CECS 579 - Information Security, California State University, Long Beach

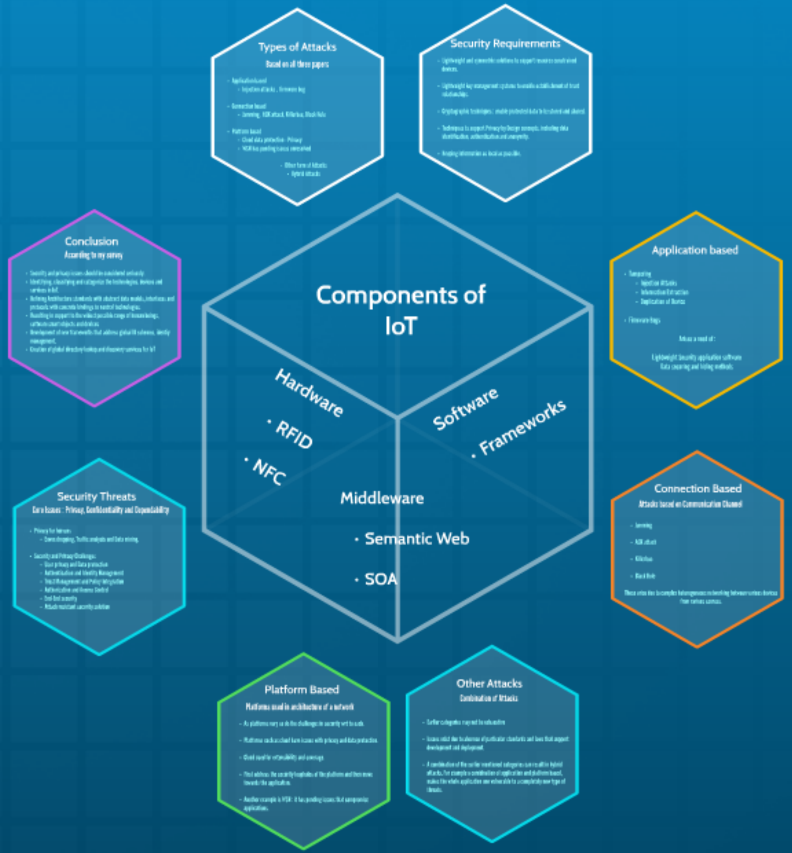
A Study of IoT

Attacks, Security threats and Requirements

Introduction

- IoT (Internet of Things) is a vision to ensure devices stay connected and collaborate with each other over the internet.
- Allows objects to be sensed and controlled remotely across existing infrastructure.
- " Things ", in IoT sense refer to devices, which are uniquely identified.
- These devices collect useful data that can be exchanged.

- Where there is communication, there are always ATTACKS



Types of Attacks

Based on all three papers

- Application based
  - Injection attacks , firmware bug
- Connection based
  - Jamming, KCK attack, Killerbee, Black hole
- Platform based
  - Cloud data protection - Privacy
  - NSX has pending issues unresolved
- Other form of Attacks
  - Hybrid attacks

Security Requirements

- Lightweight and symmetric solutions to support resource constrained devices.
- Lightweight key management systems to enable establishment of trust relationships.
- Cryptographic techniques : enable protected data to be stored and shared.
- Techniques to support Privacy by Design concepts, including data identification, authentication and anonymity.
- Keeping information as local as possible.

Conclusion

According to my survey

- Security and privacy issues should be considered seriously.
- Identifying, classifying and categorize the technologies, devices and services in IoT.
- Defining Architecture standards with abstract data models, interfaces and protocols with concrete bindings to neutral technologies.
- Providing in support to the widest possible range of human beings, software smart objects and devices.
- Development of new frameworks that address global ID schemes, identity management.
- Creation of global directory lookup and discovery services for IoT

Components of IoT

Hardware
- RFID
- NFC

Software
- Frameworks

Middleware
- Semantic Web
- SOA

Application based

- Tampering
  - Injection Attacks
  - Information Extraction
  - Duplication of Device
- Firmware Bugs

Arises a need of :

Lightweight Security application software
Data scanning and hiding methods.

