Anatomy of Threat to the Internet of Things

Author: Iman Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, Wei Ni

IEEE Communications Survey and Tutorials, Vol. 21, No. 2, second quarter **2019**

Presenter: Seonghyeon Gong

Advanced Internet of Things Security, 2019-09-17

국립 서울과학기술대학교
SEOUL NATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY
Cryptography and
Information Security Lab

Table of Contents

Cryptography and Information Security Lab

1. Introduction

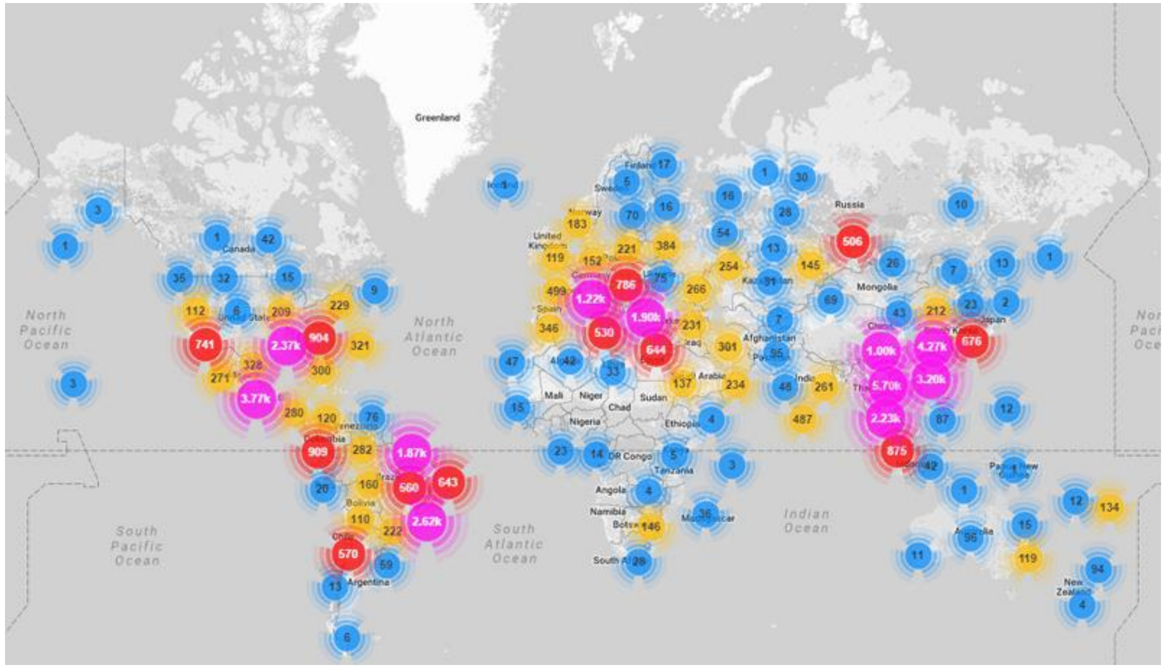
- IoT Trend Outlook
  - A massive number of these devices have been interconnected to each other and further connected to the Internet to form an Internet of Things (IoT).
  - IoT based services have seen an exponential economic growth in last five years especially in telehealth and manufacturing applications and are expected to create about USD 1.1-2.5 Trillion contribution in the global economy by 2020[2].
    - ✓ more than 85% of enterprises around the world will be turning to IoT devices in one form or the other, and 90% of these organizations are not sure about the security of their IoT devices[12].

1. Introduction

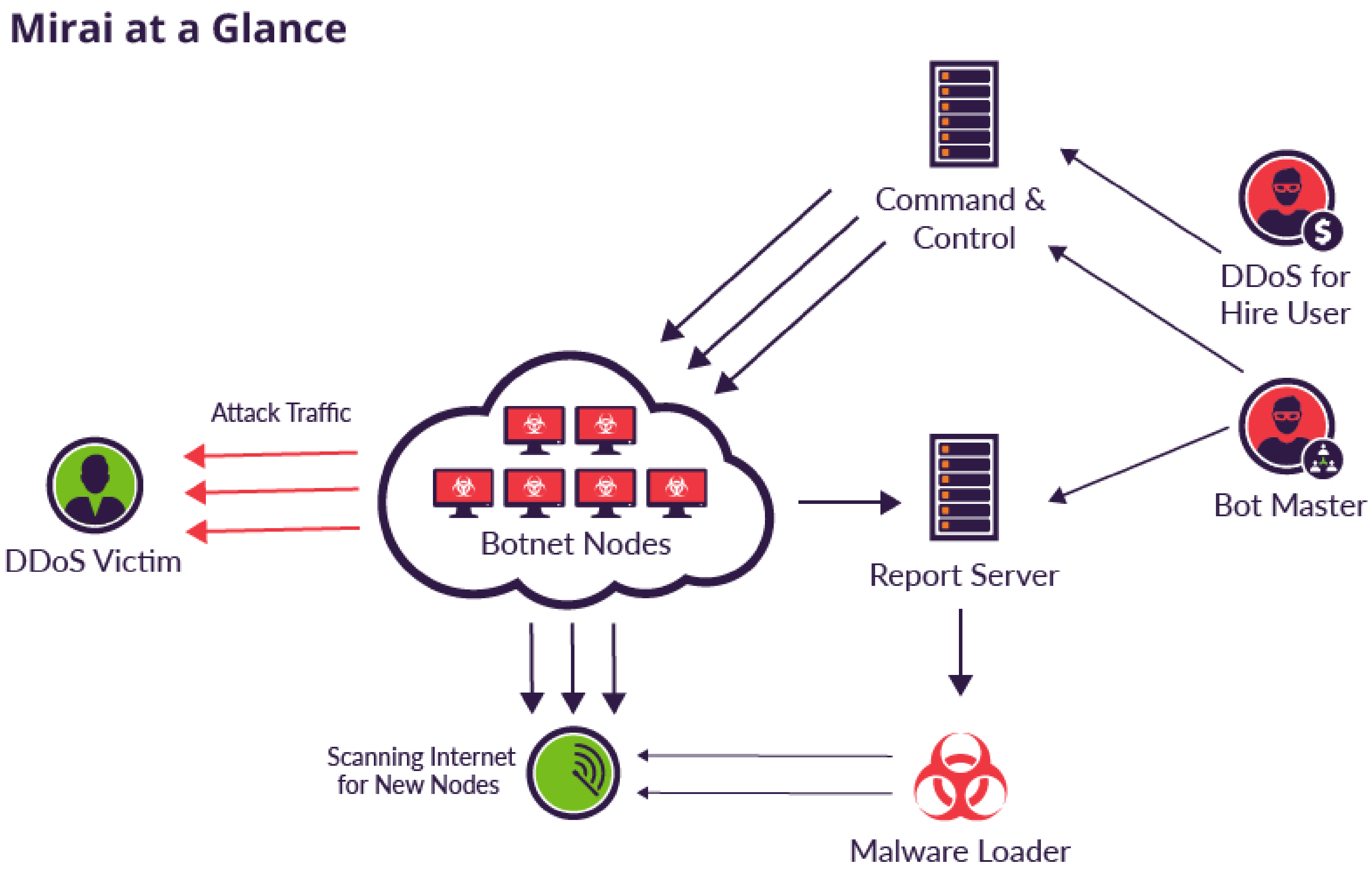
❖ Security Issues

- HP revealed that 70% of the devices connected to the Internet are vulnerable to numerous attacks[14]
- Smart cars and Legacy industrial systems such as manufacturing, energy, transportation, chemical, water and sewage control systems have greater security risks[15]
- Expected that by the end of 2020, more than 25% of corporate attacks would be because of compromised IoT devices[17]

- Successful launch of sophisticated cyber-attacks on ICS and other critical infrastructure have rendered existing IoT protocols ineffective
  - ✓ i.e. like Mirai[18], Ransomware[19], Shamoon-2[20] and DuQu-2[20]



❖ Real Case: Mirai Attack (DDoS as a Service)



1. Introduction

❖ Contribution of this research

- Presenting an "All in one package" that comprehensively covers most of the aspects of IoT security
- Deducing an attack strategy of a Distributed Denial of Service (DDoS) attack through IoT botnet
- Presenting a comprehensive ser of security guidelines based on industrial best practices
- Discussing open research challenges

2. Threats to the IoT

Cryptography and Information Security Lab

- ❖ IoT Architecture
  - ➢ lack of consistency and standardization in IoT solutions across the globe due to which there are issues related to interoperability, compatibility, and manageability[27].
  - ➢ To reduce this non-uniformity, this research present a consolidated generalized IoT architecture and a layered IoT protocol stack.

