# Artificial Intelligence Techniques Used in Secure Military

*Dr. Sandeep Kumar[1],Anurag Gupta[2]*
*[1.]Director, Aryan Institute of Technology, Ghaziabad, U.P., India*
*[2.]Assistant Professor (Dept. CSE), ABES Engineering College, Ghaziabad*
*sandeepmrt@yahoo.com*

***Abstract*-This paper identifies open strategic issues needing immediate attention and provides recommendations for a unified, comprehensive strategy to address the security concerns within secure military [SM]. Peer-to-Peer artificial intelligence techniques in Security: Most feasible proposals to date Virtual Certificate Authority – Threshold prolog approach Certificate Chaining based on Pretty Good Privacy (PGP).**
**Keywords: Characteristics, Protocol design constraints, AI Tools, Prolog.**

## 1.INTRODUCTION

Security is primary requirement of any organization (Military) protocol. In order to find a solution to this always up to date problem. Artificial intelligence technique is constructed to provide secure communication applications. so, the clever deign of a AI technique is essential if the security of an application is to be maintained. Many works from different .research groups have been published, analyzing AI techniques for finding holes in the security strength of today's key.

Figure 1: AI technique control tracking area

Thus new key of artificial intelligence techniques are needed that don't have such security holes. That however might have the side effect of high complexity, which can make the implementation of a key technique very difficult if not impossible.

"One of the major problems of modern computer security is the design of artificial intelligence techniques that have as little vulnerabilities as possible while maintaining their low implementation complexity.

Many techniques that are secure are not easily implemented in computer applications especially in hardware. Thus the need for hardware implementation of secure AI technique becomes even greater."

Related Works

Defined by the following major characteristics:

No Infrastructure: Does not require centralized units (base stations, access points) to provide network functionality.

Dynamic Network Topology.

Distributed Network Services.

Communication over wireless channel: error-prone.

Self-Organized, Spontaneous, Unplanned and Impromptu.

Sporadic Connectivity.

Constraints on protocol design:

Limited processing power.

Limited memory resources.

Limited bandwidth.

Poor physical security.

Characteristics itself is constraints!