Security Threats

Core Issues :: Privacy, Confidentiality and Dependability

- Privacy for humans
  - Eaves dropping, Traffic analysis and Data mining.
- Security and Privacy Challenges:
  - User privacy and Data protection
  - Authentication and Identity Management
  - Trust Management and Policy Integration
  - Authorization and Access Control
  - End-End security
  - Attack resistant security solution

Connection Based

Attacks based on Communication Channel

- Jamming
- KCK attack
- Killerbee
- Black Hole

These arise due to complex heterogeneous networking between various devices from various sources.

Platform Based

Platforms used in architecture of a network

- As platforms vary so do the challenges in security set to each.
- Platforms such as cloud have issues with privacy and data protection.
- Cloud used for scalability and coverage.
- First address the security loopholes of the platform and then move towards the application.
- Another example is NSX : it has pending issues that compromise applications.

Other Attacks

Combination of Attacks

- Earlier categories may not be exhaustive
- Issues exist due to absence of particular standards and laws that support development and deployment.
- A combination of the earlier mentioned categories can result in hybrid attacks. For example a combination of application and platform based, makes the whole application are vulnerable to a completely new type of threats.

AGENDA

- Introduction to IoT
- Components of IoT
- Types of Attacks on IOT
- Application based Attacks
- Connection based Attacks
- Platform based Attacks
- Other Attacks
- Security threats and Requirements

Conclusion

by Anuj Sharma 012755572

CECS 579 - Information Security, California State University, Long Beach

A Study of IoT

Attacks, Security threats and Requirements

Introduction

- IoT (Internet of Things) is a vision to ensure devices stay connected and collaborate with each other over the internet.
- Allows objects to be sensed and controlled remotely across existing infrastructure.
- "Things ", in IoT sense refer to devices, which are uniquely identified.
- These devices collect useful data that can be exchanged.

  - Where there is communication, there are always ATTACKS

AGENDA

Introduction to IoT

Components of IoT

Types of Attacks on IOT

Application based Attacks

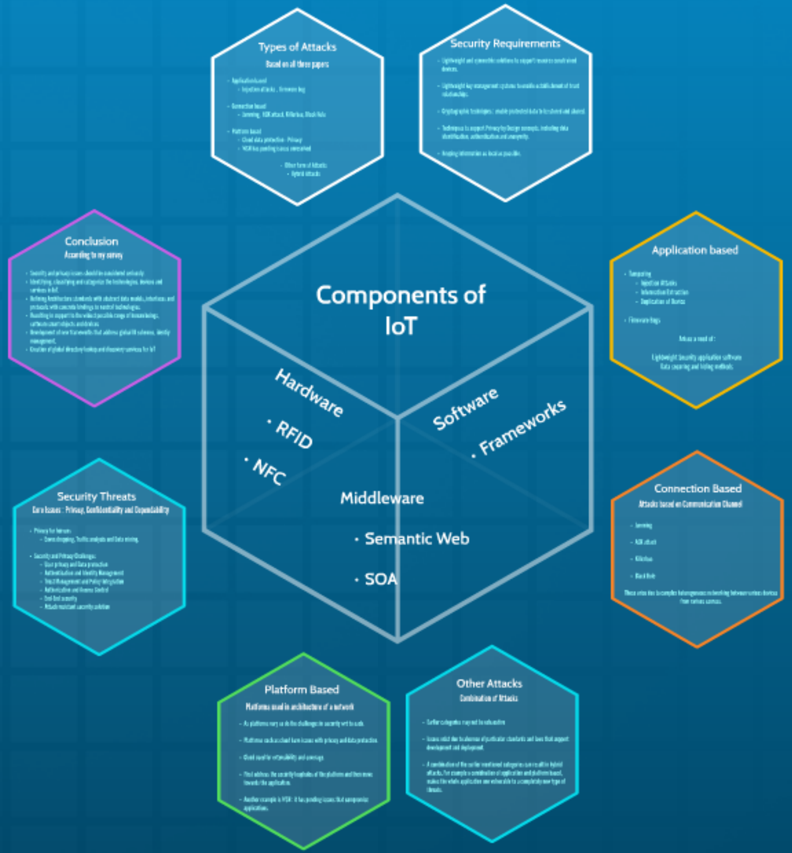
Connection based Attacks

Platform based Attacks

Other Attacks

Security threats and Requirements

Conclusion



Types of Attacks

Based on all three papers

- Application based
  - Injection attacks , firmware bug
- Connection based
  - Jamming, NSK attack, Killerbee, Black Hole
- Platform based
  - Cloud data protection - Privacy
  - NSK has pending issues unresolved