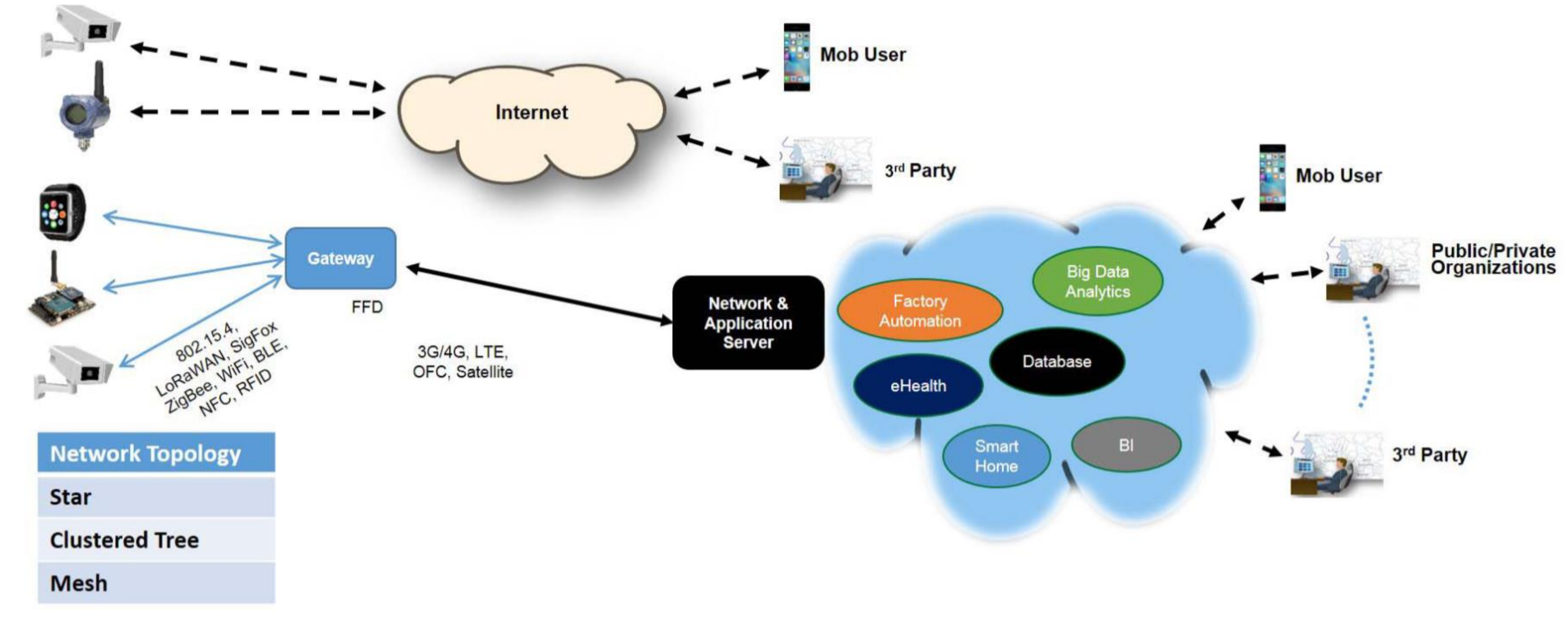


Fig. 1. Generalized IoT Architecture.

2. Threats to the IoT

Cryptography and Information Security Lab

❖ IoT Protocol Stack

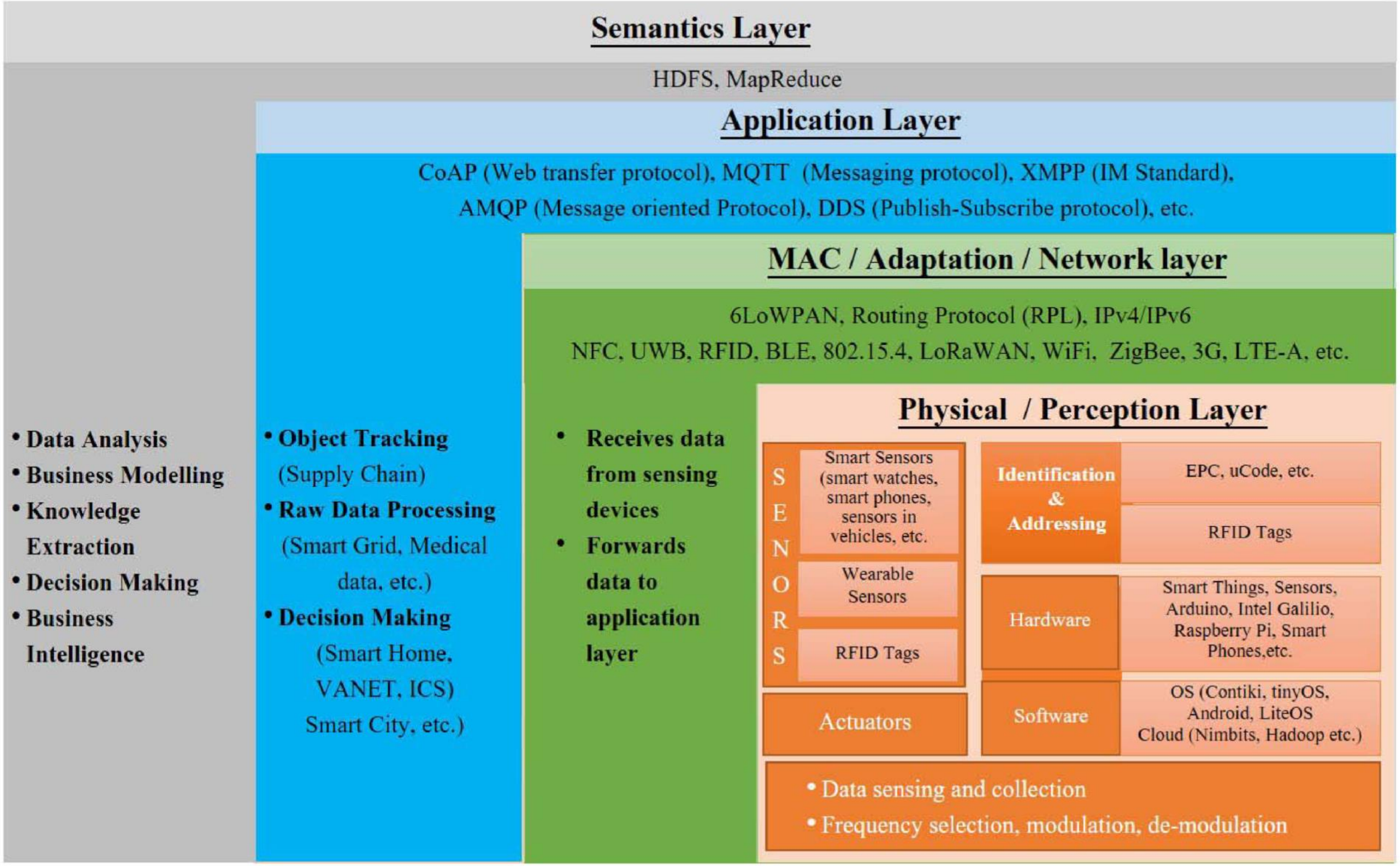


Fig. 2. IoT Protocol Stack.

