figure 4.3 shows the possible attacks that are posed over a mobile agent carrying data in a distributed environment. There are various possibilities of malicious attacks; the mobile agent itself may be malicious or the platform may be malicious or the attack may be initiated by a third party which may or may not be a part of the system. The above statement infers that a mechanism need to be devised to protect the data carried by the mobile agent. Encryption algorithms are used to protect the data and hash functions are deployed to ensure the integrity of the data.

4.1 CHAOTIC APPROACH FOR DATA PROTECTION :

This work emphasize the usage of chaotic cryptography over the data carried by mobile agents. To apply chaotic cryptography over the data, one must be familiar with certain terms which are to be used in the fore coming sections of this chapter. The effectiveness of chaos-based encryption depends on the selection of maps. In this system, the Chebyshev map is used. Chebyshev maps possess a set of characteristics which makes it possible to be used in a cryptographic system. The characteristics that make Chebyshev maps suitable for cryptographic systems is discussed below.

Chebyshev Maps :

4.3.1

Let Tp be a Chebyshev polynomial map of degree p which can be defined as

$$T_{p+1}(x) = 2xT_p(x) - T_{p-1}(x) \qquad (4.1)$$

Let there be an assumption T0 2=(x) and x 1=T (x) . Using Equation (4.1)

$$T_2(x) = 2x^2 - 2$$
$$T_3(x) = 4x^3 - 5x$$

The above set of polynomials which are resulted on substituting appropriate values to the Chebyshev maps are called Chebyshev polynomials.

4.2 CHEBYSHEV POLYNOMIAL BASED CRYPTOSYSTEM FOR MOBILE AGENTS :

The mobile agent Environment in the proposed system contains a number of mobile agents which are originated from different hosts. The mobile agents are aware of their itinerary. The host contains a static chaotic agent which is responsible for encrypting and decrypting the data carried by mobile agents, using chaotic cryptographic technique.

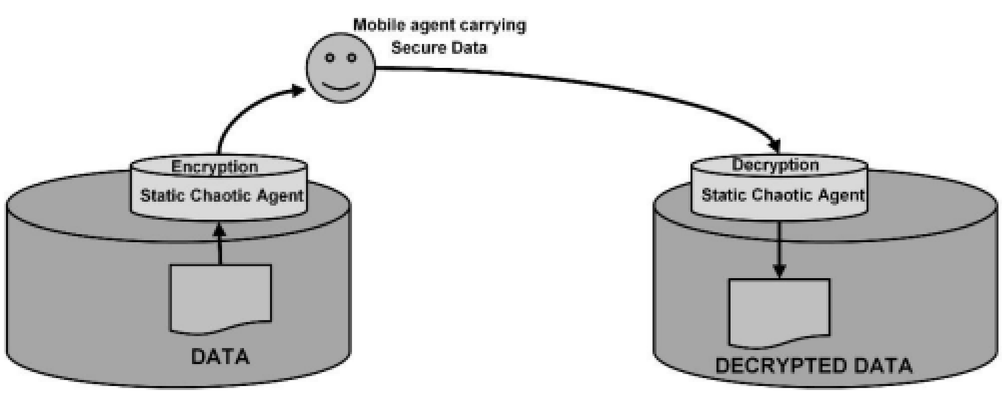

Figure 4.4 Chaos-based encryption and decryption

The data communication involves two important parties, namely the sender platform and the receiver platform. In general, the sender platform S sends some data D to the receiver platform R. The sender platform contains a static chaotic agent SP and receiver platform contains a chaotic agent RP. A generic cryptographic process contains three steps namely key generation, encryption and decryption. The process is illustrated in Figure 4.4.

CONCLUSION :

Mobile agents are considered to be the most reliable means of computing where intelligence and adaptability is required. This is most important when it involves computation in the distributed environment. The mobile agents provide the best solutions for problems related to network management, network security etc. However, the mobile agents are prone to a number of attacks during the phase of their itinerary. The attacks have a major focus over the data carried by the mobile agents. Hence, providing security to the data carried by the mobile agents is a prime concern. The mobile agents would be more secure if there exists a decision support system which helps mobile agents to find safer platforms and hosts. This research provides a solution to the major problems namely data security and design of a decision support system for safe transactions in distributed system.

REFERENCES :

1. Li, C.; Zhang, Y.; Yong, E. When an attacker meets a cipher-image in 2018: A year in review. J. Inf. Sec. Appl. 2019, 48, 1–9. [CrossRef]
2. Özkaynak, F. Brief Review on Application of Nonlinear Dynamics in Image Encryption. Nonlinear Dyn. 2018, 92, 305–313. [CrossRef]
3. Cho, J.; Kim, T.; Kim, S.; Im, M.; Kim, T.; Shin, Y. Real-Time Detection for Cache Side Channel Attack using Performance Counter Monitor. Appl. Sci. 2020, 10, 984. [CrossRef]
4. Açıkkapı, M.S.; Özkaynak, F.; Özer, A.B. Side-channel Analysis of Chaos-based Substitution Box Structures. IEEE Access 2019, 79030–79043. [CrossRef]
5. Nyberg, K. Differentially uniform mappings for cryptography. In Workshop on the Theory and Application of of Cryptographic Techniques; Springer: Berlin/Heidelberg, Germany, 1994; Volume 765, pp. 55–64.
6. Daemen, J.; Rijmen, V. AES proposal: Rijndael. In Proceedings of the 1st Advanced Encryption Conference, Ventura, CA, USA, 20–22 August 1998; pp. 1–45.
7. Özkaynak, F. Construction of Robust Substitution Boxes Based on Chaotic Systems. Neural Comp. Appl. 2019, 31, 3317–3326. [CrossRef]
8. Strogatz, S. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering (Studies in Nonlinearity); Westview Press: Boulder, CO, USA, 2001.
9. Kocarev, L.; Lian, S. Chaos Based Cryptography Theory Algorithms and Applications; Springer: Berlin/Heidelberg, Germany, 2011.
10. Zhu, C.; Wang, G.; Sun, K. Cryptanalysis and Improvement on an Image Encryption Algorithm Design Using a Novel Chaos Based S-Box. Symmetry 2018, 10, 399. [CrossRef]
11. Zhang, X.; Wang, X. Multiple-Image Encryption Algorithm Based on the 3D Permutation Model and Chaotic System. Symmetry 2018, 10, 660. [CrossRef]
12. Ding, L.; Liu, C.; Zhang, Y.; Ding, Q. A New Lightweight Stream Cipher Based on Chaos. Symmetry 2019, 11, 853. [CrossRef]
13. Demir, K.; Ergün, S. An Analysis of Deterministic Chaos as an Entropy Source for Random Number Generators. Entropy 2018, 20, 957. [CrossRef]
14. Özkaynak, F. An Analysis and Generation Toolbox for Chaotic Substitution Boxes: A Case Study Based on Chaotic Labyrinth Rene Thomas System. Iran. J. Sci. Tech. Trans. Elect. Eng. 2020, 44, 89–98. [CrossRef]

1\. 15. Cusick, T.; Stanica, P. Cryptographic Boolean Functions and Applications; Elsevier: Amsterdam, The Netherlands, 2009.