  - Other form of Attacks
    - Hybrid attacks

Security Requirements

- Lightweight and symmetric solutions to support resource constrained devices.
- Lightweight key management systems to enable establishment of trust relationships.
- Cryptographic techniques : enable protected data to be stored and shared.
- Techniques to support Privacy by Design concepts, including data identification, authentication and anonymity.
- Keeping information as local as possible.

Conclusion

According to my survey

- Security and privacy issues should be considered seriously
- Identifying, classifying and categorize the technologies, devices and services in IoT.
- Defining Architecture standards with abstract data models, interfaces and protocols with concrete bindings to neutral technologies.
- Resulting in support to the widest possible range of human beings, software smart objects and devices.
- Development of new frameworks that address global ID schemes, identity management.
- Creation of global directory lookup and discovery services for IoT

Components of IoT

Hardware
- RFID
- NFC

Software
- Frameworks

Middleware
- Semantic Web
- SOA

Application based

- Tampering
  - Injection Attacks
  - Information Extraction
  - Duplication of Devices
- Firmware Bugs

Arises a need of :

Lightweight Security application software
Data capturing and hiding methods

Security Threats

Core Issues : Privacy, Confidentiality and Dependability

- Privacy for humans
  - Eaves dropping, Traffic analysis and Data mining.
- Security and Privacy Challenges:
  - User privacy and Data protection
  - Authentication and Identity Management
  - Trust Management and Policy Integration
  - Authorization and Access Control
  - End-End security
  - Attack resistant security solution

Connection Based

Attacks based on Communication Channel

- Jamming
- NSK attack
- Killerbee
- Black Hole

These arise due to complex heterogeneous networking between various devices from various sources.

Platform Based

Platforms used in architecture of a network

- As platforms vary so do the challenges in security set to scale.
- Platforms such as cloud have issues with privacy and data protection.
- Cloud used for extensibility and coverage.
- First address the security loopholes of the platform and then move towards the application.
- Another example is NSK : it has pending issues that compromise application.

Other Attacks

Combination of Attacks

- Earlier categories may not be exhaustive
- Issues exist due to absence of particular standards and laws that support development and deployment.
- A combination of the earlier mentioned categories can result in hybrid attacks. For example a combination of application and platform based, makes the whole application are vulnerable to a completely new type of threats.

by Anuj Sharma 012755572

Prezi

AGENDA

- Introduction to IoT
- Components of IoT
- Types of Attacks on IOT
- Application based Attacks
- Connection based Attacks
- Platform based Attacks
- Other Attacks
- Security threats and Requirements

Conclusion

Introduction

- IoT (Internet of Things) is a vision to ensure devices stay connected and collaborate with each other over the internet.
- Allows objects to be sensed and controlled remotely across existing infrastructure.
- " Things ", in IoT sense refer to devices, which are uniquely identified.
- These devices collect useful data that can be exchanged.