2. Threats to the IoT

❖ IoT vs Traditional Network

➢ Significant difference between conventional networks and IoT is the level of the resourcefulness of end devices[26].

Architecture	Traditional Network	IoT Network
Device	plentiful resource devices (computer server, smartphone, etc.)	resource constraint embedded devices (RFID, sensor nodes, etc.)
Memory	high	low
Computing power	high	low
Disk space	high	low
Power consumption	high	low
Security protocol	complex & multi-factor security protocol	protocol with lightweight security algorithm
Communication	secure and faster (DSL/ADSL, WiFi, 4G, LTE, etc.)	slow and less secure (802.15.4, 802.11a/b/g/n/p, LoRa, ZigBee, NB-IoT, SigFox, etc.)
Data format	almost same OS and data format	application-specific data type and lack of OS
Security	firewall, IDS/IPS, host-based anti-virus and SW patches	absence of host-based approach (AV, patches), lack of IoT-focused attack signature, cross-device dependency

2. Threats to the IoT

Cryptography and Information Security Lab

❖ Generalized Threats

Threat	Vulnerability Exploited	Attach Method
Eavesdropping and traffic analysis	Lack of encryption and network access control	
Masquerading and unauthorized disclosure of personal information	Weak data security, authentication and authorization mechanism	
Device integrity	Lack of physical security, no temper-proofing, trustless environment, open physical interfaces, boot process vulnerabilities	H/W attack, Side-channel attack, Reversing attack
Remote code execution	Lack of host-based of string network level security	Mirai[44]
Software/Code integrity	No malware detection mechanism, weak network and application layer security	Mirai[44], Gooligan[17]
Threats to communication protocols (MITM, unauthorized access, DoS)	Spoofing the ARP, brute-forcing pre-shared Wi-Fi keys, vulnerability in the exchange of disassociation message	ARP spoofing, IMSI catching
DoS (Resource exhaustion) attacks	Weak network and application layer security	

2. Threats to the IoT

❖ Threats at Difference Layers of IoT Architecture (Physical/Perception Layer)

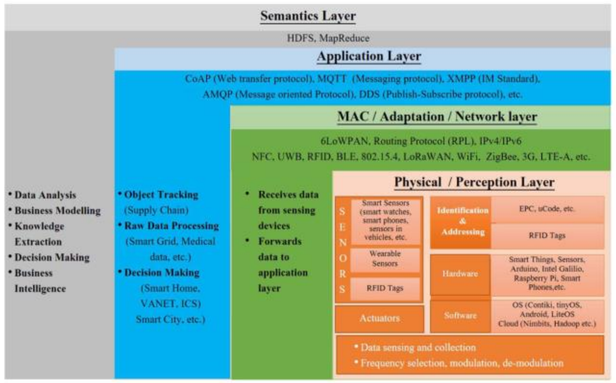


Fig. 2. IoT Protocol Stack.

Threat	Vulnerability Exploited
Eavesdropping	Unprotected communication channel, no encryption
Battery drainage attacks	Unchecked volume of legal requests, lack of spam control
Hardware failure/exploitation	Negligence by the manufacturers, faults of developers, unprotected interfaces, weak application/web/network security
Malicious data injection	Weak access control
Sybil attack	Lack of identity and device management
Disclosure of critical information	Lack of physical protection for the devices
Device compromise	Vulnerable physical interface, boot process vulnerability
Timing attack and hardware exploitation	Open debugging ports
Node cloning	Lack of standardization and hardware security and temper-proofing
Semi-invasive and invasive intrusions	Lack of physical security and temper-proofing
Change of configuration/Firmware-version	Weak implementation of cryptographic algorithm
Unauthorized access to the devices	Use of default or hardcoded username and passwords

2. Threats to the IoT

❖ Threats at Difference Layers of IoT Architecture (MAC/Adaption/Network Layer)

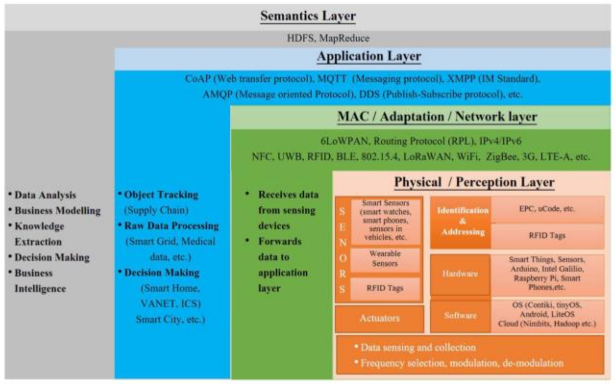


Fig. 2. IoT Protocol Stack.

Threat	Vulnerability Exploited
Unfairness, impersonation and interrogation attack	Weaknesses in communication protocols (channel access scheme), MAC spoofing, weak network access control
DoS attack to include collision attack, channel congestion attack, battery exhaustion attack, exploitation of CSMA, PANId conflicts	Flaws in medium-access control and communication process
Fragmentation attack	Lack of security mechanism in 6LoWPAN
MITM, eavesdropping	Weak authentication and data security
Spoofing, hello flood and homing attacks	Weak authentication and anti-replay protection
Network intrusion and device compromise (remotely using malware)	Weak network intrusion detection/prevention system, weak device access control once the device is operational, inefficient identity management
Message fabrication/modification/replay attacks	Weak data authentication and anti-replay protection
Node replication attack and insertion of rogue devices	Weak network and device access control mechanism
Selective forwarding attack, Sybil attack, wormhole attack, blackhole attack	Weaknesses in network routing protocols
Storage attack	Centralized data storage, non-replication of data storage, no protection against malware such as cryptlocker and ransomware
DoS attacks launched by sending fake/false messages to a node, server or a gateway device	Weak link layer authentication and lack of anti-replay protection

2. Threats to the IoT

Cryptography and Information Security Lab

❖ Threats at Difference Layers of IoT Architecture (Application Layer)

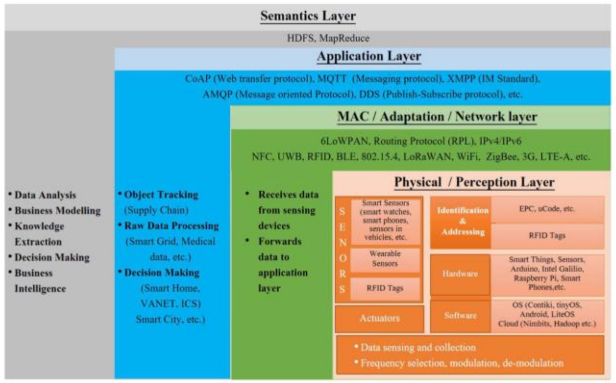


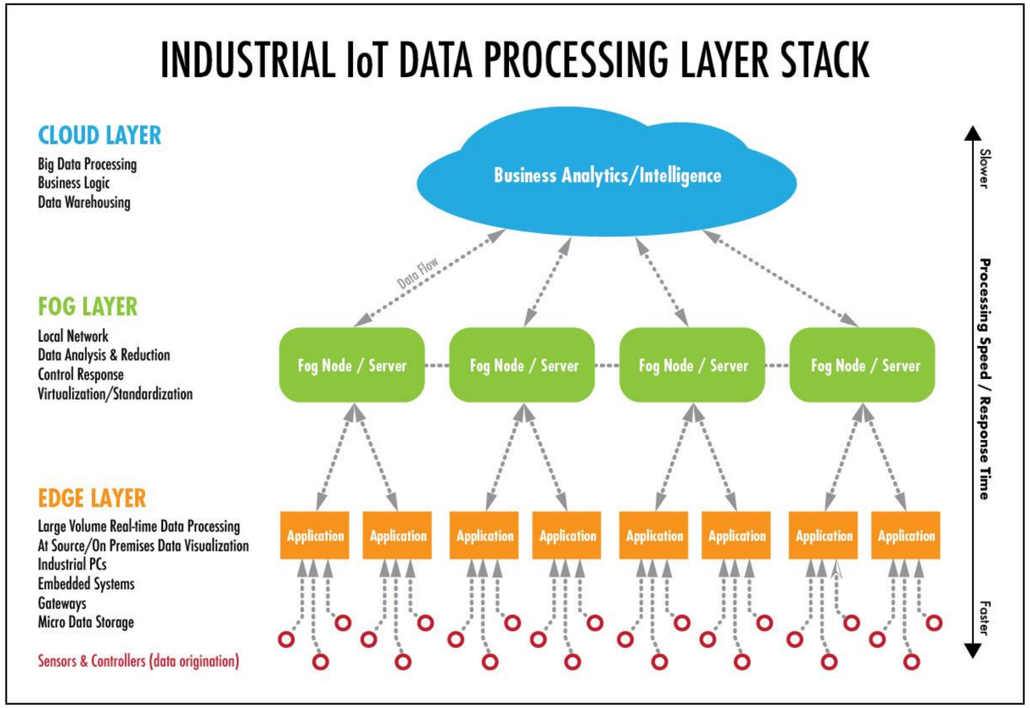
Fig. 2. IoT Protocol Stack.

