Internet of Things: Impact of IoT in Business Environment and Challenges in Secure Implementation

Archana Sharma

Abstract: ***The Internet of Things as new paradigm is interconnection of computing ,physical and mechanical device together with people with the ability to transfer the data over network. The embedded devices may gather and swap over data with the support of network connectivity, sensors and electronics. The diversified deployment area of IoT are not limited to smart home application, health care industry, education industry and agriculture, etc. It also taking step ahead in developing new products or services in business. With the help of this emerging technology business will have the major impact by improved customer engagement, productivity enhancement, and better access to data, enhanced inventory tracking and security*****. Whereas t****he rapid growth rate of IoT network is getting attention of the cyber criminals. In recent advancement, different types of embedded IoT devices are connected together with wireless network and continuously access internet for communication. Cyber criminals are finding vulnerabilities on IoT devices and compromise them to launch massive attacks (e.g. DDoS, Spamming, MITM, RFID Skimming) to destroy the network. IoT devices having default authentication credentials are easy target. This paper highlights that how IoT may introduce the better opportunities in business and challenges of secure IoT connection and while communicating the IoT device. This research also highlights the security aspects of existing technologies and existing technologies and challenges with implementation.***

Keywords: IoT, sensors, tracking device, embedded system, digital signature, DSA, RSA

I. INTRODUCTION

With the exponential growth of the ICT , it has a major impact of a person's daily life like the various domestic appliances could exchange data using build-in data sensors, automation of various services etc. Earlier, the "smart" devices were part of the science fiction movies, but now a days these devices are the part of routine life. The life become more comfortable due to these technologies and generate a variety of conveniences, different services have been speed up and automated the management. A threat of dependency on these new technologies in different application areas is really a serious issue, thus users need to be learned the proper functioning of these objects properly. As in current scenario, the Internet of Things is the need to explore the business, retail and various application areas and the presented research highlights its main applications in various aspects of life and challenges. In present communication paradigm, the Internet of Things visualize a near future, in which the Physical Objects, Controller, Sensor, Actuators are grouped together through Internet for digital communication and desired protocol stacks as an integral part of the Internet make all these resources able to communicate with one another. [1] Digital economy have realized the technology's influence and various business models have been developed to gain astonishing profits. Now a days, there are Nemours number of scope to implement new digital business models by for traditional companies.

II. TECHNOLOGIES AND OPPORTUNITIES FOR RETRANSFORMATION OF BUSINESS STRATEGY

To involve new technologies and more dependency on technologies in business environment, companies should be more responsive. Innovative tools are needed to build the strategies. Such innovative competitive strategies can effectively change their business models and fulfill the expectations of stakeholders[2]. The business models need to be connected with the technological innovation, satisfying the customer's need and delivering satisfaction [3]. With the consideration of new factors affecting the business model, IoT , the companies can achieve better performance. The distinctive opportunities may be provided by Internet of Things to penetrate technology and automation in various applications of the business and provide a massive area for businesses to develop innovative business models to hold the market share[4]. In all aspects of the user's lives generates data in different manner like Smart watches, smartphones, trackers, etc keep track of each and every step and sense also. With these insights customer and producer get benefited. Eventually, the scenario is being emerged towards into an Internet of Things (IoT) world due to beneficiary for everyone while keeping inter connected to the things and people. The IOT devices help in monitoring of import process by record and data transfer and provides the innovative insights, improve efficiency, and permit companies to make more knowledgeable decisions. With help of AI and analytics , which can identify the patterns of use or behavior , IoT briefs the organizations, what exactly happening in organizations , more willingly than what they presume or expect is happening. The traditional retailers are also benefited with the IOT tools to compete and coexist with the online vendors as "omni-channel" shopping wipe away the dissimilarity between online and offline shops. The Internet of

Revised Manuscript Received on June 22, 2020.
*Corresponding Author
Dr. Archana Sharma, IT Department, Institute of Management Studies Noida, Noida, India. E-mail: asharma12569@gmail.com

Things, may direct the shopper about the item consumer has been looking at online at the time customer enters the retail shop and text her a personalized coupon to make the shop in-store that day. IoT technology can also provide data to optimize store layouts, enable fully automated checkout, and fine-tune inventory management.