  - Where there is communication, there are always ATTACKS usion

my survey

l be considered seriously.
orize the technologies, devices and

vith abstract data models, interfaces and
to neutral technologies.
possible range of human beings,
s
hat address global ID schemes, identiy

n and discovery services for IoT

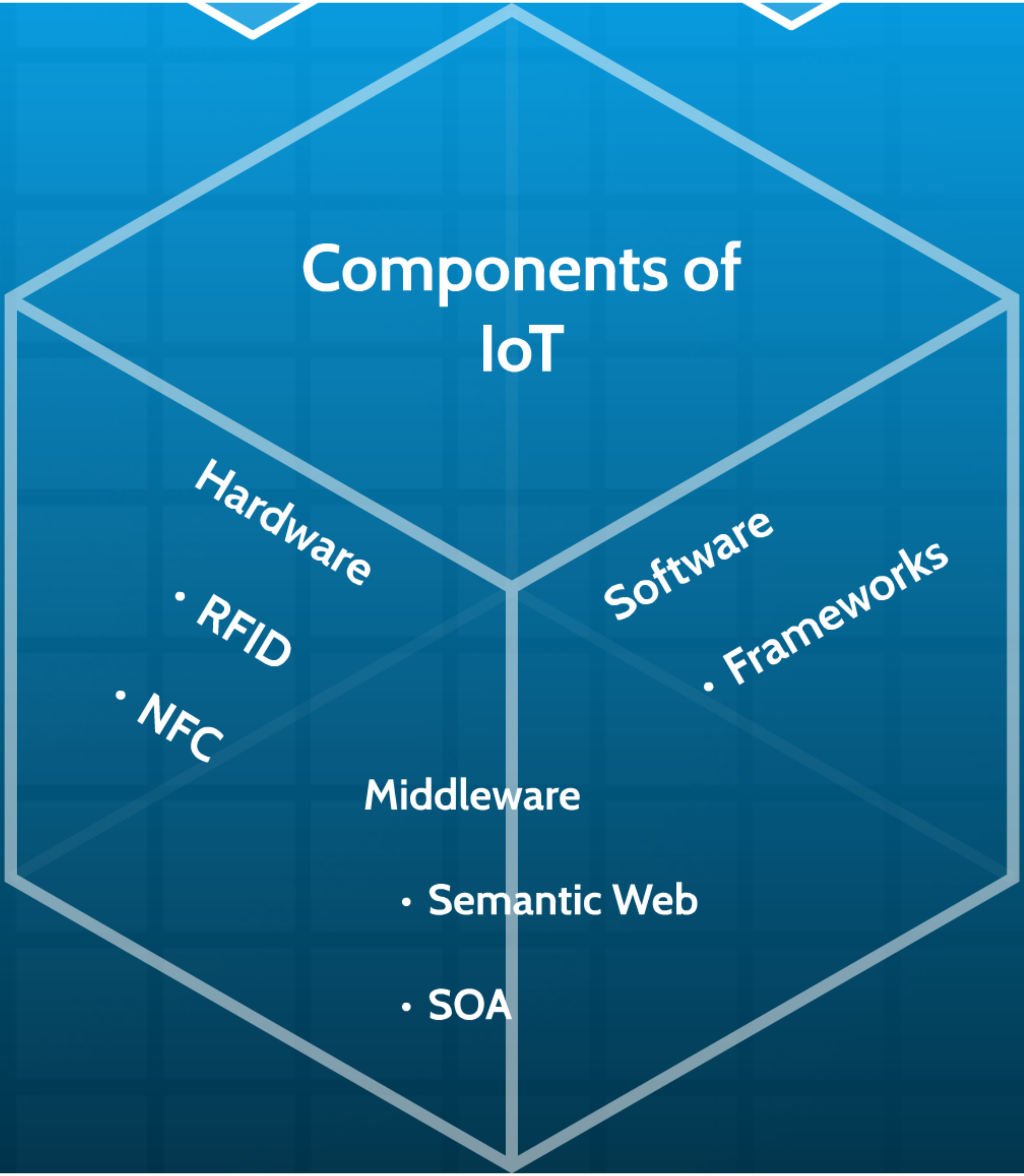
y Threats

fidentiality and Dependability

lysis and Data mining.

ection
y Management
icy Integration
Control

olution



Components of IoT

Hardware

- RFID
- NFC

Software

- Frameworks

Middleware

- Semantic Web
- SOA

Applicatio

- Tampering
    - Injection Attacks
    - Information Extraction
    - Duplication of Device
- Firmware Bugs