Threat	Vulnerability Exploited
Malicious codes	Lack of application/web security, authentication and authorization mechanism
Software modification	Lack of application/web security
Brute force and dictionary attacks, escalation of privileges and data tempering	Weak authentication and authorization mechanism
SQL injection attacks	Injection flaws in SQL/noSQL databases, OS and Lightweight Directory Access Protocol (LDAP)
Identity theft and password/key/session token compromise	Incorrect implementation of authentication in application vis-a-vis session management
Disclosure of sensitive/private data	Insecure web application and APIs
Cross-site scripting (XSS)	Vulnerability in web applications and user unwareness

❖ Threats at Difference Layers of IoT Architecture (Semantics Layer)

Threat	Vulnerability Exploited
Identity theft, compromise of user privacy	Lack of data/application security

- Security and Privacy Challenges to Cloud-Supported IoT
  - Data originating from a various devices will be available for open sharing across a range of applications, servers, users
    - ✓ Public sharing is achieved with the cloud technologies
    - ✓ Most IoT systems are developed for a particular application
    - ✓ The security aspects are also limited to that particular application
  - Security Considerations in Cloud-supported IoT
    - ✓ Security of Data
    - ✓ Handling of Heterogeneous Data
    - ✓ User Anonymity vis-a-vis ID Management
    - ✓ In-Cloud Data Sharing
    - ✓ Large-Scale Log Management
    - ✓ Vulnerability to DoS Attacks
    - ✓ The Threat of Malicious Things



- Security and Privacy Issues in Fog Computing for IoT
  - Cloud's centralized data storage and computing framework could be single point of failure.
  - Fog computing does compliment by reducing the latency and process load.
  - Trade-off between security and availability

3. Malware Threat

- Threat: constant danger that has the potential to cause harm to an information system
  - malware, application misconfiguration, and humans

- Attack: successful execution of a malicious act by exploiting vulnerabilities in an information system
  - Xafecopy, WannaCry, Cryptlocker, Mirai, Havex, Stuxnet

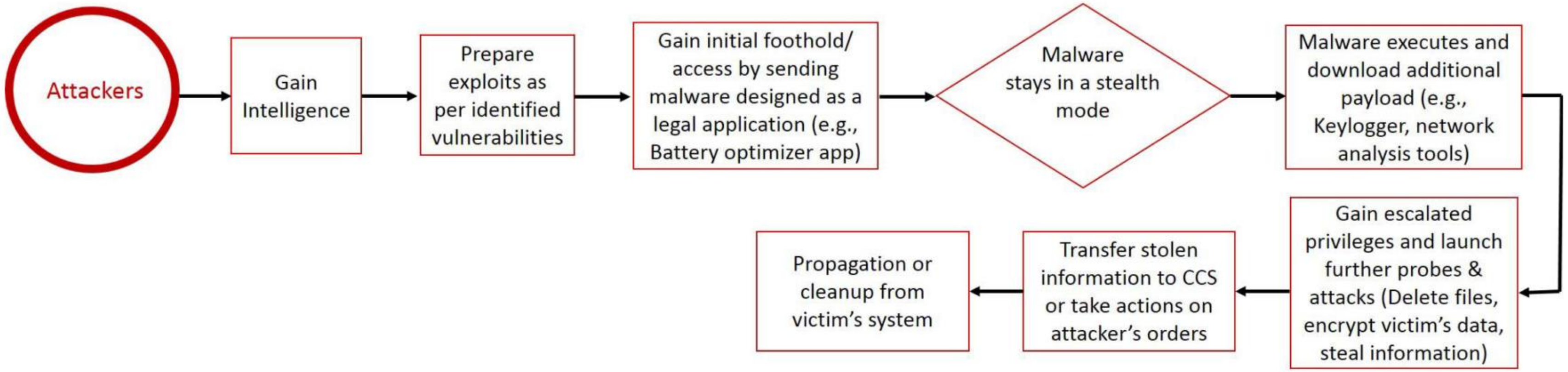


TABLE III
TRENDING IN MALWARE ATTACKS

Malware Type	1981-1990	1991-2000	2001-2010	2011-2016	2017	2018
Virus	10	07	03	-	-	-
Worm	01	02	27	01	-	-
RAT + Rootkit	-	-	21	12	-	01
Botnets	-	-	02	02	-	-
Ransomware	01	-	-	16 [99]	02	-
Total	**12**	**09**	**53**	**31**	**02**	**01**

3. Malware Threat

❖ Attack Methodology

1. Preparatory phase
2. Initial exploitation and infiltration phase
3. Execution phase
4. Propagation phase
5. Hideout and clean-up phase