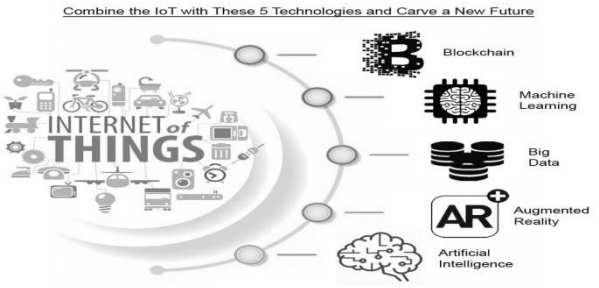

Figure 1: IoT with Revolutionary Technologies

Due to customer centric approach of the business now a days, Internet of things (IoT) has become the buzz word of the Industries and getting success. Two categories of devices are more focused in IoT, first as sensors which gather and track data and other one will be responsible to perform the action based on the data get received from such devices like locks , actuators, alarms etc. Based on these devices, numerous applications has been developed in different types of manufacturing and service industries.

Thus, the combination of IoT and other innovative technologies are needed to collaborate together to make the significant different kind of applications area including business.

A. Combination of IoT with Revolutionary Technology Trends

- *The IoT and Blockchain*

In Business world, the IoT and blockchain provides the additional security to first kind of data which gather the data. In blockchain data has been encrypted and managed the real-time data securely with the support of distributed filing system.

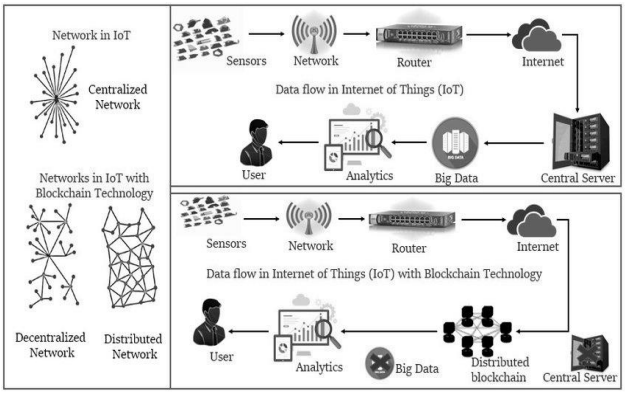

Figure 2: IoT and Blockchain

With the combination of these two, various smart devices get connected securely and automated to detain and store data. Due to revolution of IoT with blockchain, many business look forward to ensure the rigorous data security and avoid the data breaches.

Applications with the combination of IoT and Blockchain technology -

- Tracking activity can be applied by installing a system where a supply chain system in multiple organization.
- Automated System with the data encryption will improve security of data.

- *The IoT and Big Data*

Increasing gathering of devices in IoT brings the innovative technology- the Big Data. In real-time, the Sensors detain the data and as a consequence of the massive nature of this information, certain scenario is desired to process it on-the-go, without having to captureing and storing the data. The entire success of IoT depends on the data.

The critical basis of the success of IoT depends on the data and how it gets stired up across the system. Thus Big data technology and the IoT are so strongly connected, to consider both of them as separate entities and transforming business together towards a singular goal.

Impact of IoT and Big Data in Business

- Numerous data have been captured by the enterprises pertaining to their customers, products and services to improve their decision making-keeping data at the central of significant decisions.
- Enterprises will make real-time decisions about their prices, sales, logistics etc. by getting correct information processes into actionable insights.

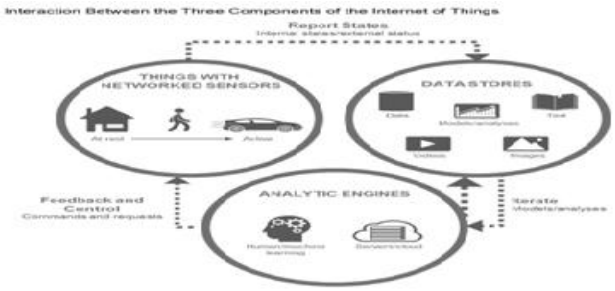

Figure 3: IOT and Big Data

- *The IoT and Machine Learning*

IoT applications are totally based on machine-to-machine communication. In general the IoT solutions are static. Thus, there is a need of thought to impart intelligence to machine to know about the desired parameters have shifted. Machine intelligence is the important factor for any machine to modify the outcome of any operations. It supports various formats for stir up knowledge into devices locally and this knowledge may also be transferred among the connected devices.