Arises a r

Lightweight Security a
Data securing and

Connectio

Attacks based on Commu

- Jamming
- ACK attack
- Killerbee
- Black Hole

These arise due to complex heterogene
from vario

Types of Attacks

Based on all three papers

- Application based
    - Injection attacks , firmware bug

- Connection based
    - Jamming, ACK attack, Killerbee, Black Hole

- Platform based
    - Cloud data protection - Privacy
    - WSN has pending issues unresolved

- Other form of Attacks
    - Hybrid Attacks

Application based

- Tampering
  - Injection Attacks
  - Information Extraction
  - Duplication of Device

- Firmware Bugs

Arises a need of :

Lightweight Security application software
Data securing and hiding methods

Connection Based

Attacks based on Communication Channel

- Jamming
- ACK attack
- Killerbee
- Black Hole

These arise due to complex heterogeneous networking between various devices from various sources.

Platform Based

Platforms used in architecture of a network

- As platforms vary so do the challenges in security wrt to each.
- Platforms such as cloud have issues with privacy and data protection.
- Cloud used for extensibility and coverage.
- First address the security loopholes of the platform and then move towards the application.
- Another example is WSN : it has pending issues that compromise applications.

- Earli
- Issue
devel
- A con
attac
make
threa

ch.

rotection.

n move

mise

Other Attacks

Combination of Attacks

- Earlier categories may not be exhaustive
- Issues exist due to absence of particular standards and laws that support development and deployment.
- A combination of the earlier mentioned categories can result in hybrid attacks. For example a combination of application and platform based, makes the whole application one vulnerable to a completely new type of threats.

Security Threats

Core Issues : Privacy, Confidentiality and Dependability

- Privacy for humans
  - Eaves dropping, Traffic analysis and Data mining.
- Security and Privacy Challenges
  - User privacy and Data protection
  - Authentication and Identity Management
  - Trust Management and Policy Integration
  - Authorization and Access Control
  - End-End security
  - Attack resistant security solution

Security Requirements

- Lightweight and symmetric solutions to support resource constrained devices.
- Lightweight key management systems to enable establishment of trsut relationships.
- Cryptographic techniques : enable protected data to be stored and shared.
- Techniques to support Privacy by Design concepts, including data identification, authentication and anonymity.
- Keeping information as local as possible.

Conclusion

According to my survey

- Security and privacy issues should be considered seriously.
- Identifying, classifying and categorize the technologies, devices and services in IoT.
- Defining Architecture standards with abstract data models, interfaces and protocols with concrete bindings to neutral technologies.
- Resulting in support to the widest possible range of human beings, software smart objects and devices
- Development of new frameworks that address global ID schemes, identiy management.
- Creation of global directory lookup and discovery services for IoT

CECS 579 - Information Security, California State University, Long Beach

A Study of IoT

Attacks, Security threats and Requirements

Introduction

- IoT (Internet of Things) is a vision to ensure devices stay connected and collaborate with each other over the internet.
- Allows objects to be sensed and controlled remotely across existing infrastructure.
- " Things ", in IoT sense refer to devices, which are uniquely identified.
- These devices collect useful data that can be exchanged.