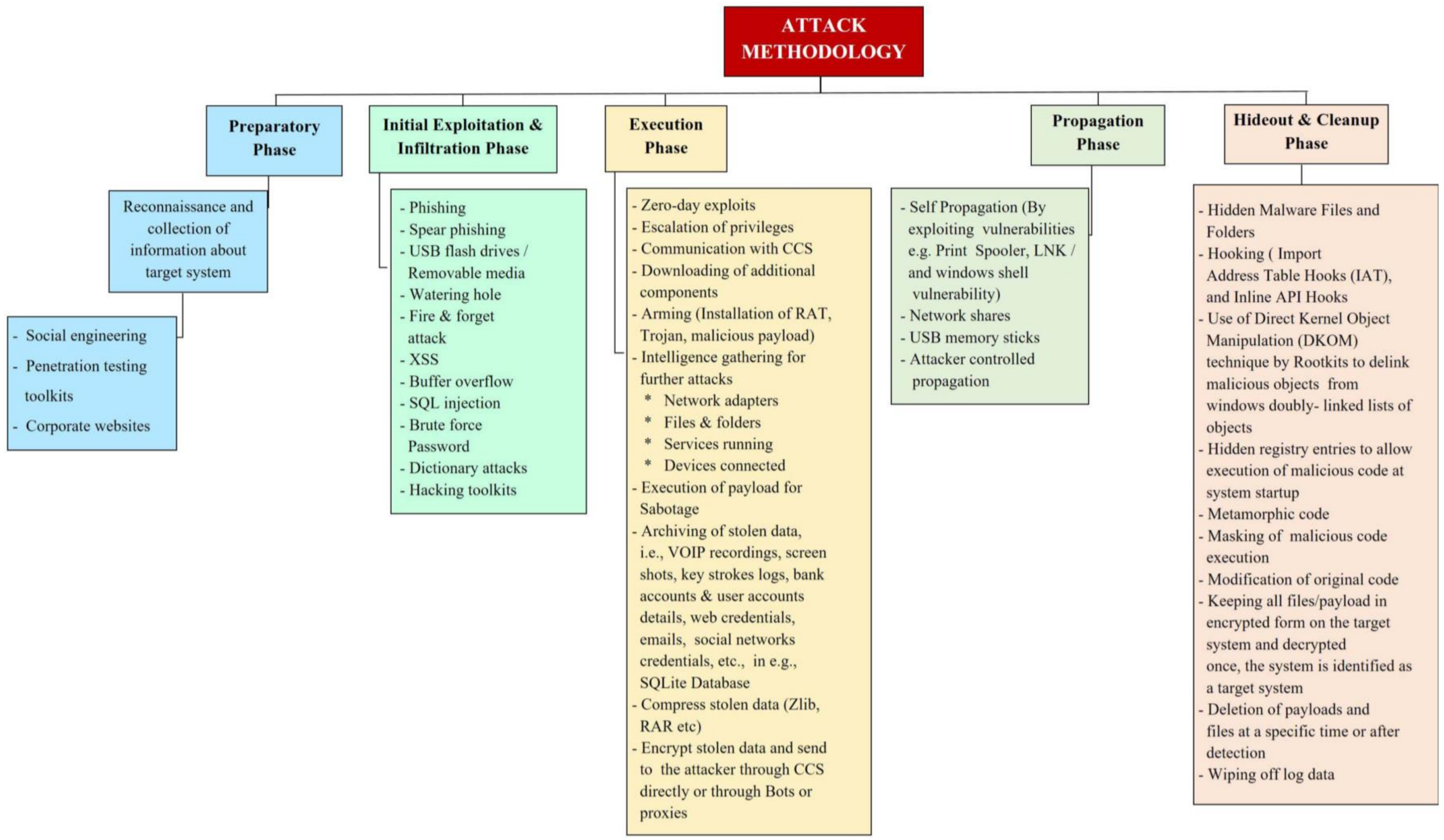
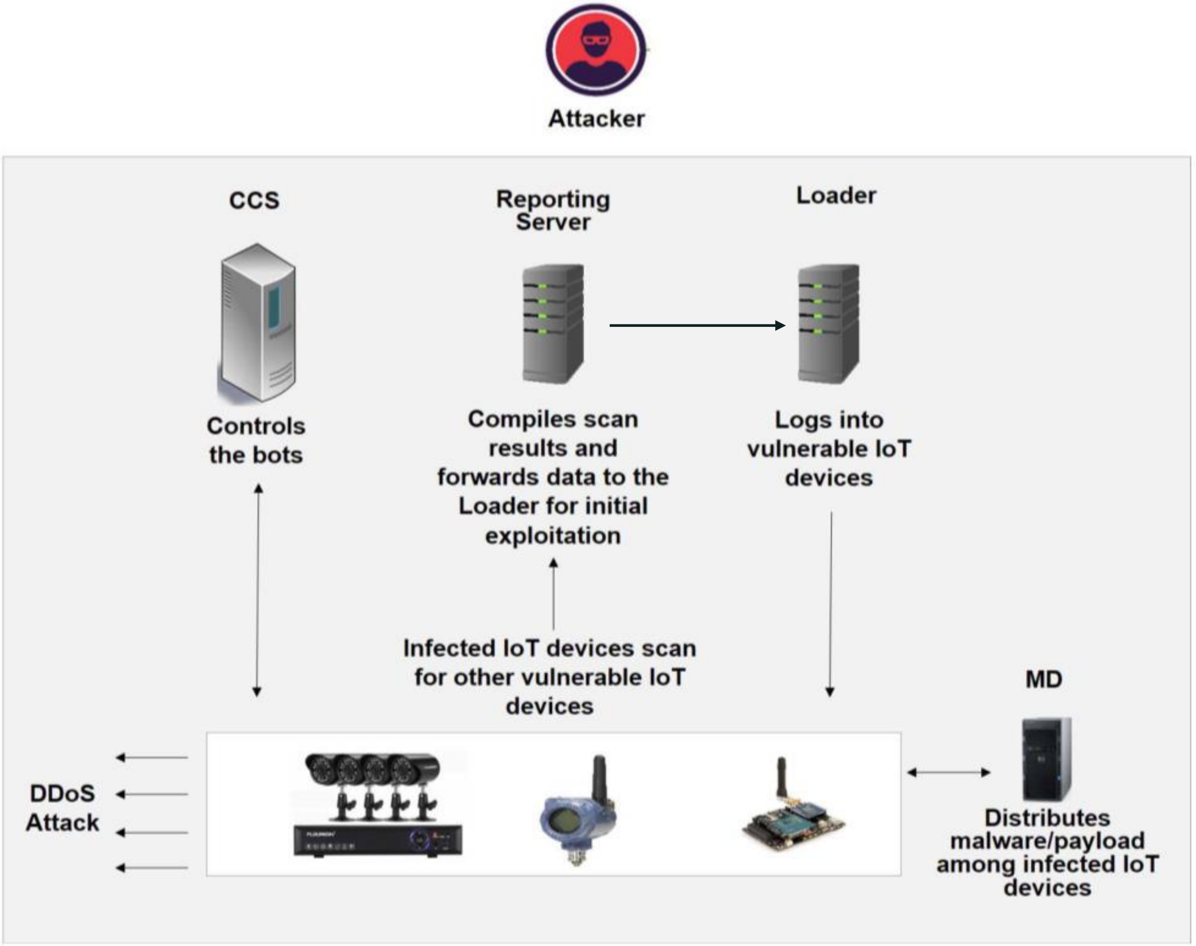


Fig. 9. Methodology of a Malware Attack Targeting IoT/ICS.

4. Gap Analysis and Security Framework

Cryptography and Information Security Lab

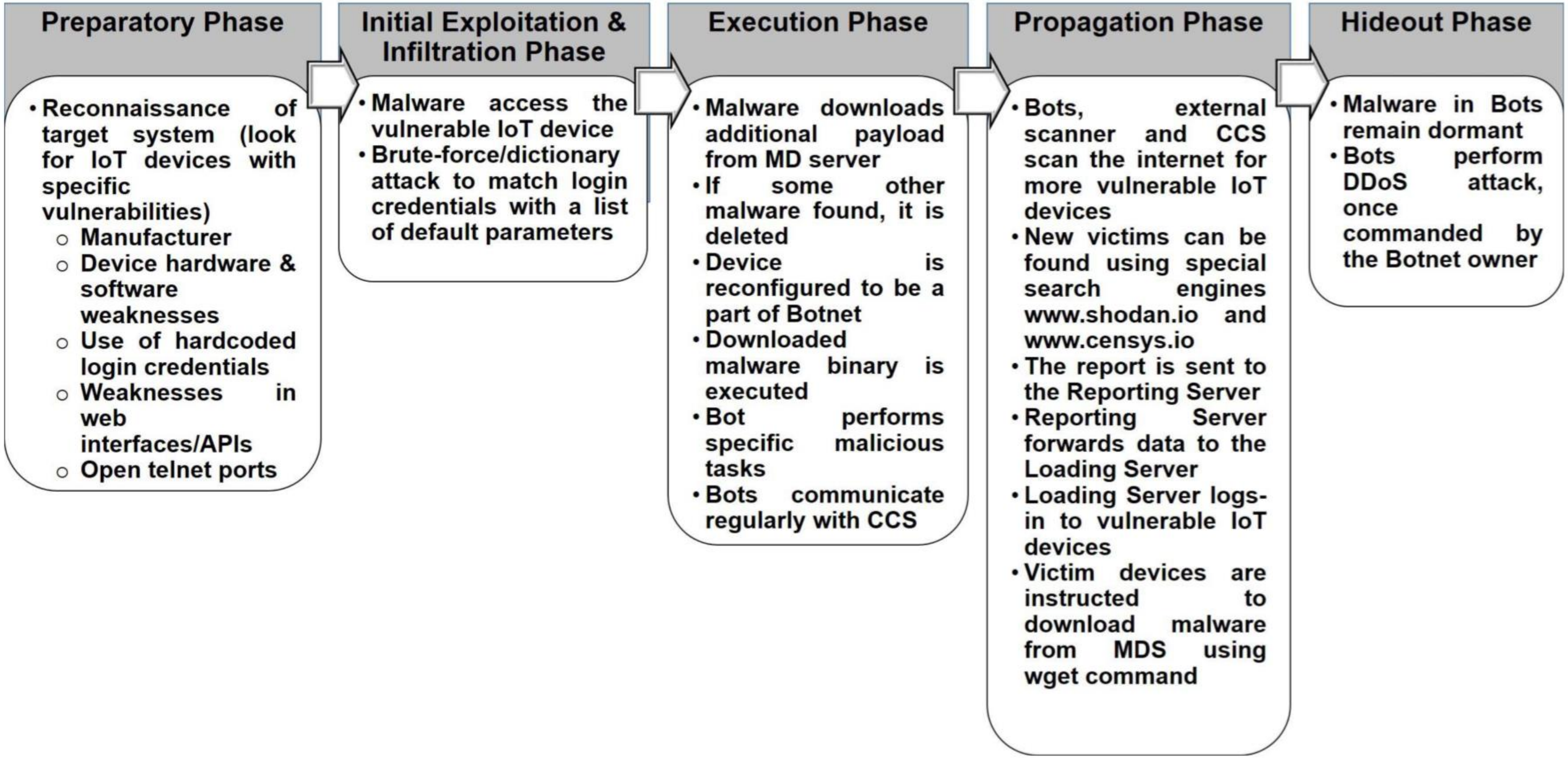
❖ high probability that IoT devices may be used to create a botnet army to launch various other attacks such as DDoS and distribution of ransomware/spyware