2.3 How to build an AI Strategy for secure military?

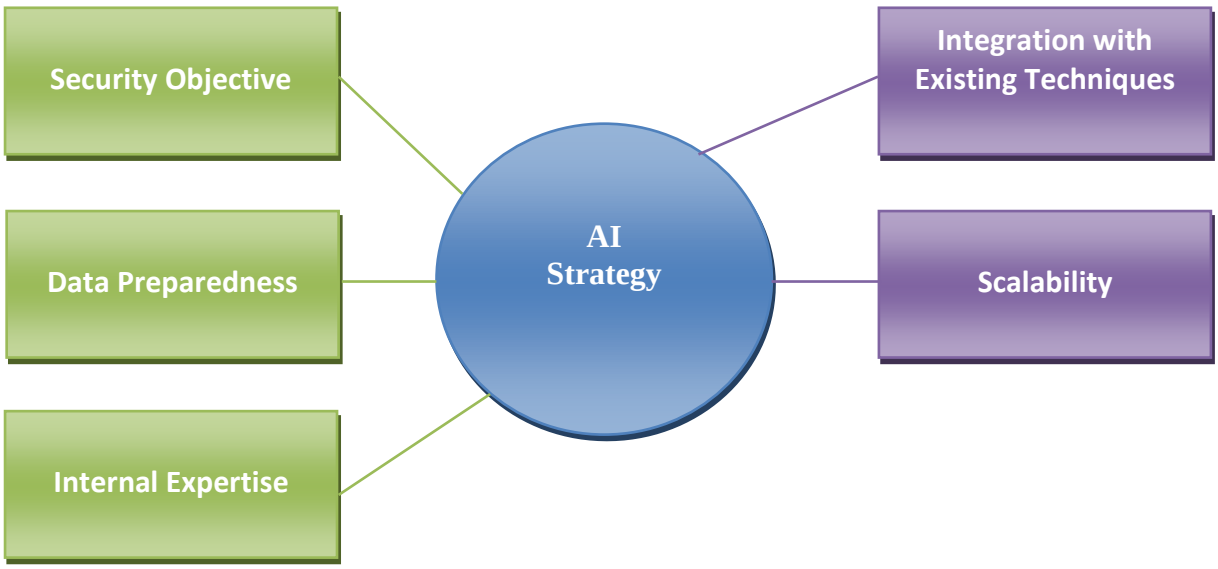


Figure 2: AI Strategy for secure military

Defining AI Techniques

Techniques and procedure for:

Initializing users within a domain.

Generation, distribution and installation of all keying material.

Control the use of keying material.

Update, revocation and destruction of keying material.

Storage, backup/recovery and archival of keying material.

Certificate Authority (trusted third party)

Sign certificated using its private key.

Store certificates.

Distribute certificates.

Users verify certificates with CA public key.

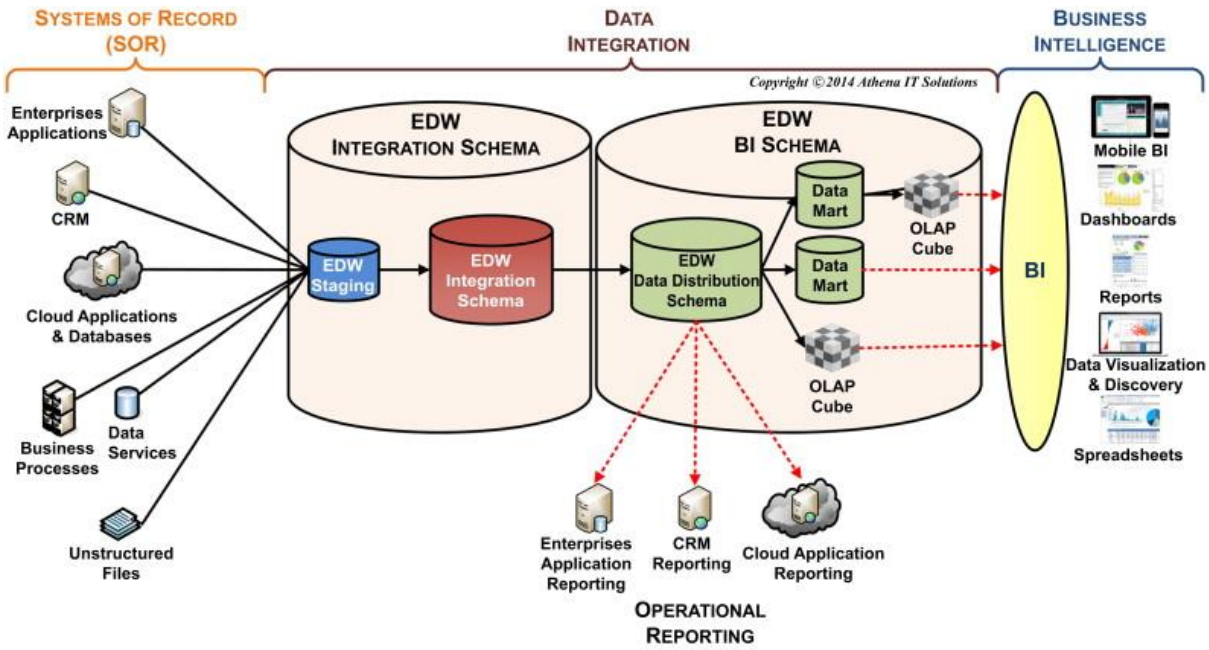


Figure 3: Prolog tools used in system

Feasible proposals-

1. Virtual Certificate Authority

1.1 Prior to network formation-Trusted Third Party (network administrator) distributes the following:

i. Load all nodes with its public key certificate.

ii. Select n CA servers and securely transfer

partial CA private key shares.

iii. Provide n nodes with certificates of all nodes in the network.