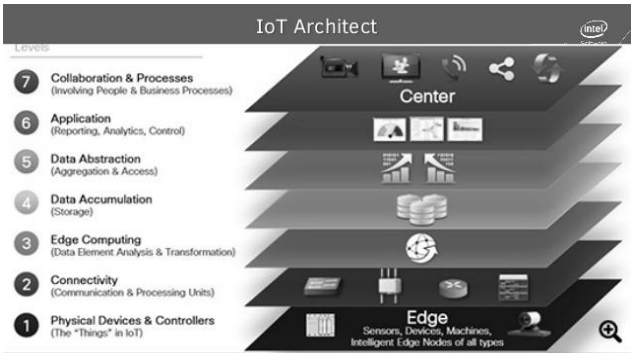

Figure 4: IoT and Machine Learning

Impact of IoT and ML on Business

- Machine Learning solutions with IoT may save the huge amount of cost while applying the preventive measure by setting up an alarms at time maintenance will be required by machine.
- By combining the Iot and Machine learning Business can generate their cunsumer's purchasing behavior patterns according to their purchasing habits.
- Room Temperature can be automatically set with these two combination in hospitality industry.

- *The IoT and Artificial Intelligence*

Two major technologies, IoT and Artificial Intelligence with their combination create use case in all different kind of industries globally. All major companies make use of these devices as IoT is capable to capture data from various end devices and with the support of AI, these devices may become smart.

Use cases :

- Operational functionality of equipments can be improved by predictive maintenance and anomaly of the equipments may be identified timely.
- Operational efficiency can be significantly improved by generating predictions of the tasks which can be automated in an organization.

III. ADVANTAGES OF INTERNET OF THINGS

The impact of IoT on Business (5,6) as advantage are as follows:

A. Communication – Built-in-sensors and various technologies ensures a permanent connection among the devices and data exchange between these devices and users. There are various examples of it like it make possible to track the health indicators of patients, items and goods location during transportation, building status monitoring etc.

B. Automation and Control – In case of IoT application installed on the consumers devices like tablets, phone can remotely control the AI enabled devices(smart devices) and may choose the options accordingly. Automatics massage sending, warning may be possible to these devices, like ordering of food by fridge from supermarket in case of product shortfall, room temperature control at their home while they are far away.

C. Cost savings of time, money and resources– The response times and human labor have been reduced due to strong connectivity and fast communication among devices, which increased efficiency and productivity. Many of the home appliances make the homes "smart" while saving electricity, money and extra resources. Predictive maintenance can help in preventing the failures in IoT ecosystems.

IV. SECURITY CHALLENGES OF IOT

The identical Internet based technologies to IoT are the major issues and challenges like - data security and protection of data and quality maintenance ,interoperability proper the use of common standards and protocols, interoperability, legal issues, etc.

Some foremost challenges have been facing while deployment of the Internet of Things [7] are as follows:

Making a common addressing mechanism deployment for effective addressing of the devices, low cost embedded devices availability with more energy efficient and reliable, need of governing bodies to govern the usage of the devices, to be the fast and reliable communication, load minimization with fast response time minimizing the load on servers as and on the embedded devices etc . are the major issues , which are needed to be solved by all participants, especially government and companies. They all must be united to understand the issues and try to solve them accordingly in time and implementation of policies under the law for proper use of the Internet of Things.

A. Privacy: Perceived privacy where individual data can be accessed is one of the biggest challenges. Tracking of devices identification , their action which are performed, and the collection of personal data of the user from various applications make feel scout to the user and threat of the data privacy [8].