probable architecture of a botnet controlled by an attacker

4. Gap Analysis and Security Framework

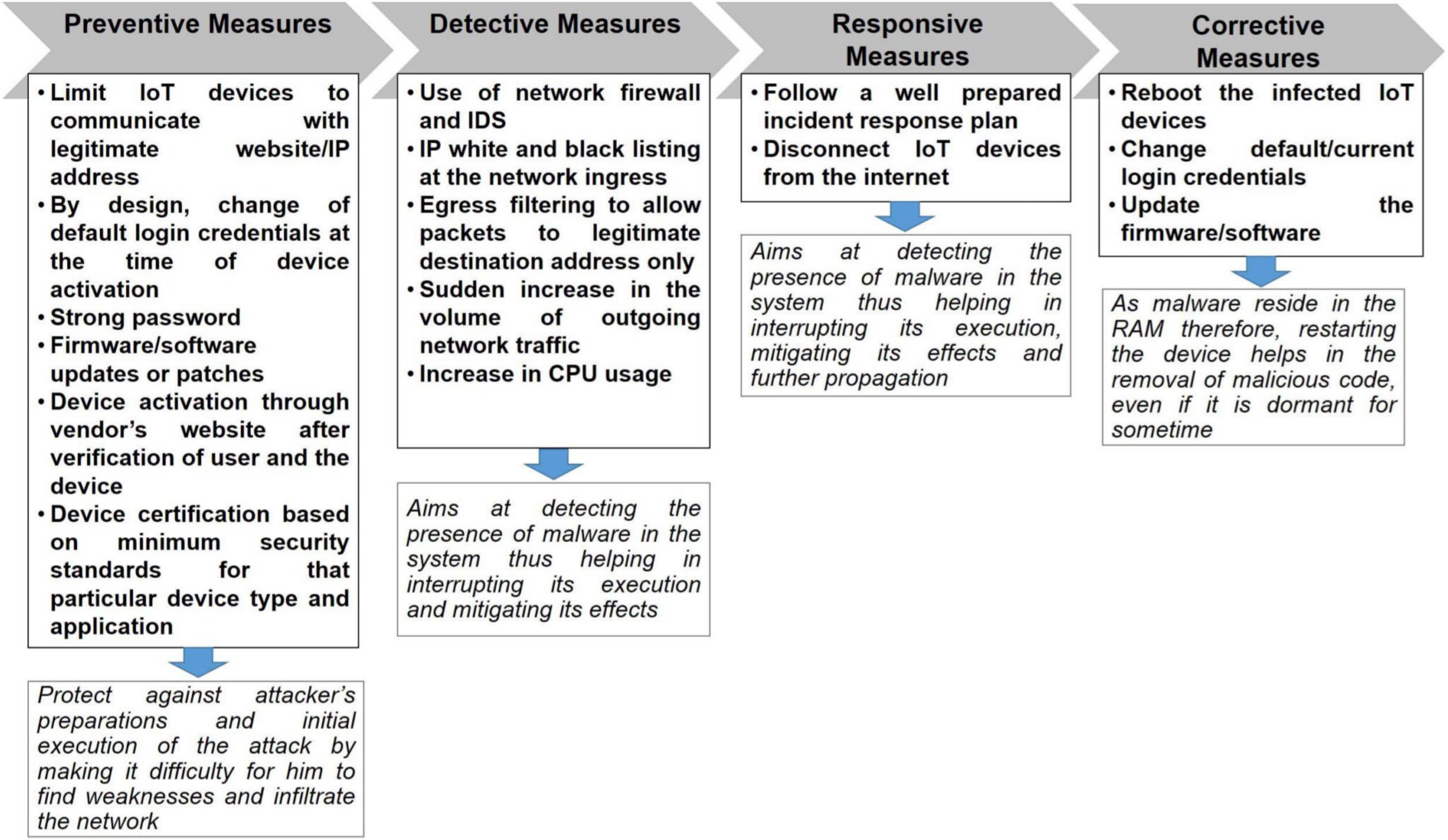
❖ DDoS Attack on IoT



4. Gap Analysis and Security Framework

Cryptography and Information Security Lab

❖ IoT Security Against DDoS Attack



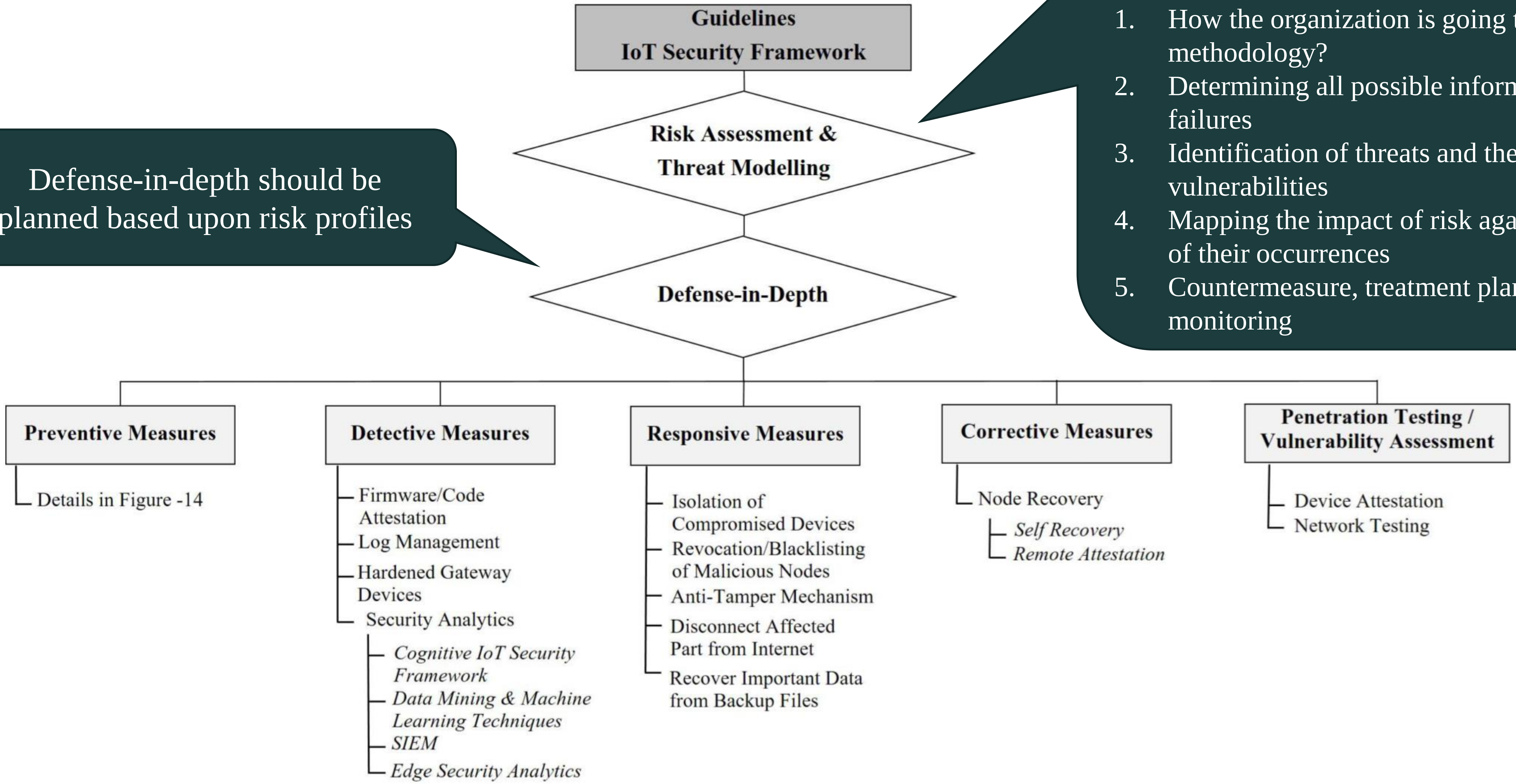
4. Gap Analysis and Security Framework

❖ Guidlines IoT Security Framework

Risk assessment for all processes, equipment, stakeholders and information assets