1.2 Nodes contact Virtual CA for certificates


Figure 4: Network architecture for secure military

Private Key of certificate authority is distributed between n servers to form a distributed prolog service with universal private/public key pair.

Figure 4 (b): Network schematic architecture for secure military

Virtual CA sign message m with (n, t+1) threshold digital signature scheme. Each server partially signm with its private/public key share. These are combined at C.

2. Certificate Chaining based on Pretty Good Privacy (PGP)

i. Self-Organized, scalable solution

ii. No trusted third party required

iii. All users create their own public/private key pair

iv. Create, store and distributed their own public key certificates

v. Sign certificates of other nodes they trust.

vi. Store certificates of neighbouring nodes and 'friend' nodes in local certificate repositories.

Figure 5: Signing authority node to node

## 3. PEER TO PEER PROLOG BASED ON MOBILITY.

Design Objectives:

Provide strong security

Routing-security interdependence problem.

Address ownership problem.

Sybil Attacks.

Initialization Phase

Off-line TTP provides each node with a certificate and optional network member list.

TTP provides a strong security root: bind users, nodes and keying material.

Post-initialization Phase

Nodes that come within each other's transmission range exchange their certificates.

Each node is its own authority domain.

Avoids routing–security interdependence cycle: do not need routing protocol as it runs over one-hop radio links.

Major advantages

Provide network access control and user authentication.

Easy to prove security level suitable for military application.

Break routing-security interdependency cycle.

Mitigate Sybil attacks: TTP can provide one-to-one binding between the node and user.


Figure 6: to prove security level suitable for **military application**

## 4. MOTIVATION AND CONTRIBUTION

The individual technique described above may not be suitable for implementing multicast in MANETs. Boolean technique gives better security but complexity ti high.

In modified Huffman technique the complexity is less but it is suitable for a small group and hence scalability is not supported.

Figure 6 (b): to prove security level suitable for **military application**

In our proposed model we utilize the merits of Boolean minimization technique and modified Huffman technique to achieve the security well as better complexity in the MANET. In MANET one mode (normally cluster head) acts as the master node which controls the other nodes in its vicinity. Here cluster head acts as a group controller. Group controller is responsible for creating and maintaining the group key, Additional an unique ID for every user in the group is given based on Boolean technique but the length of this unique ID is not same for all the nodes. The length is based on the probability of leave of a member from the group. So based on the probability of leave different subgroups are formed with different unique ID lengths and this can be achieved the member join/leave is handles as discussed using Boolean technique for the sub groups.

## 5. EXPERIMENTATION RESULTS AND COMPLEXITY ANALYSIS

Storage complexity:

It includes the storage requirements of both group controller and users. The group controller has to store auxiliary keys of all the members and one group key. For example, the user size of 8, it has to store k0k1k2, k0'k1'k2' and one group key which is equal to $2\log_2 8 + 1 = 7$. in general, the storage complexity of the server is $2\log_2 n+1$ where n is number of members. As for the storage requirement of the individual user is concerned, an user has to store all the auxiliary keys from the leaf node to the root and one group key. So it is $\log_2 n+1$.

Communication and Computation Analysis:

Communication complexity is measured in terms of no. of rekeying messages' sent by the group controller and computation complexity is measured in terms of number of encryptions needed by the group controller. Both complexities depend on the position of the existing members in the tree after the left out members.