B. Security: IoT devices use internet for communication hence vulnerable to external threats. Cyber criminals can attack the IoT device and use them as a bot. Further these devices can be used as botnets to destroy communication of a victim network. Botnets are major threats for IoT. Botnets are nothing but compromised internet connected IoT devices. Attackers can use these compromised devices as botnet to launch DDoS attacks. Aidra, Bashlite, Linux/IRCTelnet, Hajime, Linux.Wifatch, Brickerbot and Mirai are some popular IoT botnets. Hajime is one of the IoT botnet who targets IoT devices via Telnet and gains access by brute-forcing default credentials. Although defaults credentials of devices like routers must be changed before use, however this could be ignored. These devices are easy target for cyber criminals. TLS, SSL and Digital Signature Certificate standards can be used for security from such threats [9][10]. Digital signatures are gaining legal acceptance over the traditional hand-written signatures. it works on a public key cryptography which is designed to protect the genuineness of a digital document. Digital signature schemes have been proposed in to get overcome the security problems in authentication, confidentiality, and Integrity related problems in IoT.

Many digital signature schemes have been proposed earlier like RSA, DSS, and Al-Gamal digital signature schemes. Using digital signature for secure authentication process would certainly prevent the IoT devices to be compromised easily. Figure 1 represents the base model of digital signature algorithm. Digital signature is a proof that coming message or command is from authentic source [11][12].

Table I. Advantages and dis-advantages of some widely used digital signatures[13].

Signature Scheme	Advantage	Disadvantage	Signing Speed
RSA	fearless key distribution large networks have smaller number of keys	SlowOperation High computation cost Vulnerable to multiplicative attacks	Slow
DSA	Short signature length Lower signature computation time Less storage requirement	Signature verification must have complicated remainder operators	Moderate
ECDSA	No application performance issues Fast signing and verifying process Support for national information protection standards	A chance of error that makes it possible to select a private key value and identical signatures for different documents can be obtained. Requires a random number per signature.	Moderate
EdDSA	High speed High performance Independence of the random number generator	Can be hacked by large quantum computers	Fast
BLS [23]	Short signatures Better performance Simplified computing No need of random number Many signature blocks can be combined into a single signature.	Pairing is hard and not efficient Security proof is hard	Fast

Digital signatures are getting used in e-commerce, banking, software systems and an effective technique to verify authenticity and non-repudiation of the message. All these sectors have versatile computing devices connected through a network, need a very strong authentication scheme to verify the identity proof and genuineness of transmitted data. Many digital signature schemes have been proposed by researchers to mitigate the security related vulnerabilities in IoT. In table II, we have illustrated some newest digital signatures with their technical summary. These digital signature techniques certainly deliver us new improved algorithms that provide the better security than earlier algorithms. Still these digital signature algorithms need to be verified for their hidden drawbacks to present an improved and completely secure Internet of Things network. This improvement is also necessary to make its users fearless about security related risks in IoT. Secure communication is the key requirement between two communicating IoT devices. The owner of the IoT network may need to upgrade the firmware of IoT devices to deploy some security patches. It is to be ensured that data transmission is to be done within a secure and authenticated environment.

In many cases, cybercriminals may compromise the communicating device and use them as a bot to launch future attacks to harm a specific target system. Patching or executing a malicious program can lead to severe damages or losses if the device is deployed in a critical environment such as smart power grids, nuclear facilities, traffic management systems or flight management systems. So, this is highly required to verify the authenticity of the receiver before transferring the confidential data or installing the important patches. There are several digital signature schemes such as DSA, ECDSA, EdDSA but the problem with these cryptographic signatures they are very much insecure and vulnerable to be broken by a quantum computer [10]. There should be a stronger, complex and unbreakable algorithm for the digital signature scheme so that security of IoT devices can be ensured.

Table II. Different Digital Signature Schemes implemented in IoT for security.

Digital Signature Scheme	Year	Proposed By	Technique Used
Shortened Complex Digital Signature Scheme (SCDSA) [24]	2018	Mughal, M. A., Luo, X., Ullah, A., Ullah, S., & Mahmood, Z.	A lightweight Shortened Complex Digital Signature Algorithm (SCDSA) for providing secure communication between smart devices in human-centered IoT
Lamport Signature Scheme [25]	2018	Abdullah, G. M., Mehmood, Q., & Khan, C. B. A.	Lamport signature scheme, which is quantum resistant, for authentication of data transmission and its feasibility in IoT devices.
Proxy Blind ECDS Algorithm [26]	2018	Harini N, Kamakshi Devisetti R N, Aruna D	Elliptic Curve Cryptography (EEC) based on proxy blind signing procedure
Cloud-Based Digital Signature Application [27]	2018	Sahar A. El-Rahman, DaniyahAldawsari, OmairnahAlrashed, Ghadeer Alsubaie	a digital signature mobile applicationwhere it provides a cloud-based digital signature with high security to sustain with the growth of IoT.
Elliptic Curve Digital Signature Algorithm [28]	2016	B. Sindhu, R. M. Noorullah	Used the standards of Elliptic Curve digital signature scheme.