1. How the organization is going to define its risk methodology?
2. Determining all possible information assets and failures
3. Identification of threats and the potential vulnerabilities
4. Mapping the impact of risk against the likelihood of their occurrences
5. Countermeasure, treatment plan and continuous monitoring

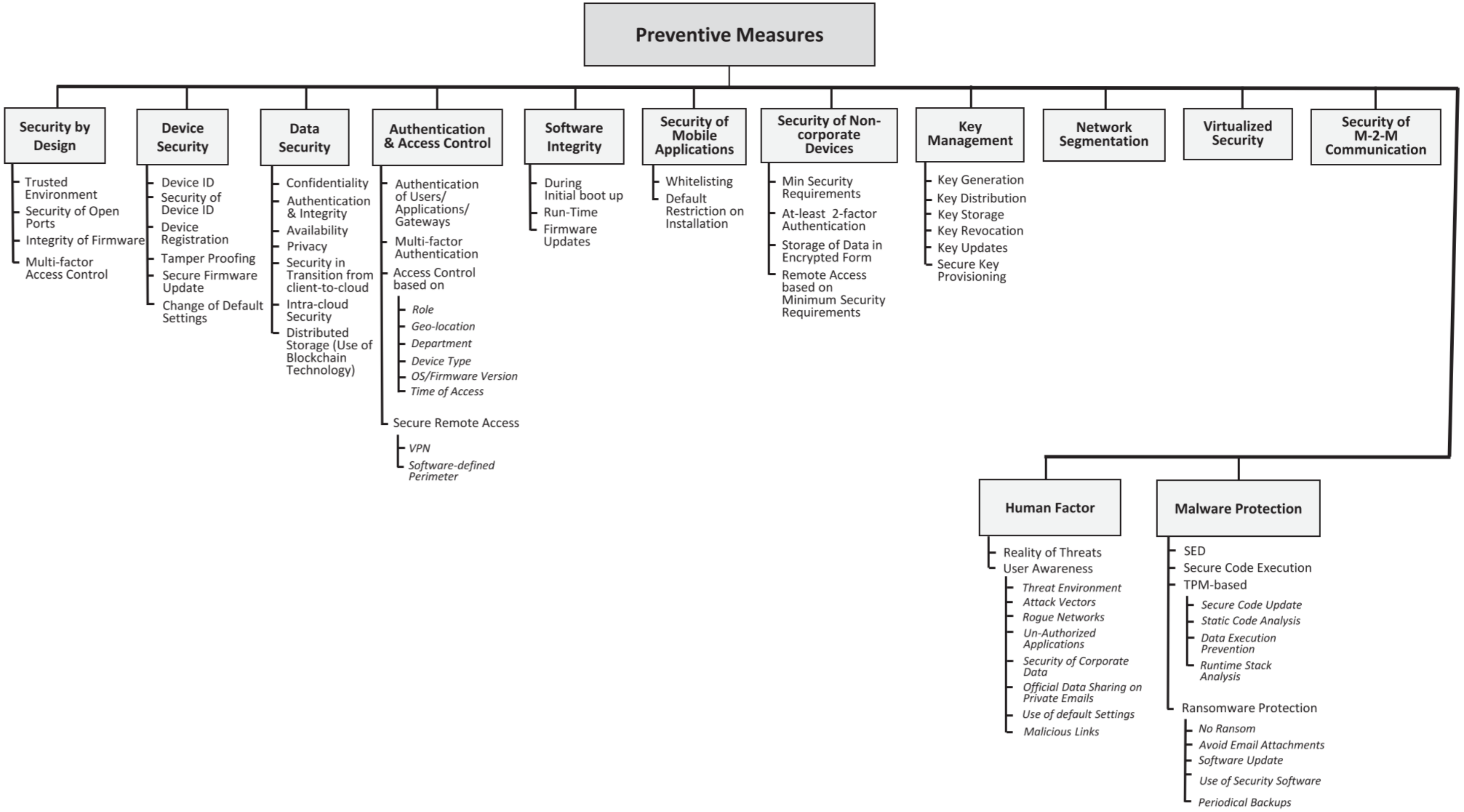
Defense-in-depth should be planned based upon risk profiles