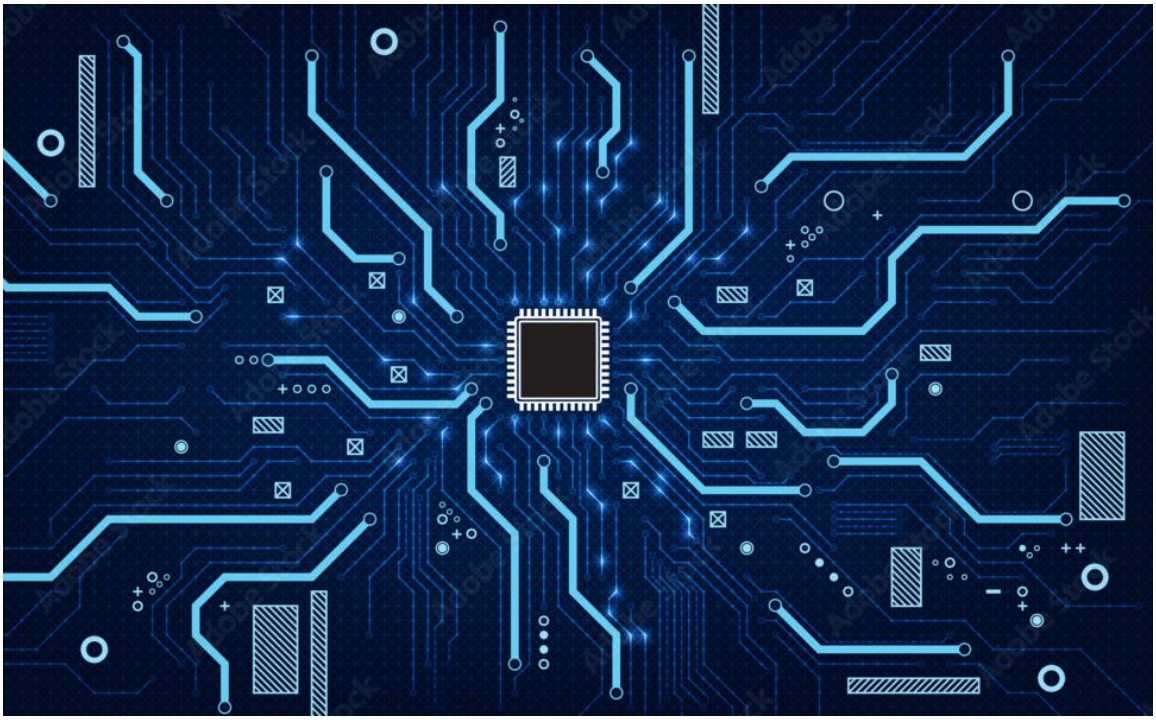

Figure 7: Communication and Computation Analysis

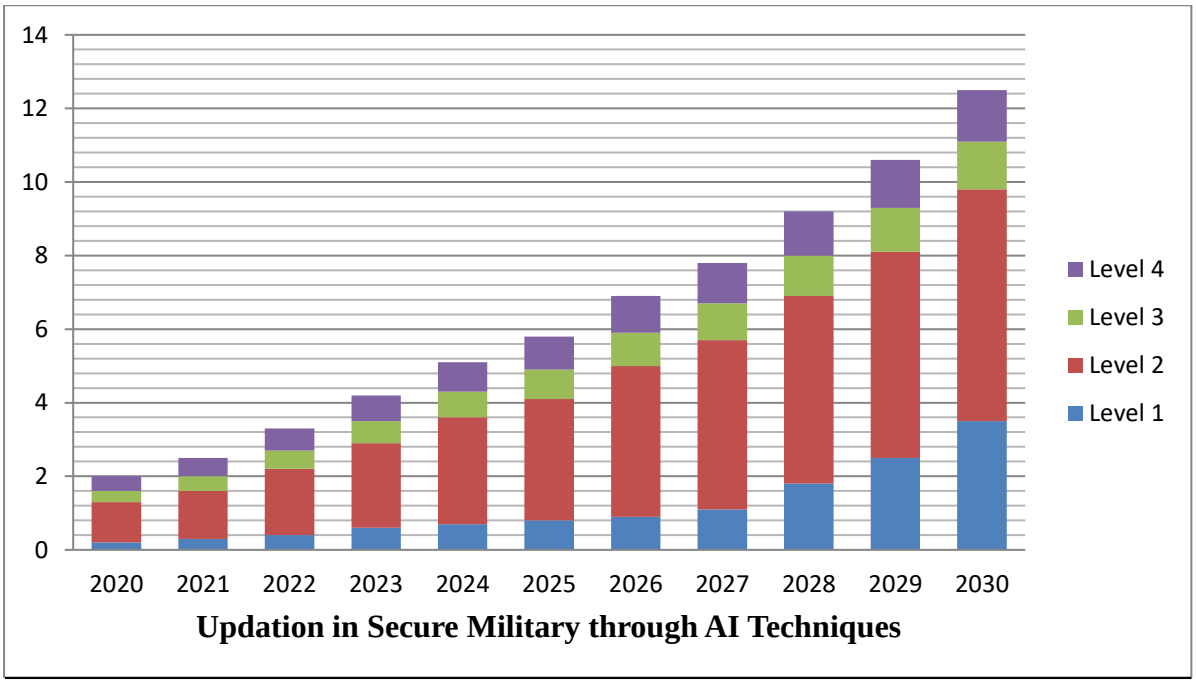


**Figure 8:** Updating in Secure Military through AI Techniques in graphical chart

## 6.CONCLUSION

1. Distribution of CA in mobile ad hoc networks cannot provide military level security.
2. Eliminating all forms of on-line and off-line TTP degrades security. Pure mobile ad hoc networks thus not suitable for military applications.
3. Combining a self-organized approach with an off-line TTP will provide adequate security.

**3.1** Need to make scheme independent of mobility and incorporate a self-organized key renewal mechanism.

**3.2** Each nodes its own authority domain.

**4.** Due to the increased usage of group communication there is a heavy demand for security in multicasting.

**5.** The security in multicasting imposes several problems and finding solutions to them become research challenges.

**6.** The most important feature of secure multicast is group dynamic (i.e.) the member of the multicast groups can join and leave the session at any time without intercepting the current session.

**7.** The main objective of this paper is to minimize the computational and communication cost involved in multicasting while changing the keys.

**8.** Intelligence is embedded in to the group controller so that instead of assigning a constant length UID for the user.

**9.** It assigns the UID based on the probability of leave.

**10.** The results are encouraging and comparable with existing techniques.

REFRENCES

[1]. Investigating Intrusions", Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 -84965 -1.
[2]. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, 15-Dec 2010.