- Where there is communication, there are always ATTACKS

AGENDA

Introduction to IoT

Components of IoT

Types of Attacks on IOT

Application based Attacks

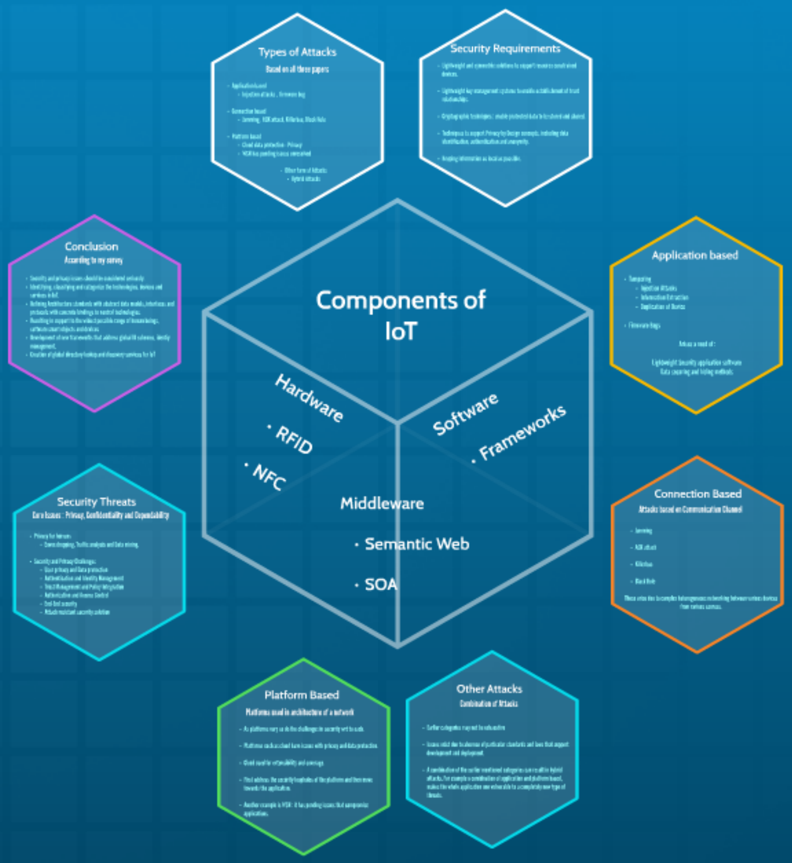
Connection based Attacks

Platform based Attacks

Other Attacks

Security threats and Requirements

Conclusion



Types of Attacks

Based on all three papers

- Application based
  - Injection attacks , firmware bug
- Connection based
  - Jamming, NDN attack, Killerbee, Black hole
- Platform based
  - Cloud data protection - Privacy
  - NDN has pending issues unresolved
- Other form of Attacks
  - Hybrid attacks

Security Requirements

- Lightweight and symmetric solutions to support resource constrained devices.
- Lightweight key management systems to enable establishment of trust relationships.
- Cryptographic techniques : enable protected data to be stored and shared.
- Techniques to support Privacy by Design concepts, including data identification, authentication and anonymity.
- Keeping information as local as possible.

Conclusion

According to my survey

- Security and privacy issues should be considered seriously.
- Identifying, classifying and categorize the technologies, devices and services in IoT.
- Defining Architecture standards with abstract data models, interfaces and protocols with concrete bindings to control technologies.
- Providing in support to the widest possible range of human beings, software smart objects and devices.
- Development of new frameworks that address global ID schemes, identity management.
- Creation of global directory lookup and discovery services for IoT

Components of IoT

Hardware

- RFID
- NFC

Software

- Frameworks

Middleware

- Semantic Web
- SOA

Application based

- Tampering
  - Injection Attacks
  - Information Extraction
  - Duplication of Devices
- Firmware Bugs

Arises a need of :

Lightweight Security application software
Data covering and hiding methods

Security Threats

Core Issues :: Privacy, Confidentiality and Dependability

- Privacy for humans
  - Eaves dropping, Traffic analysis and Data mining.
- Security and Privacy Challenges:
  - User privacy and Data protection
  - Authentication and Identity Management
  - Trust Management and Policy Integration
  - Authorization and Access Control
  - End-End security
  - Attack resistant security solution

Connection Based

Attacks based on Communication Channel

- Jamming
- NDN attack
- Killerbee
- Black Hole

These arise due to complex heterogeneous networking between various devices from various sources.

Platform Based

Platforms used in architecture of a network

- As platforms vary so do the challenges in security set to each.
- Platforms such as cloud have issues with privacy and data protection.
- Cloud used for adaptability and coverage.
- First address the security loopholes of the platform and then move towards the application.
- Another example is NDN : it has pending issues that compromise applications.

Other Attacks

Combination of Attacks

- Earlier categories may not be exhaustive
- Issues exist due to absence of particular standards and laws that support development and deployment.
- A combination of the earlier mentioned categories can result in hybrid attacks. For example a combination of application and platform based, makes the whole application one vulnerable to a completely new type of threats.

by Anuj Sharma 012755572