4. Gap Analysis and Security Framework

Cryptography and Information Security Lab

❖ Guidlines IoT Security Framework – Prevention Measure



5. Summary, Lessons Learnt and Pitfalls

Cryptography and Information Security Lab

❖ Snapshot of the impact of security

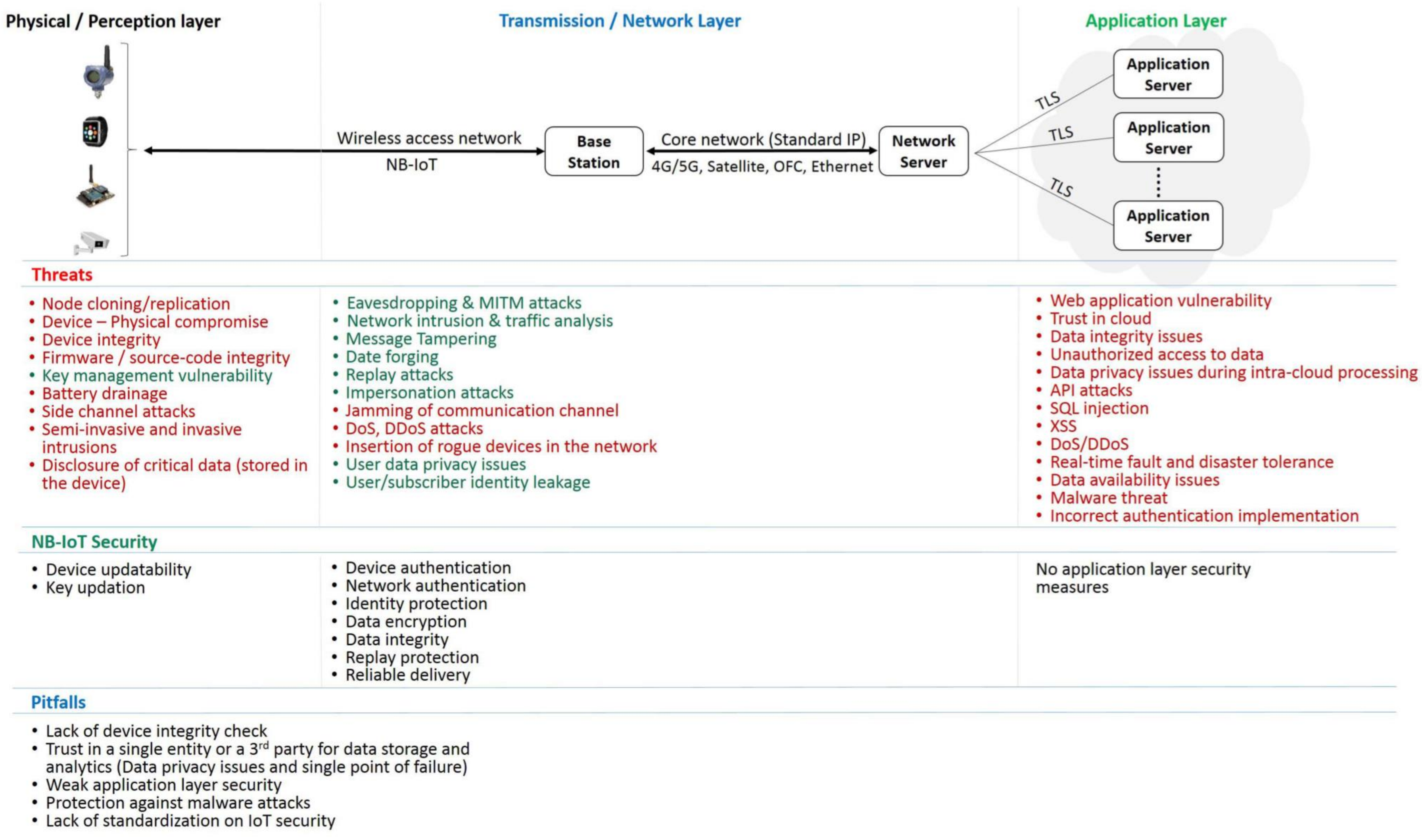


Fig. 15. NB-IoT Security in IoT Threat Environment.

Feature	LTE-M	NB-IoT
Licensed spectrum	Yes	Yes
Device / subscriber authentication	UICC/eUICC	UICC/eUICC
Network authentication	Yes LTE-AKA	Yes LTE-AKA
Identity protection	TMSI	TMSI
Data confidentiality	128-AES	128-AES
Data integrity	Limited	DoNAS (Optional)
Control signal integrity	Yes	Yes
End-to-Middle security	No	No
Forward secrecy	No	No
Replay protection	Yes	Yes (Optional)
Reliable delivery	Yes	Yes
Device updatability	Yes	Yes
Keys updatability	Yes (Optional	Yes (Optional)
Updation of long term keys	Yes (OTA)	Yes (OTA)
Requirement of certified equipment	Yes	Yes
IP network	Yes (Optional	Yes (Optional)

5. Summary, Lessons Learnt and Pitfalls

Cryptography and Information Security Lab

- IoT threats at various layers exploit different vulnerabilities and use different attack vectors to achieve malicious objectives.
- Attacks at physical layer cannot be protected only by cryptographic security provided by IoT communication protocols.
- DDoS attacks are mostly launched through compromised IoT devices.
- Absence of anti-virus/malware detection mechanism in IoT is one of the causes of successful attacks on the integrity of the code/software of an IoT end device[8], [9].
- Security is not the primary concern while designing IoT technologies or products.
- Standard IT security protocols cannot be deployed on resource constraint IoT devices.
- Security is a holistic property. Hence, it should not be considered in isolation.

6. Open Research Challenges

Cryptography and Information Security Lab

- Baseline Security Standard
  - taking into account the constraint resources of many IoT devices, there is a need to develop lightweight fully optimized cryptographic security protocols for IoT devices[199].

- Privacy-Preserving Data Aggregation and Processing

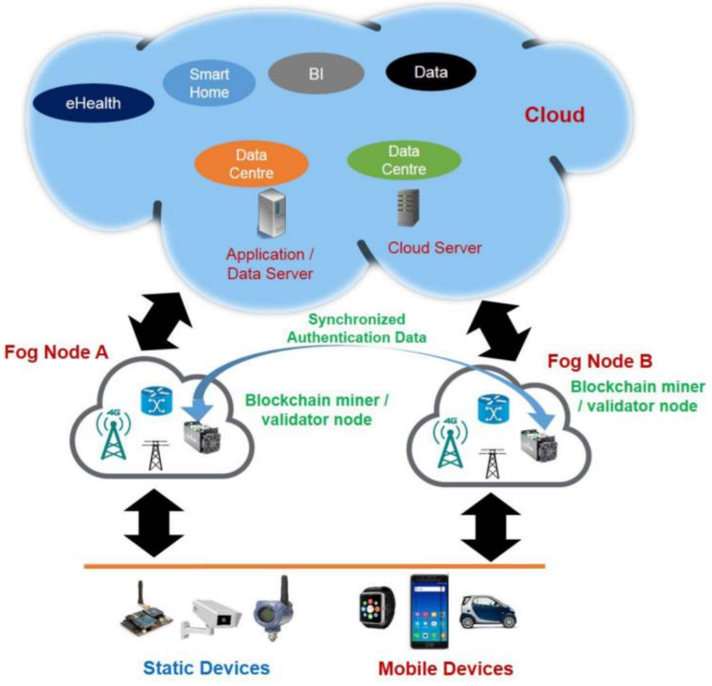
- Software/Code Integrity
  - the most dependable solutions are hardware-based that require execution of complete attestation process in a secure environment.
  - there is a need to explore a secure software-based solution that can be easily deployed in resource constraint IoT devices with the flexibility of timely upgradation.

6. Open Research Challenges

❖ Blockchain – An Instrument to Augmented IoT Security

❖ Challenges to Fog Computing in IoT

➢ challenges in fog computing is to realize identity authentication while ensuring low latency of real-time services, the mobility of users, decentralized fog computing nodes and avoiding de-anonymization attacks[210].



BLOCKCHAIN for IOT

Bitcoin Blockchain Pros & Cons	Features Suited for IoT & Research Challenges
Transaction integrity & authentication	Transaction integrity & authentication
Non repudiation	Non repudiation
No double spending / avoids duplication	No replay
Prevents data forgery	Prevents data forgery
Decentralized control	Decentralized control
User anonymity	Identity management vis-à-vis user privacy
Neutralizes affects of Ransomware & Cryptlocker	Needs to neutralize affects of Ransomware & Cryptlocker
Ideal for untrusted environment	Untrusted Environment
Public Blockchain	Can be Public / Private / Consortium Blockchain
No encryption	Encryption (data security at rest & in transit)
Latency & low throughput	Near real-time transaction confirmation
PoW consensus is computation and energy intensive	IoT focused consensus with low energy, computation and communication overheads
Scalability issues	Should be scalable
Financial value based transaction validation	Needs IoT centric transaction validation

7. Conclusion and Future Work

Cryptography and Information Security Lab

- Contributions
  - Highlighted most of the known threats to the IoT systems by quoting examples of some of the real attacks
  - Presented a comprehensive attack methodology for most common real-world attacks
  - Deduced an attack strategy of a DDoS attack through IoT botnet followed by requisite security measu
  - Presented a comprehensive set of security guidelines based on industry best practices
  - Discussed open research challenges related to IoT security

- Future work: Blockchain
  - Blockchain can solve most of the data integrity issues of IoT due to its ability to run distributed apps in the form of smart contracts and storing data on multiple nodes.

8. Opinions

- IoT Security =

  Lower communication layer security (based on resource-restricted environment) +

  Upper communication layer (based on security in data flow)

- For IoT Security
  - Integrated and secure communication framework or architecture (from physical layer to application and semantic layer)
  - Entirely modulated protection technique
  - **High quality of Semantics Layer** (for defense-in-depth) with **omnipotent data expression**

- IoT Security with 5G
  - 5G is communication technology based on physical communication.
  - When 5G is emerged with IoT, the trade-off between limitation of resource and performance of physical communication should be considered.

CIS LAB

Thank you for your attention