[3]. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.
[4]. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
[5]. Chatterjee, R. Chaudhuri, D. Vrontis, A. Thrassou, S.K. Ghosh, Adoption of artificial intelligence-integrated CRM systems in agile organizations in India, Technol. Forecast. Soc. Change 168 (2021), 120783
[6]. T. Davenport, A. Guha, D. Grewal, T. Bressgott, How artificial intelligence will change the future of marketing, J. Acad. Market. Sci. 48 (1) (2020) 24–42.
[7]. U.S. Department of State, "Abstract of concept of operations for the integration of contactless chip in the U.S. passport," U.S. Department of State, Tech. Rep., April 2004.
[8]. Oreizy, P., Gorlick, M.M., Taylor, R.N., Johnson, G., Medvidovic, N., Quilici, A., Rosenblum, D., and Wolf,
[9]. An Architecture-Based Approach to Self-Adaptive Software. IEEE Intelligent Systems May/June 1999.
[10]. Shaw, M., and Garlan, D. Software Architectures: Perspectives on an Emerging Discipline. Prentice Hall, 1996.
[11]. N. Medvidovic and R. N. Taylor. A framework for classifying and comparing architecture description languages. In Proceedings of the 6th European Software Engineering Conference held jointly with the 5th ACM SIGSOFT Symposium on the Foundations of Software Engineering, Zurich, Switzerland, Sep. 1997.
[12]. Alan B Craig, William R Sherman and Jeffrey D Will, "Developing Virtual Reality Applications:
[13]. Foundations of Effective Design", Morgan Kaufmann, 2009.
[14]. John Vine, "Virtual Reality System", Addison Wesley, 1995.
[15]. William Stallings, "Data and Computer Communication", Pearson.
[16]. William Stallings, Network Security Essentials: Applications and Standards,