A. Problem Statement

An existing digital signature system must not vulnerable to attackers. An attacker can launch Fault Based Attacks and Bleichenbacher Attack in old RSA based digital signature schemes to obtain the private key. RSA-PSS may be a solution for this attack. It has been proven that the signature generated by RSA-PSS could not let the attacker extract the private key. Performance related issues can be minimized using batch processing and multithreading approaches.

ECDSA has less impact over EdDSA and is newer technology than EdDSA. EdDSA provide high performance on platforms and does not need random number for each signature. It is enough strong against side-channel attacks. EdDSA provides collision resilience, meaning that hash-function collisions do not break this system. As the table 1 presents that EdDSA is the best select digital signature scheme on various factors like performance, complexity, and speed. EdDSA has minimum disadvantages among DSA, RSA, ECDSA, BLS based short signature schemes. So this digital signature scheme is desirable in IoT network for the protection of authenticity of messages.

B. Proposed Solution

An existing digital signature system must not vulnerable to attackers. An attacker can launch Fault Based Attacks and Bleichenbacher Attack in old RSA based digital signature schemes to obtain the private key. RSA-PSS may be a solution for this attack. It has been proven that the signature generated by RSA-PSS could not let the attacker extract the private key. Performance related issues can be minimized using batch processing and multithreading approaches.

ECDSA has less impact over EdDSA and is newer technology than EdDSA. EdDSA provide high performance on platforms and does not need random number for each signature.

It is enough strong against side-channel attacks. EdDSA provides collision resilience, meaning that hash-function collisions do not break this system. As the table 1 presents that EdDSA is the best select digital signature scheme on various factors like performance, complexity, and speed. EdDSA has minimum disadvantages among DSA, RSA, ECDSA, BLS based short signature schemes. This digital signature scheme is desirable in IoT network for the protection of authenticity of messages.The only drawback of the EdDSA scheme found that it can be hacked through large quantum computers.

C. Performance Analysis

DSS is considered to be stronger than El-Gamal, since in this scheme the secret number k is harder to obtain from r because of the reduction mod q. The verification step in DSS is also faster than the corresponding step in El-Gamal, since there are fewer modular exponentiations to perform, and this is an important practicalconsideration. Performance analysis shows the RSA has the worst performance regarding signature generation time (7.8 milli seconds) and BLS has the worst performance in signature verification phase (.8.6 milli seconds). The outcome of this paper can affect the selection of digital signature scheme of the sophisticated software network system seeking security related issues. Performance analysis has been done on various factors like key size, signature size, signature generation time, and signature verification time. EdDSA has the minimum signature generation time (0.08 milli-second) and signature verification time (0.16 milli-second) having 256 bits of key size and 512 bytes of signature size. Figure 3 demonstrates the chart of signature generation time comparison and figure 4 displays the signature verification time comparison for all five selected algorithms.

V. SUMMARY

Authors have analyzed different types of digital signature schemes like EdDSA, RSA based digital signature, Lamport Signature Scheme, and Secure Proxy Blind ECDS. The working technique, advantages, security strength with limitation and drawbacks have been discussed briefly. Few problems of existing digital signature schemes for securing the IoT network have been identified like performance, complexity and storage related. Authors find EdDSA has the top performance regarding signature generation and verification processes. EdDSA can be adopted for IoT as the optimized digital signature scheme. RSA signature can be selected if signature generation is getting performed on client side. This will certainly affect the server performance as the signature verification process takes minimal time among all five selected and benchmarked digital signatures.

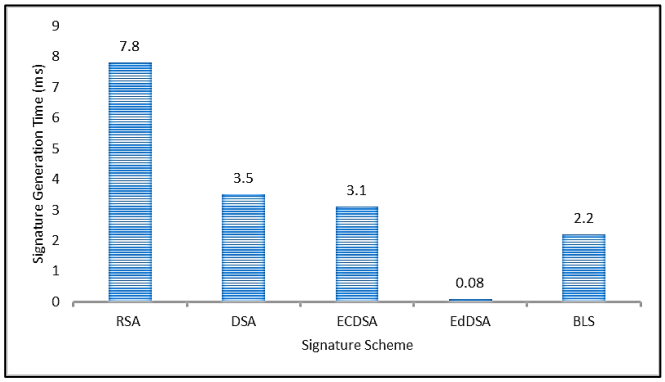

Figure. 5. Digital signature generation time comparison.

Fig. 6. Digital signature verification time comparison.

Table III. Digital Signature Schemes characteristics.

Signature Scheme	Key Size (bits)	Signature Size (bytes)	Signature Generation Time (ms)	SignatureVerification Time (ms)
RSA	1024	128	7.8	0.4
DSA	1024	384	3.5	4.5
ECDSA	160	64	3.1	8.2
EdDSA	256	512	0.08	0.16
BLS	100	20	2.2	8.6

VI. CONCLUSION

This research highlights the IoT and various emerging technologies associated with IoT like blockchain, Big Data, machine learning etc and its impact on business. The meticulous analysis of the different digital signature schemes reflects their advantages in terms of performance, correctness, complexity, suitability in IoT platform and stability against security threats found as a major challenge for IoT network. Performance improvement is the key challenge in implementing digital signature in IoT. This research opens up the need for a detailed study of practical threats and related analysis. This can possibly help to create a generic, concrete and usable authentication scheme based on the digital signature.

REFERENCES

1. Haller, S., Karnouskos, S., & Schroth, C. (2009). The Internet Of Things In An Enterprise Context Springer Berlin, Heidelberg, pp. 14-28.
2. Mahadevan, B., (2000) Business models for Internet-based e-commerce: An anatomy, alifornia Management Review, vol. 4, pp. 55-69.
3. Baden-Fuller C., and Stefan Haefliger S., Business models and technological innovation, Long Range Planning, vol. 46/6, 2013. p. 419-426.
4. Narasimha Murthy, D., Vijaya Kumar, B., (2015) Internet Of Things (Iot): Is Iot A Disruptive Technology Or A Disruptive Business Model? Indian Journal of Marketing, vol. 45/8, pp. 18-27.
5. Lopez Research LLC, An Introduction to the Internet of Things (IoT), 2013
6. Meola, A., IoT for small business: Effects, opportunities & platforms, Business Insider, http://www.businessinsider.com/internet-of-things-small-business-opportunities-platforms-2016-18
7. Rashid, H.,Securing the Internet of Things, A Technical Seminar Report submitted for fulfilment of the requirements for the Degree of Bachelor of Technology, Biju Pattnaik University of Technology, 2012
8. Roman, R., Najera, P., Lopez, J., Securing the internet of things, Computer, vol. 44, pp. 51-58, 2011.
9. Zhang, W. (2010, April). Integrated security framework for secure web services. In 2010 Third International Symposium on Intelligent Information Technology and Security Informatics (pp. 178-183). IEEE.
10. Geer, D. (2003). Taking steps to secure web services. Computer, 36(10), 14-16.
11. Hassan, R., & Qamar, T. (2010). Asymmetric-key cryptography for contiki.
12. Wong, C. K., & Lam, S. S. (1998, October). Digital signatures for flows and multicasts. In Proceedings Sixth International Conference on Network Protocols (Cat. No. 98TB100256) (pp. 198-209). IEEE.
13. ZhannaLyasota (Aug, 2018). A Guide to Digital Signature Algorithms [Online]. Available: https://dzone.com/articles/digital-signature-1.

AUTHOR PROFILE

Dr. Archana Sharma has over 26 years of experience spanning the IT industry and academia in different capacities and has published 33 research papers of which 12 are in international journals. She has also authored one text book for MCA and B.Tech. students. She has organised and attended various conferences, Faculty Development Programmes, workshops and seminars during her stint in different organizations and has been credited with awards and commendations. Her major areas of competencies include Advanced Database, DBMS,Distributed systems, Mobile Commerce, Operating System, C/C++, Data Structure, Network Security, IoT and Blockchain.